

# E-Mails versenden – aber sicher!

## Sichere E-Mail Kommunikation bei Rohde & Schwarz

**Leitfaden V1.1.10**

Dieses Dokument ist nur in der jeweils aktuellsten Fassung gültig.



**ROHDE & SCHWARZ**

# Inhalt

I	Abbildungsverzeichnis .....	2
1	Vorwort .....	3
2	Schutzziele und Maßnahmen .....	4
2.1	<b>Authentizität</b> .....	4
2.2	<b>Integrität</b> .....	4
2.3	<b>Vertraulichkeit</b> .....	5
3	Möglichkeiten zur gesicherten Übertragung .....	7
3.1	<b>Variante 1: Verschlüsselung mittels S/MIME oder PGP</b> .....	7
3.2	<b>Variante 2: Kommunikation über TLS / SMTPS</b> .....	7
3.3	<b>Variante 3: Web-Mail mit SSL-Verschlüsselung</b> .....	7
4	Dieerste Kontaktaufnahme .....	8
5	Variante 1: Verschlüsselung mittels S/MIME oder PGP.....	10
5.1	<b>Einsatz von Domainzertifikaten</b> .....	10
5.1.1	<b>S/MIME Domainzertifikat</b> .....	10
5.1.2	<b>PGP Domainschlüssel</b> .....	11
6	Variante 2: Kommunikation über TLS/ SMTPS .....	11
7	Variante 3: Rohde & Schwarz Secure E-Mail Webinterface (SSL).....	15
7.1	<b>Anmeldung am Rohde &amp; Schwarz Secure E-Mail Webinterface</b> .....	15
7.2	<b>Eingabe der Benutzer-Informationen</b> .....	16
7.3	<b>Definieren der Sicherheitsfragen / -antworten</b> .....	17
7.4	<b>Login</b> .....	17
7.5	<b>Ihr Rohde &amp; Schwarz Secure E-Mail Postfach</b> .....	18
7.6	<b>Ihr Rohde &amp; Schwarz Secure E-Mail Posteingang</b> .....	18
7.7	<b>Antworten</b> .....	19
7.8	<b>Passwortänderung</b> .....	20
7.9	<b>Sie haben Ihr Passwort vergessen?</b> .....	20
7.10	<b>Administration von S/MIME Zertifikaten oder PGP Schlüsseln</b> .....	22
7.11	<b>Mobile Login</b> .....	23
8	Änderung der Variante .....	24
9	Anforderung öffentlicher Schlüssel .....	25
10	Hinweise .....	26
11	FAQ .....	27
12	Haben Sie weitere Fragen? .....	29

# I Abbildungsverzeichnis

Abbildung 1: Rohde & Schwarz Secure E-Mail - Registrierungsemail.....	8
Abbildung 3: Rohde & Schwarz Secure E-Mail Webinterface - Login.....	15
Abbildung 4: Rohde & Schwarz Secure E-Mail Webinterface - Begrüßung .....	16
Abbildung 5: Rohde & Schwarz Secure E-Mail - Username / Passwort setzen .....	16
Abbildung 6: Rohde & Schwarz Secure E-Mail – Sicherheitsfragen definieren.....	17
Abbildung 7: Rohde & Schwarz Secure E-Mail - Login Maske .....	17
Abbildung 8: Rohde & Schwarz Secure E-Mail - Postfach Übersicht .....	18
Abbildung 9: Rohde & Schwarz Secure E-Mail - Posteingang.....	18
Abbildung 10: Rohde & Schwarz Secure E-Mail Webinterface – E-Mail .....	19
Abbildung 11: Rohde & Schwarz Secure E-Mail Webinterface - Neue E-Mail erstellen.....	19
Abbildung 12: Rohde & Schwarz Secure E-Mail Webinterface - Passwort ändern .....	20
Abbildung 13: Rohde & Schwarz Secure E-Mail Webinterface - Passwort zurücksetzen 1 .....	20
Abbildung 14: Rohde & Schwarz Secure E-Mail Webinterface - Passwort zurücksetzen 2 .....	21
Abbildung 15: Rohde & Schwarz Secure E-Mail Webinterface - Passwort zurücksetzen 3 .....	21
Abbildung 16: Rohde & Schwarz Secure E-Mail Webinterface - Passwort zurücksetzen 4 .....	21
Abbildung 17: Rohde & Schwarz Secure E-Mail Web Interface – Administration von S/MIME Zertifikaten und PGP Schlüsseln.....	22
Abbildung 18: Rohde & Schwarz Secure E-Mail Webinterface - Mobile Login .....	23
Abbildung 19: Rohde & Schwarz Secure E-Mail Webinterface - Mobile Posteingang.....	23
Abbildung 20: Rohde & Schwarz Secure E-Mail Webinterface - Ändern der Zustellmethode.....	24
Abbildung 21: Rohde & Schwarz Secure E-Mail Webinterface - Zertifikat Upload .....	24
Abbildung 22: Rohde & Schwarz Secure E-Mail Webinterface - Public Key anfordern.....	25
Abbildung 23: Rohde & Schwarz Secure E-Mail Webinterface - Public Key E-Mail .....	25

