Sending E-mails – without the risk!

Secure E-Mail Communications with Rohde & Schwarz

Guide V1.1.10

Only the most recent version of this document is valid.

ROHDE&SCHWARZ

Contents

I List of figures

1 Foreword

E-mails have become an integral part of everyday life. For many years now, this medium has been used as a fast and uncomplicated way to communicate. Nevertheless, aspects that most people do not consider critical in their personal communications can be associated with substantial risks in business communications. As a communications media, e-mail is vulnerable to risks such as monitoring of e-mail content, faking of an e-mail identity, phishing or spam. Users are not always able to detect such threats at first glance. It is possible, for example, for third parties to read or falsify unsecured messages during transport. Furthermore, there is a danger of e-mails being misdirected or imitated without the sender or the recipient ever knowing that it happened. This can cause incalculable damage for both parties.

2 Security objectives and measures

In order to do a better job of mitigating the risks described in the foreword, this section describes the security objectives that Rohde & Schwarz will be seeking to achieve by implementing advanced technical measures.

2.1 Authenticity

Weak points:

Your e-mail program shows you a sender's address; however, falsifying that information is trivial from a technical perspective. As a medium, e-mail is fundamentally unsuitable for reliably verifying the sender's authenticity unless supplementary technical measures are implemented. E-mail technology makes it possible, with little effort, to hide the sender's true address or systematically steal an identity by falsifying the sender address that appears to the reader.

Threats:

Identity theft frequently occurs in connection with phishing attacks (often coupled with social engineering attacks), while general concealment of the true sender's address is used to send spam e-mails.

Measures:

Attaching a digital signature enables the recipient to verify that a given message has been sent from within the Rohde & Schwarz organization and that it was signed there digitally using a key that is assigned to a specific e-mail address. With very few exceptions, at Rohde & Schwarz, the signature of an e-mail that is visible in an external relationship was applied at a central location. These are not qualified or advanced signatures as defined by the German Signature Law (Signaturgesetz, SigG), because it is not necessary to fulfill all of the stipulations set forth in that law to achieve the primary security objectives (integrity and confidentiality).

2.2 Integrity

Weak points:

It takes relatively little effort to change the content of unprotected e-mails during transport between the person sending the e-mail and the recipient.

Threats:

In combination with identity theft, this can lead to the e-mail having an authentic structure, which lends it a correspondingly trustworthy and genuine appearance, although the content has been carefully manipulated to accomplish the purpose of an attack.

Measures:

Attaching a digital signature on the sender's end to an e-mail that is to be sent to an external destination enables the recipient to verify the integrity of the e-mail message and reliably detect any manipulation of the e-mail that might occur after the message leaves the system that signed it.

2.3 Confidentiality

Weak points:

As a medium, e-mail offers no special protection for ensuring confidentiality, and sending an e-mail can be compared to sending a post card. En route from the sender to the recipient, the message can be read at any point within the communications chain.

Threats:

Everyone who uses this medium should always be aware that "monitoring" of the worldwide flow of data is a common practice and that only a few simple tools are needed to tap into the data stream, even in smaller network environments. For this reason, it is no problem to extract information from unprotected e-mail messages without the sender or recipient ever being able to know if that happened. As a result, it is possible for a company's business-critical information to end up in the wrong hands.

Measures:

By employing suitable forms of encryption prior to sending the message via an untrustworthy (public) network, it is possible to ensure the confidentiality of the message content during transport, and – depending on the selected procedure and agreement between the communications partners – at the storage location, too.

Rohde & Schwarz makes it possible to use cryptographically secured external communications employing the recognized and standardized S/MIME[1] and PGP[2] methods. Encrypting outgoing e-mails that contain business-critical content is mandatory when the recipient's trustworthy, public key material is available. Here, Rohde & Schwarz prefers to use the S/MIME method rather than PGP.

If business-critical information is present, but there is no trustworthy key material available for the addressed recipient, the information is kept on hold and not sent. Instead, the information is held available for a certain period on the Rohde & Schwarz Secure E-Mail web interface, where it can be viewed and picked up.

For this purpose, the Rohde & Schwarz sender provides the external recipient with an initial (one-time) password via an alternative communications channel (out of band, e.g. SMS or telephone). Via the Rohde & Schwarz Secure E-Mail web interface, the recipient can also transfer valid public S/MIME or PGP key material to Rohde & Schwarz. Preferably, however, a signed e-mail should be sent to a Rohde & Schwarz recipient; that e-mail is then used to extract the key material and verify its trustworthiness.

In order to send an e-mail that has been encrypted using S/MIME or PGP to an e-mail address at Rohde & Schwarz, the recipient's key material can be obtained by requesting a signed e-

---

[1] Wikipedia (translated from the German version): S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for encrypting and signing MIME-encapsulated e-mails using a hybrid encryption system. S/MIME is a hierarchical certification model in which the authenticity of public keys is verified by a higher authority.

[2] Wikipedia (translated from the German version): Pretty Good Privacy (PGP) is a program created by Phil Zimmermann for encrypting and signing data. PGP uses a "public-key" process that employs a key pair assigned unambiguously to an identity. This pair consists of a public key that anyone can use to encrypt the data meant for the recipient, and a private key, which is kept secret. The private key is password-protected, and only the recipient is allowed to know it. Messages being sent to a recipient are encrypted using the recipient's public key. Once that has happened, the information can only be decrypted with the aid of the recipient's private key. This is also referred to as an asymmetric method, because the sender and the recipient use two different keys.

mail (from the Rohde & Schwarz communications partner) or (if the key material has already been generated for the e-mail address in question) by querying it on the Rohde & Schwarz Secure E-Mail web interface.

E-mails containing content that is not considered to be business-critical can be exchanged without encryption.

3 Possibilities for encrypted transmission

In the future, there will be three different possibilities available to you to enable the secure exchange of e-mails with Rohde & Schwarz. These will be described briefly in the sections below.

3.1 Variant 1: encryption using S/MIME or PGP

For the first variant, you need to have an S/MIME certificate or a PGP key on your e-mail client. Depending on the e-mail client you use, you might also need additional software for encryption/decryption. Microsoft Outlook, for example, supports S/MIME; however, it requires an additional plug-in for PGP. With this variant, you can read confidential e-mails, or write to your Rohde & Schwarz communications partner, directly in your e-mail client without having to use the web interface (see section 7).

If you do not have such keying material, we recommend that you have a public certification authority issue you an S/MIME certificate or that you generate a PGP key. Keys or certificates are always issued for a specific e-mail address for a specific person. Doing that also enables encrypted e-mail communications with any other communications partner who employs such a system.

3.2 Variant 2: communications via TLS/SMTPS

For this variant, your e-mail server must be able to receive and send its e-mail messages via either STARTTLS (TCP port 25) or SMTPS (TCP port 465). Detailed technical information on this can be found in section 6.

3.3 Variant 3: web mail with SSL encryption

To use the web-mail system, you need Internet access and a current browser. Operating this system is comparable to using the systems employed by web-mail service providers such as GMX or web.de. You will find detailed information on this in section 7.

4 Making initial contact

When you initiate the communications

If you want to take the first step in communicating securely with Rohde & Schwarz by e-mail, you can call up the relevant key material on the Rohde & Schwarz Secure E-Mail web interface (see section 9) or request it from your contact at Rohde & Schwarz. You will find a detailed description for doing this in sections 5 and 6.

When Rohde & Schwarz initiates the communications

If Rohde & Schwarz wants to initiate secure communications with you by e-mail for the first time but does not have any trustworthy key material for you, you will receive an automatic, signed registration e-mail (see Fig. 1) for the Rohde & Schwarz Secure E-Mail web interface. Initially, Rohde & Schwarz will hold back the actual e-mail itself that is being sent to you. To ensure that the e-mail is not overlooked and that it does not land in the recycle bin, below you will find two pieces of relevant information regarding the registration e-mail:

- Subject: "*Register to Receive an Encrypted Email*"

- From: The e-mail address of your communications partner at Rohde & Schwarz
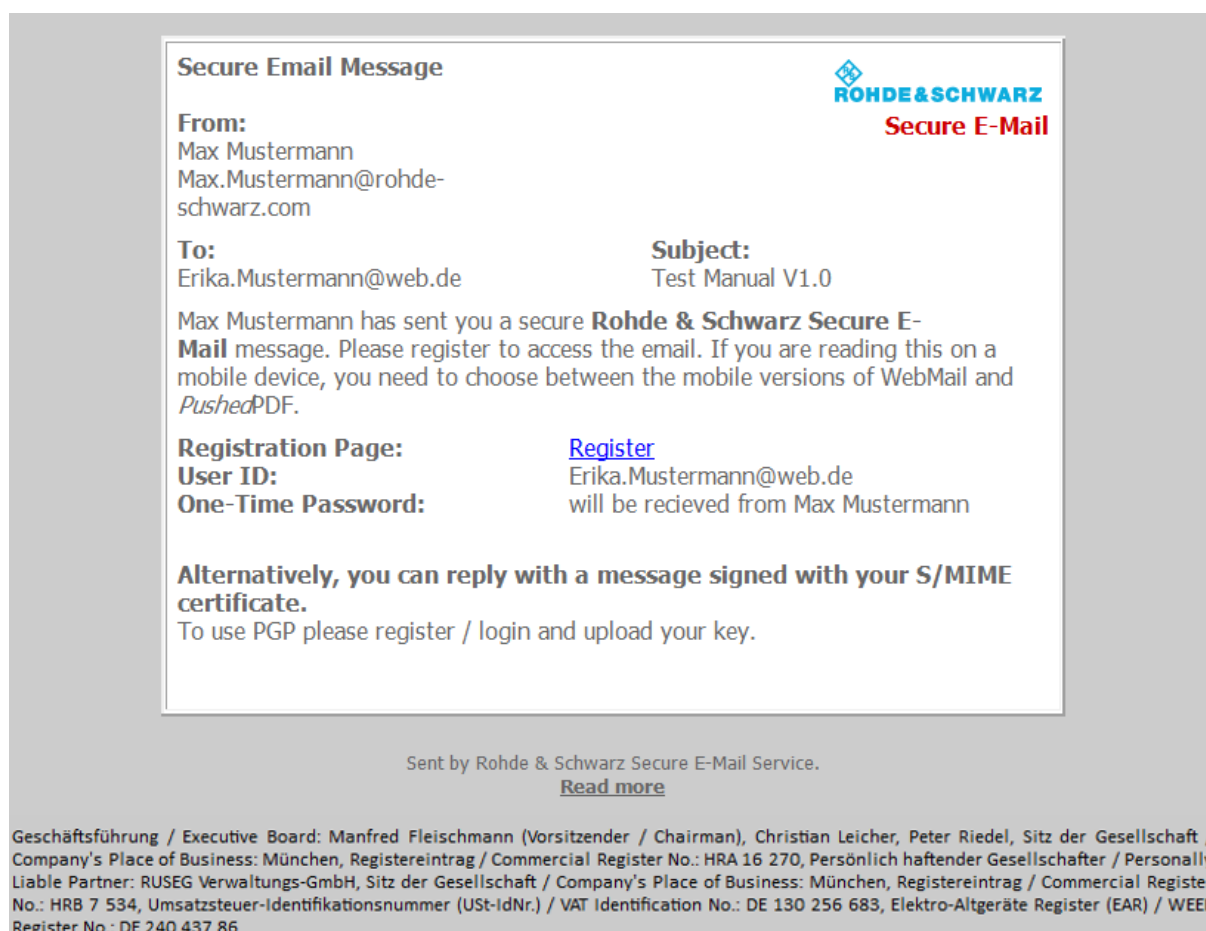

Fig. 1: Registration e-mail for Rohde & Schwarz Secure E-Mail.

You will receive the initial ("one-time") password mentioned in the registration e-mail from your communications partner at Rohde & Schwarz. For that task, a different communications channel (such as a telephone call or a letter) is used – for your protection – instead of e-mail. You need the initial password to register on the Rohde & Schwarz Secure E-Mail web interface and read your confidential e-mail there.

This registration e-mail is signed with a key that has been issued by the Quovadis certification authority that Rohde & Schwarz uses.

If you are already able to send encrypted e-mails via S/MIME, you can respond to the registration e-mail with a signed e-mail message. The Rohde & Schwarz encryption gateway extracts your public key from the signed message, validates it, and sends you the confidential information in encrypted form by e-mail. If PGP is used, please register on the Rohde & Schwarz Secure E-Mail web interface and upload your public PGP key (see section 8).

5 Variant 1: encryption using S/MIME or PGP

If you use an S/MIME certificate or PGP key for e-mail encryption, you will always receive the e-mails directly in your personal e-mail program (such as Mozilla Thunderbird or Microsoft Outlook). In this case, the encryption/decryption of the messages takes place automatically between your e-mail program and the Rohde & Schwarz encryption gateway.

To be able to use this variant, you must have an electronic certificate issued by a third party or have a PGP key. To set things up, please respond to the registration e-mail and sign this response with your S/MIME certificate. That enables the exchange of the public keys for both communications partners. The Rohde & Schwarz encryption gateway verifies your signature and your public key. If they are valid, the confidential message is sent to you immediately in the form of an S/MIME encrypted message.

If your S/MIME certificate is from a "private" public-key infrastructure (PKI), Rohde & Schwarz will perform an additional check on the key material prior to activation. Such a check is always performed when PGP keys are used.

In such cases, you have the opportunity to upload your certificate/key yourself in the Rohde & Schwarz Secure E-Mail web interface under the menu item `Preferences – Certificates` (see section 8).

You can call up Rohde & Schwarz keys (S/MIME or PGP) for specific people under the following URL: https://securemail.rohde-schwarz.com

5.1 Using domain certificates

If you use an e-mail encryption gateway, you can also encrypt the messages on the basis of S/MIME domain certificates or PGP domain keys. To do so, please send us your corresponding domain key (S/MIME or PGP). You will find information about the domain keys (S/MIME and PGP) for Rohde & Schwarz GmbH & Co. KG in the next two sections, 5.1.1 and 5.1.2.

5.1.1 S/MIME domain certificate

Please ask your Rohde & Schwarz representative for the domain certificate.

This key is issued by

```
CN  =  QuoVadis Swiss Advanced CA G2
O   =  QuoVadis Trustlink Switzerland Ltd.
C   =  CH
```

in this name:

```
E   =  secureemailgw-admin-mu@rohde-schwarz.com

CN  =  S/MIME DOMAIN CERTIFICATE

OU  =  Secure E-Mail

O   =  Rohde & Schwarz GmbH & Co. KG

C   =  DE
```

The public key has this SHA-1 fingerprint:

58 8a 30 8a 3d 3b 2d 43 8b 7b 6c c4 07 99 65 2b ee 4c b9 ad

5.1.2 PGP domain key

Please ask your Rohde & Schwarz representative for the domain key.

The PGP domain key bears the name: "Secure E-Mail Gateway PGP domain key (Rohde & Schwarz) <SecureEmailGW-Admin-MU@rohde-schwarz.com>" and is signed with the PGP CA key for the Rohde & Schwarz Secure E-Mail Gateways (Rohde-Schwarz-SecureEMailGW-CA (rohde-schwarz.com) <secureemailgw-admin-mu@rohde-schwarz.com>).

The fingerprint for the PGP domain key is:

ECEB FF22 B8AE 8A08 A61A 71DA 6E8C A68D 66C4 36A7

6 Variant 2: communications via TLS/SMTPS

If you would like to have encryption of the e-mails on the transport layer between your e-mail domains and the Rohde & Schwarz e-mail domains, this is the right variant to select.

Your e-mail gateway must be able to send and receive e-mails using STARTTLS or SMTPS. The TLS/SMTPS encryption is performed between your e-mail gateway and the Rohde & Schwarz TLS mail gateway on the application layer (transport encryption).

Since Rohde & Schwarz uses its own e-mail systems for this on its end, e-mails to the Rohde & Schwarz domains must be sent on your system to dedicated Rohde & Schwarz mail servers, and not to the MX record[3] present in the DNS. The server is: securemail.rohde-schwarz.com (IP: 80.246.41.42)

If necessary, it is also possible for the e-mails being sent to your domains from the Rohde & Schwarz end to also be sent to dedicated mail systems.

For secured communications via TLS/SMTPS, we expect the following framework conditions:

- With STARTTLS, the communications take place via TCP port 25. Here, it must be ensured that both ends allow only TLS encryption.

- With SMTPS, the secure communications take place via TCP port 465.

- The SSL certificates that are used for the TLS protocol must have been issued by a public certification authority.

- No user-signed keys will be accepted.

- The keys must be at least 2048 bits long.

- The RC4 encryption algorithm is not supported.

- Session keys must be at least 128 bits long.

- The common names (CN) of the certificates that are used must correspond to the host names for the corresponding e-mail gateways.

- The mail server must be operated in your network and must not be hosted externally.

---

[3] Wikipedia (translated from the German version): A domain's mail exchange (MX) record is an entry in the Domain Name System that refers exclusively to the SMTP service. This entry specifies the Fully Qualified Domain Name (FQDN) at which the mail server for a domain or a subdomain can be reached.

The Rohde & Schwarz TLS key has been issued to:

```
CN                            =  securemail.rohde-schwarz.com
OU                            =  IT Department
SERIALNUMBER                  =  HRA 16270
2.5.4.15                      =  Private Organization
L                             =  Muenchen
S                             =  Bayern
C                             =  DE
O                             =  Rohde & Schwarz GmbH & Co. KG
1.3.6.1.4.1.311.60.2.1.1      =  Muenchen
OID.1.3.6.1.4.1.311.60.2.1.2  =  Bayern
1.3.6.1.4.1.311.60.2.1.3      =  DE
```

and has been signed by the following authority:

```
CN  =  thawte Extended Validation SHA256 SSL CA
O   =  Thawte, Inc.
C   =  US
```

The associated fingerprint is:

39 1e 63 ca 99 a0 a1 93 04 26 03 08 bf fc 0b fa 2c 87 7b db

Rohde & Schwarz currently supports the following cipher suites for TLS/SMTPS:

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
```

Rohde & Schwarz reserves the right to make adaptations to this list. For this reason, your system should support several of the above-listed suites to ensure compatibility. Doing that ensures that encrypted communications between you and Rohde & Schwarz continue to work if changes are made to the variants that are available.

This variant requires coordination between the IT personnel that operate your mail server and the IT personnel at Rohde & Schwarz. To make that possible, please get in touch with your contact at Rohde & Schwarz.

7 Variant 3: Rohde & Schwarz Secure E-Mail web interface (SSL)

If you do not have the capabilities to transmit confidential messages using S/MIME, PGP or TLS encryption, you can use the Rohde & Schwarz Secure E-Mail web interface.
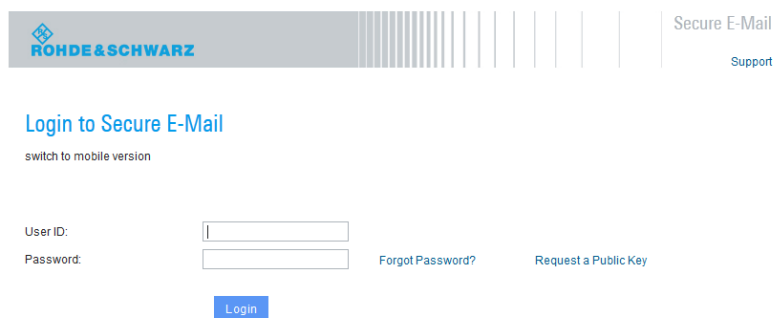
The registration password that you receive from your Rohde & Schwarz contact only works for your initial login to our system. For this reason, the first time that you log in, you must change this one-time password to a password of your choice. The new password must adhere to these guidelines:

- At least 9 characters, but no more than 20 characters

- At least one uppercase letter, one lowercase letter and one number

The password must be changed every 90 days. The e-mails remain stored in the Rohde & Schwarz Secure E-Mail system for a period of 90 days. During this period, you can access the e-mails at any time via a browser using your user ID (your e-mail address) and password. When a new e-mail arrives in your Rohde & Schwarz Secure E-Mail mailbox, you are notified with a message.

7.1 Registering on the Rohde & Schwarz Secure E-Mail web interface

Using your browser, open the page https://securemail.rohde-schwarz.com; the following registration window will appear (Fig. 2):

Fig. 2: Rohde & Schwarz Secure E-Mail web interface – login mask.

Enter your user ID (your e-mail address) in the "User ID" field. In the password field, enter your initial (one-time) password (from then on, always use the personal password that you have chosen). After you have entered and confirmed this information, you receive the following message (see Fig. 3), which prompts you to proceed.

Fig. 3: Rohde & Schwarz Secure E-Mail web interface – welcome message.

7.2 Entering the user information

In the next step, enter your name and your new password (see Fig. 4).

Fig. 4: Rohde & Schwarz Secure E-Mail – defining the user ID/password.

7.3 Defining the security questions / responses

Now you are prompted to select and answer three security questions (two predefined and one user-defined). You will need the responses to these security questions if you forget your password. In order to ensure that your account is not misused, you must comply with the rules shown in Fig. 5.

Fig. 5: Rohde & Schwarz Secure E-Mail – defining security questions.

7.4 Login

Once you have successfully registered, you are led to the login window (Fig. 6). At this point, you must log in using your e-mail address and the password that you just established.

Fig. 6: Rohde & Schwarz Secure E-Mail – login mask.

7.5 Your Rohde & Schwarz Secure E-Mail mailbox

In the next step (Fig. 7), you will see an overview page for your mailbox.
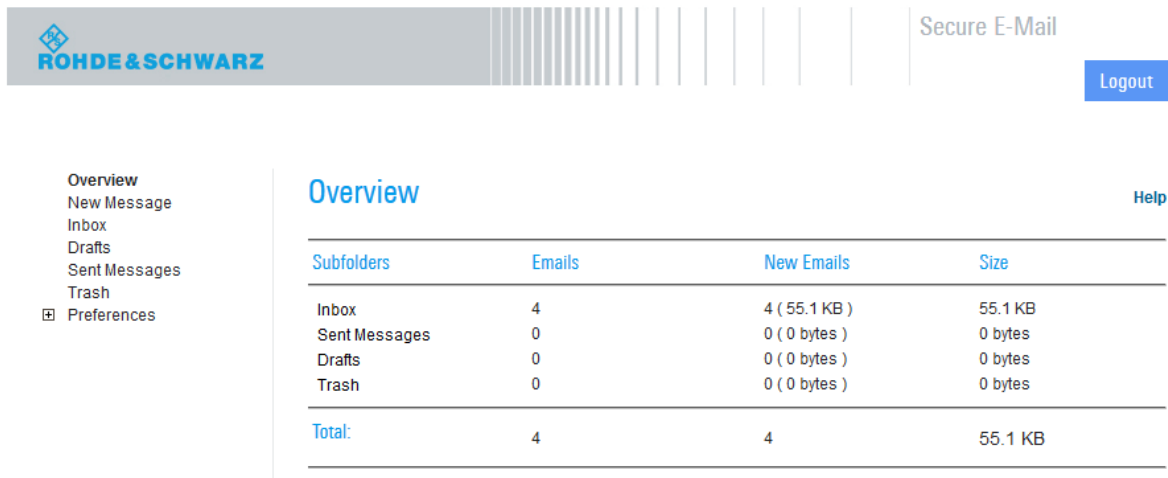

Fig. 7: Rohde & Schwarz Secure E-Mail – mailbox overview page.

7.6 Your Rohde & Schwarz Secure E-Mail inbox

The messages that the system has stored for you are listed in chronological order in your inbox (Fig. 8). By clicking on the subject line or on the envelope icon, you can open the corresponding message. Messages that have not been read are indicated by a closed envelope.
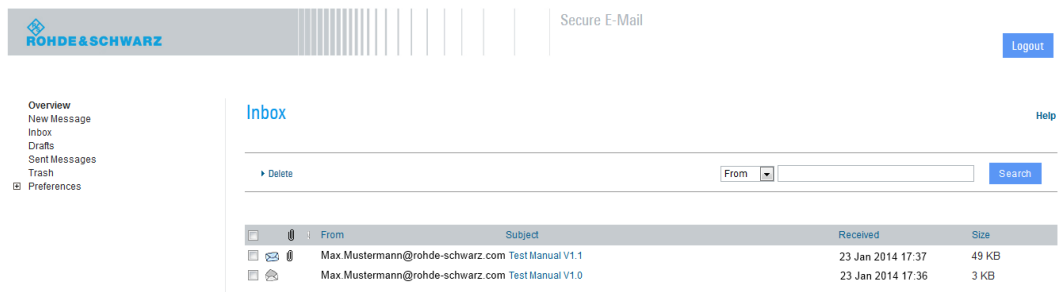

Fig. 8: Rohde & Schwarz Secure E-Mail – inbox.

When an e-mail contains an attachment, this is indicated by a paper clip shown next to the sender's name. You can download any file attachments onto your computer. In addition, you have the option to store the e-mail as an *.html or *.pdf file on your hard drive (see Fig. 9). It is also possible to export the e-mails as an *.eml file so that you can import the e-mails into your e-mail program (such as Mozilla Thunderbird or Microsoft Outlook).
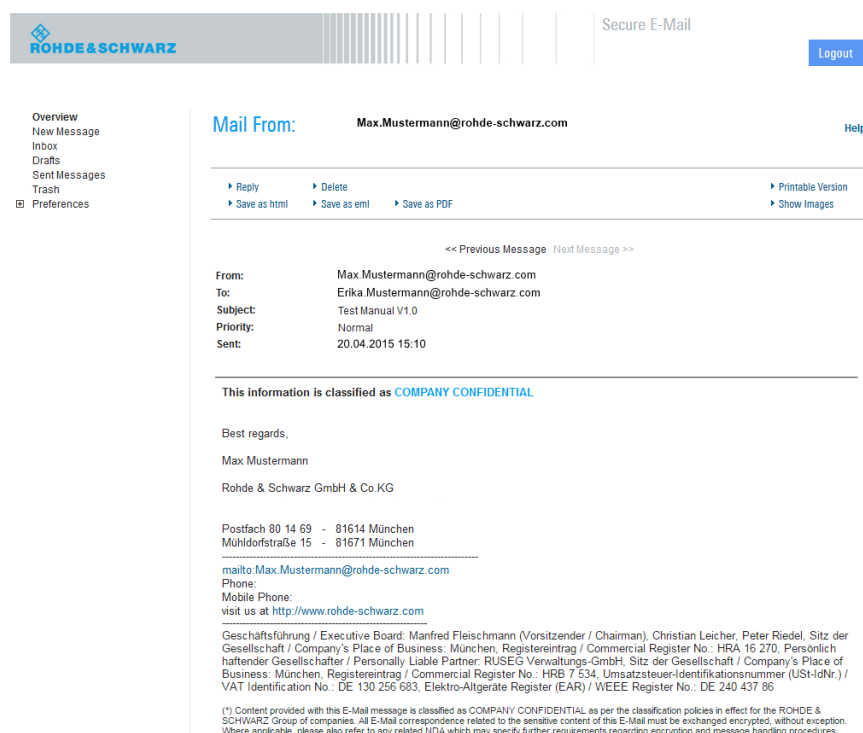
Fig. 9: Rohde & Schwarz Secure E-Mail web interface – e-mail.

7.7 Responding to an e-mail

You can also use the webmail interface to send secure messages to Rohde & Schwarz (Fig. 10). This can be a response to an existing e-mail in your mailbox, or it can be a new message. You can attach files to any e-mail. The "*To*:", "*Cc*:" and "*Bcc*:" fields only accept valid Rohde & Schwarz e-mail addresses. If you want to address multiple people at Rohde & Schwarz, their addresses are to be separated by a comma ("*,*") or semicolon ("*;*"). It is not possible to send an e-mail to a non-Rohde & Schwarz address; consequently, any message containing such an address will be rejected.
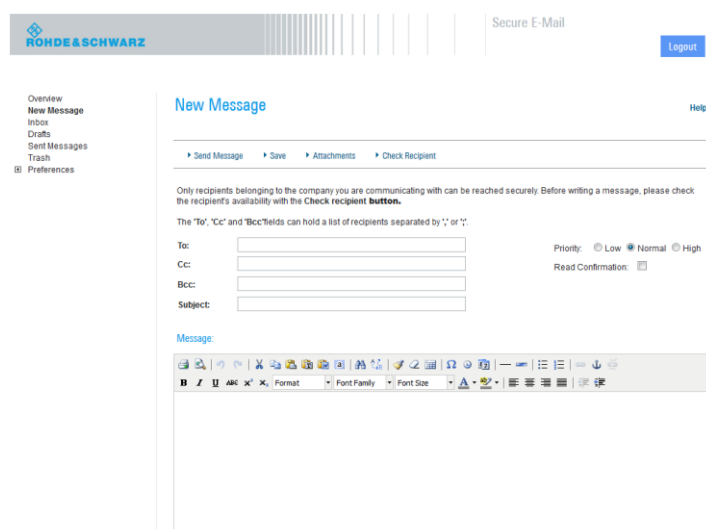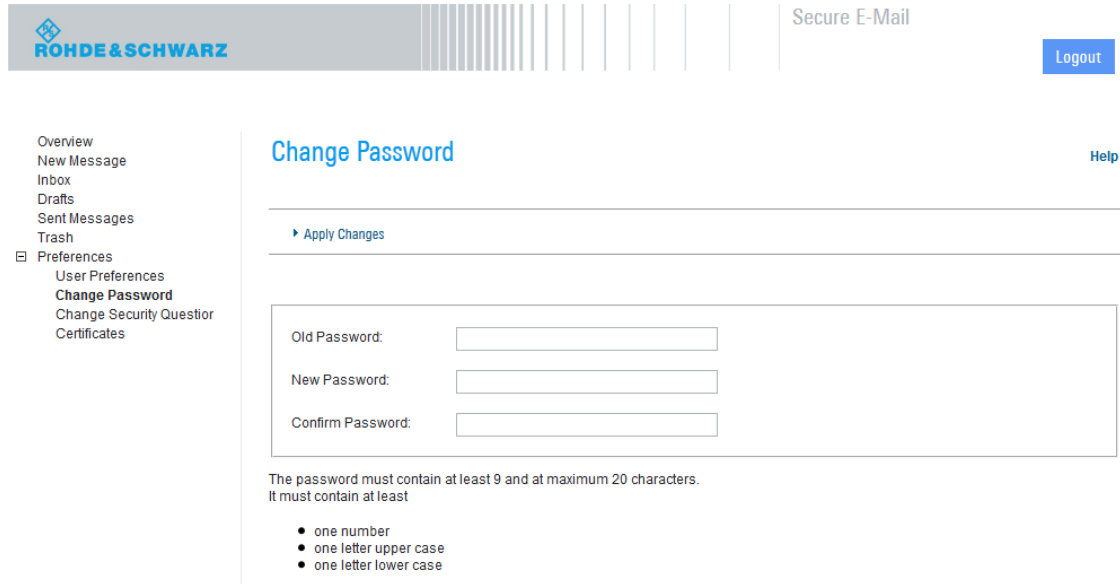

Fig. 10: Rohde & Schwarz Secure E-Mail web interface – creating a new e-mail.

7.8 Changing your password

You can change your password at any time via the `Preferences – Change Password` menu. To do so, you must first enter your old password. Then enter a new password, which must meet the requirements shown in Fig. 11.
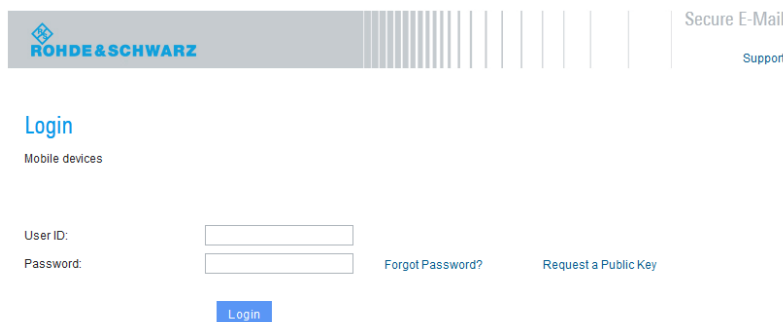
Fig. 11: Rohde & Schwarz Secure E-Mail web interface – changing your password.

7.9 Forgotten your password?

The login mask for the Rohde & Schwarz Secure E-Mail web interface (https://securemail.rohde-schwarz.com) allows you to reset your password on your own. To do so, click on "Forgot Password?" in the login mask (Fig. 12). After that, you will be prompted to enter your complete e-mail address for which the password is to be reset (Fig. 13). The dialog box that follows (Fig. 14) prompts you to answer the security questions correctly. Once you have answered all of them correctly, you can set a new password (Fig. 15). After that, you will be returned to the Rohde & Schwarz Secure E-Mail web interface.

Fig. 12: Rohde & Schwarz Secure E-Mail web interface – resetting your password, step 1.

Password reset

You can reset your forgotten password with the security questions you have chosen before. Please enter your email address.

Your Email Address

Erika.Mustermann@web.de

Next Step

Fig. 13: Rohde & Schwarz Secure E-Mail web interface – resetting your password, step 2.

Secure E-Mail
Support

Password reset for the email address: *Erika.Mustermann@web.de*

Please enter the answers of the questions you have selected before.

What is your oldest sibling's middle name?

What was your childhood nickname?

What was the last name of your third grade teacher?

If you do not know the answers anymore, please contact your communication partner.

Back   Next Step

Fig. 14: Rohde & Schwarz Secure E-Mail web interface – resetting your password, step 3.

Secure E-Mail
Support

Change Password

New Password:

Confirm Password:

Apply Changes

The password must contain at least 9 and at maximum 20 characters. It must contain at least

- one number
- one letter upper case
- one letter lower case

Fig. 15: Rohde & Schwarz Secure E-Mail web interface – resetting your password, step 4.

7.10   Administration of S/MIME certificates or PGP keys

In case you own a S/MIME certificate or a PGP key for e-mail encryption, these keys can be used form encrypted e-mail communication with Rohde & Schwarz. You are able to deposit and manage your public keys using the Rohde & Schwarz Secure E-Mail web interface.

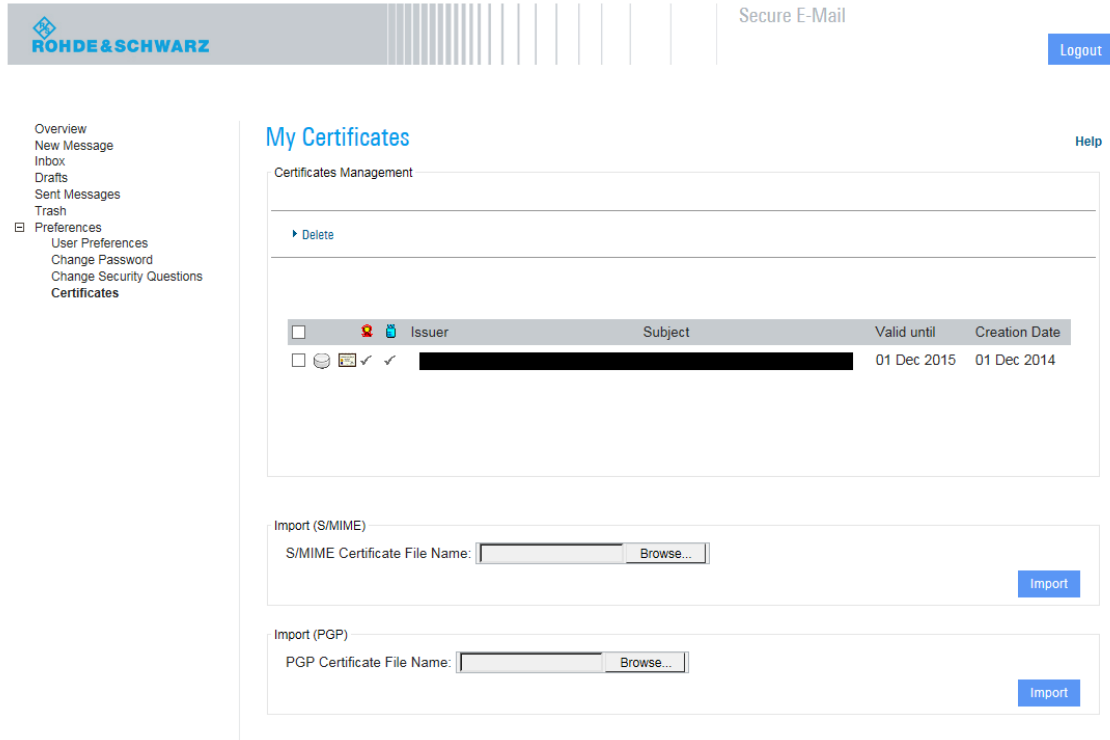You can manage your public keys at any time via the `Preferences – Certificates` menu.

Fig. 16: Rohde & Schwarz Secure E-Mail web interface – administration of S/MIME certificates and PGP keys

At this point you are able to upload your public S/MIME certificates or PGP keys using the import function. Likewise you can remove outdated or invalid keys using the "delete" button at the top of the frame.

7.11 Mobile login

The Rohde & Schwarz Secure E-Mail web interface is also available in a slimmed-down form to enable access via a mobile device (see Fig. 17 and Fig. 18). You can access this version via the "*Mobile Devices*" link (https://securemail.rohde-schwarz.com/mobileLogin.jsp). There, the following functions are available to you:

- Read/write/respond to messages

- Delete messages

- Change password

Fig. 17: Rohde & Schwarz Secure E-Mail web interface – mobile login.

Fig. 18: Rohde & Schwarz Secure E-Mail web interface – mobile inbox.

8 Changing the variant

You can change the delivery method that you use at any time via the Rohde & Schwarz Secure E-Mail web interface (see Fig. 19). To do so, log in to the Rohde & Schwarz Secure E-Mail web interface and select the `Preferences - User Preferences` menu item. There, you can set the variant that you want to use under `Security Type`.

Fig. 19: Rohde & Schwarz Secure E-Mail web interface – changing the delivery method.

If you make a change – for example by switching from webmail to S/MIME – the relevant key material must also be available. When this is required, this material must be uploaded onto the Rohde & Schwarz Secure E-Mail web interface in advance under the `Preferences - Certificates` menu item (see Fig.20).
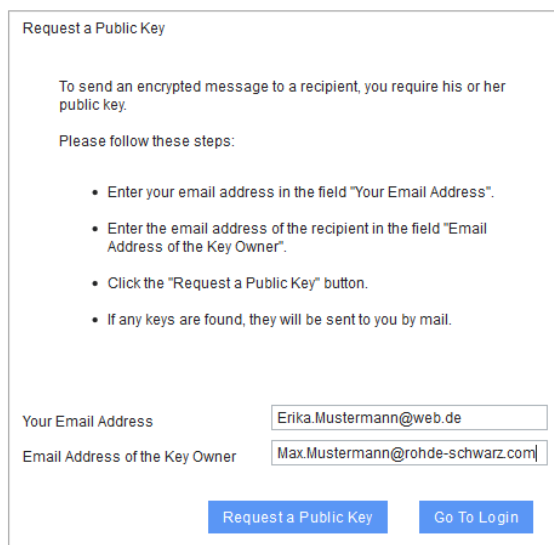
Fig.20: Rohde & Schwarz Secure E-Mail web interface – uploading a certificate.

9 Requesting public keys

If you use your own S/MIME or PGP encryption, you need the public key that your communications partner at Rohde & Schwarz uses. This key enables you to establish encrypted communications. You can request the public key from Rohde & Schwarz via the following link:

HTTPS URL: https://securemail.rohde-schwarz.com

The procedure for requesting a public key is described in the example provided in Fig. 21 below. The S/MIME certificate and the PGP key that you have requested for your Rohde & Schwarz communications partner is then sent to you by e-mail (see Fig. 22).

Fig. 21: Rohde & Schwarz Secure E-Mail web interface – requesting a public key.
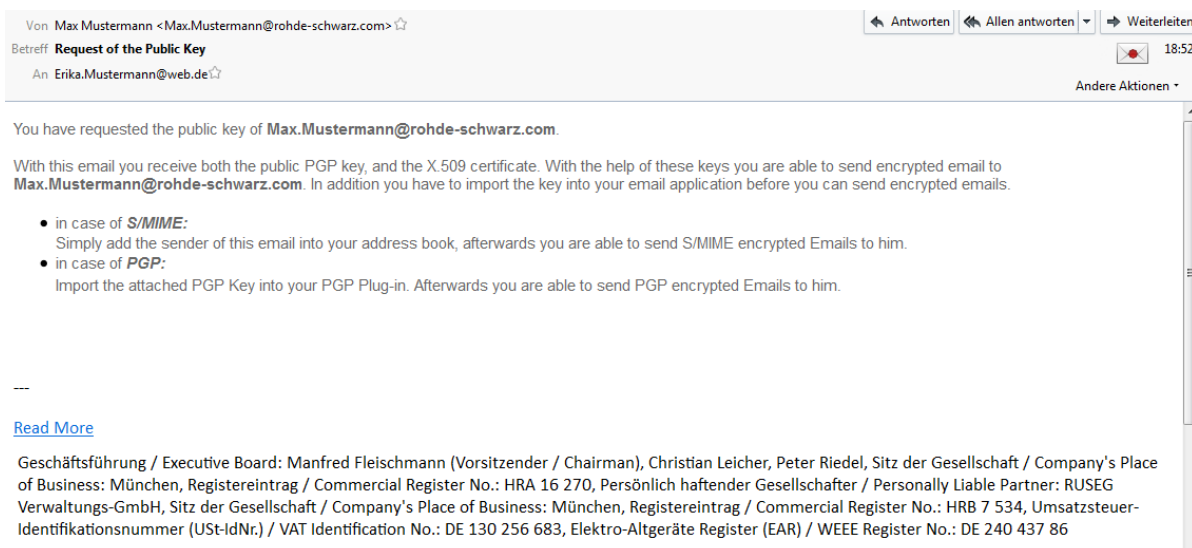
Fig. 22: Rohde & Schwarz Secure E-Mail web interface – public key e-mail.

10 Notes

Please note the following information:

Rohde & Schwarz Secure E-Mail web interface:

- The Rohde & Schwarz Secure E-Mail web interface mailbox is not a permanent archive. Please store your messages and their attachments on your own computer. Old e-mails will be deleted from your mailbox after 90 days. Accounts are deleted regularly after 180 days of inactivity.

- The maximum storage capacity for your Rohde & Schwarz Secure E-Mail web interface account is 50 Mbyte.

S/MIME / PGP:

- You can call up the public keys for Rohde & Schwarz employees via https://securemail.rohde-schwarz.com.

- Encryption based on domain keys using PGP or S/MIME is possible.

TLS/SMTPS:

- The communications for TLS/SMTPS are not accomplished using an MX record when exchanging e-mails with Rohde & Schwarz; instead, the dedicated mail system securemail.rohde-schwarz.com (IP: 80.246.41.42) is used.

- With STARTTLS, the communications take place via TCP port 25. Here, it must be ensured that both ends allow only TLS encryption.

- With SMTPS, the secure communications take place via TCP port 465.

- The SSL certificates that are used for the TLS protocol must have been issued by a public certification authority.

- No user-signed keys will be accepted.

- The keys must be at least 2048 bits long.

- The RC4 encryption algorithm is not supported.

- Session keys must be at least 128 bits long.

- The common names (CN) of the certificates that are used must correspond to the host names for the corresponding e-mail gateways.

- The mail server must be operated in your network and must not be hosted externally.

11 FAQ

Q01:   I can't find the registration e-mail.

A01:   Please also check your "unknown" or "spam" directory.

Q02:   What is my user ID?

A02:   Your personal e-mail address serves as your user ID.

Q03:   What are the requirements for defining a password?

A03:   The password must be at least 9 but no more than 20 characters long. It must contain at least one uppercase letter, one lowercase letter and one number.

Q04:   I want to log in to my Rohde & Schwarz Secure E-Mail mailbox, but I no longer have the e-mail containing the link.

A04:   You can reach the login page at https://securemail.rohde-schwarz.com. There you can log in using your e-mail address and the password that you defined during registration.

Q05:   What are the security questions for?

A05:   If you ever forget your password, you can reset it yourself in the self-service portal by correctly answering the security questions.

Q06:   What happens if I don't answer the security questions correctly?

A06:   Your account will be blocked. In this case, please get in touch with your contact person at Rohde & Schwarz, who will contact the IT staff member responsible for this. You will then receive a new registration password. Using that password, you can reregister.

Q07:   Where can I see who sent the e-mail?

A07:   The sender always appears in the text of the registration e-mail or in any of the messages generated by the Rohde & Schwarz encryption gateway.

Q08:   Is it also possible to respond to e-mails from the mailbox?

A08:   Yes, you can respond to e-mails in the Rohde & Schwarz Secure E-Mail mailbox. You can also create a new message there for Rohde & Schwarz employees in order to send them information via a secure channel.

Q09:   Is it also possible to send attachments via the Rohde & Schwarz Secure E-Mail web interface?

A09:   Yes, you can also attach files to your e-mails in the Rohde & Schwarz Secure E-Mail web interface in the same way as with conventional e-mail programs.

Q10:   How long is the mailbox valid?

A10:   Your account will be deleted after 180 days of inactivity. You will be notified if that occurs. For this reason, please store your messages and your attachments on your own computer. Rohde & Schwarz does not archive this data.

Q11:   How long is a password valid?

A11:   With the exception of the initial password, the password needs to be changed every 90 days. The new password cannot be the same as the old password.

Q12:   What subject line and sender name are used for the registration e-mail for the Rohde & Schwarz Secure E-Mail web interface?

A12:   Subject: "*Register to Receive an Encrypted Email*"
             From: Your Rohde & Schwarz communications partner

Q13:   What should I do if I am not able to call up the e-mail in the Rohde & Schwarz Secure E-Mail web interface?

A13:   Please ensure that you have already successfully registered for the Rohde & Schwarz Secure E-Mail web interface. If this is not the case, please first get in touch with your Rohde & Schwarz contact person, who will contact the IT staff member responsible. You will then receive a new registration password. Using that password, you can reregister.

Q14:   How can I, as an external communications partner, exchange key material with Rohde & Schwarz without having to constantly go through the mailbox?

A14:   If you want to make your S/MIME certificate available to us, send us a signed e-mail. If you use PGP, you can upload your certificate via the Rohde & Schwarz Secure E-Mail web interface. You can also use that option for your S/MIME certificate. If you want to obtain key material from Rohde & Schwarz, you can do so via the Rohde & Schwarz Secure E-Mail web interface (https://securemail.rohde-schwarz.com/).

Q15:   Can I send a copy (using cc) to a person who is not from Rohde & Schwarz when responding to a message via the Rohde & Schwarz Secure E-Mail web interface?

A15:   No, that is not possible, because the Rohde & Schwarz Secure E-Mail web interface is only to be used for the purpose of secure communications between you and Rohde & Schwarz.

12 Do you have any further questions?

If you have questions, please get in touch with your Rohde & Schwarz contact.

Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, radiomonitoring and radiolocation. Founded more than 80 years ago, this independent company has an extensive sales and service network and is present in more than 70 countries.

The electronics group is among the world market leaders in its established business fields. The company is headquartered in Munich, Germany. It also has regional headquarters in Singapore and Columbia, Maryland, USA, to manage its operations in these regions.

Regional contact

Europe, Africa, Middle East
+49 89 4129 12345
customersupport@rohde-schwarz.com

North America
1 888 TEST RSA (1 888 837 87 72)
customer.support@rsa.rohde-schwarz.com

Latin America
+1 410 910 79 88
customersupport.la@rohde-schwarz.com

Asia Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

China
+86 800 810 82 28 |+86 400 650 58 96
customersupport.china@rohde-schwarz.com

Sustainable product design

▪ Environmental compatibility and eco-footprint

▪ Energy efficiency and low emissions

▪ Longevity and optimized total cost of ownership

Certified Quality Management
ISO 9001

Certified Environmental Management
ISO 14001