# 1 Vorwort

E-Mails sind aus dem Alltag nicht mehr wegzudenken. Dieses Medium wird seit vielen Jahren als schnelle und unkomplizierte Form der Kommunikation genutzt. Was in der privaten Welt von den meisten Menschen als unkritisch erachtet wird, ist bei der geschäftlichen Kommunikation jedoch mit etlichen Risiken verbunden. Das Kommunikationsmittel E-Mail birgt dabei Gefahren wie das Abhören einer E-Mail, das Vortäuschen einer E-Mail Identität, Phishing oder auch SPAM. Diese sind für den Anwender auf den ersten Blick oftmals nicht zu erkennen. So ist es Dritten möglich ungesicherte Nachrichten auf dem Übertragungsweg zu lesen oder zu fälschen. Des Weiteren besteht die Möglichkeit, dass Mails fehlgeleitet oder nachgeahmt werden, ohne dass Absender oder Empfänger davon Kenntnis erlangen. Dies kann nicht kalkulierbaren Folgen für beide Seiten haben.

## 2 Schutzziele und Maßnahmen

Um den im Vorwort beschriebenen Risiken besser zu begegnen, werden die im folgenden beschriebenen Schutzziele zukünftig durch Rohde & Schwarz mit erweiterten technischen Schutzmaßnahmen adressiert.

### 2.1 Authentizität

#### **Schwachstellen:**

In Ihrem E-Mail Programm wird Ihnen eine Absenderadresse angezeigt, die jedoch mit geringem technischem Aufwand sehr leicht zu fälschen ist. Das Medium E-Mail ist ohne ergänzende technische Maßnahmen prinzipiell nicht zur verlässlichen Prüfung der Authentizität des Absenders geeignet und ermöglicht ohne großen Aufwand durch Fälschung der Absenderadresse die Verschleierung der echten Absenderadresse oder den gezielten Identitätsdiebstahl.

#### **Bedrohungen:**

Identitätsdiebstahl findet häufig in Verbindung mit Phishing-Angriffen (oft auch gekoppelt mit Social Engineering Angriffen) statt, während die allgemeine Verschleierung der echten Absenderadresse zum Versand von Spam-Mails genutzt wird.

#### **Maßnahmen:**

Durch Anbringen einer digitalen Signatur kann empfängerseitig verifiziert werden, dass die Nachricht aus der Organisation Rohde & Schwarz gesendet und dort mit einem - einer bestimmten E-Mail-Adresse zugeordneten - Schlüssel digital signiert wurde. Die im Außenverhältnis sichtbare Signatur einer E-Mail erfolgt bei Rohde & Schwarz bis auf wenige Ausnahmen an einer zentralen Stelle. Es handelt sich hierbei nicht um eine qualifizierte oder erweiterte Signatur gemäß den Vorgaben des deutschen Signaturgesetzes (SigG), da dies zur Erreichung der vorrangigen Schutzziele (Integrität & Vertraulichkeit) nicht erforderlich ist.

### 2.2 Integrität

#### **Schwachstellen:**

Mit vergleichsweise geringem Aufwand kann der Inhalt von ungeschützten E-Mails auf dem Weg zwischen Sender und Empfänger verändert werden.

#### **Bedrohungen:**

In Kombination mit Identitätsdiebstahl kann dies dazu führen, dass die E-Mail authentisch aufgebaut ist, entsprechend vertrauenswürdig und verbindlich wirkt, jedoch inhaltlich gezielt manipuliert wurde um ein bestimmtes Angriffsziel zu erreichen.

#### **Maßnahmen:**

Das senderseitige Anbringen einer digitalen Signatur an eine zum externen Versand anstehende E-Mail ermöglicht es dem Empfänger, die Integrität der E-Mail-Nachricht zu überprüfen und hierdurch Manipulationen der E-Mail nach dem Verlassen des signierenden Systems verlässlich zu erkennen.

## 2.3 Vertraulichkeit

### Schwachstellen:

Das Medium E-Mail sieht keine besonderen Schutzmaßnahmen hinsichtlich Vertraulichkeit vor und kann mit dem Versand einer Postkarte verglichen werden. Diese kann auf dem Wege vom Absender zum Empfänger von jeder Stelle in der Kommunikationskette eingesehen werden.

### Bedrohungen:

Jeder Nutzer dieses Mediums sollte sich stets bewusst sein, dass das „Abhören“ des weltweiten Datenstromes gängige Praxis ist und der Datenstrom mit einfachsten Mitteln auch in kleineren Netzwerkkumgebungen mitgeschnitten werden kann. Informationen von ungeschützten E-Mail Nachrichten können daher ohne Probleme aus dem Datenverkehr extrahiert werden, ohne dass der Absender oder Empfänger davon Kenntnis erlangen kann. Unter Umständen gelangen so unternehmenskritische Informationen in die falschen Hände.

### Maßnahmen:

Durch Anbringen einer geeigneten Verschlüsselung vor dem Versand über ein nicht vertrauenswürdiges (öffentliches) Netzwerk kann sichergestellt werden, dass die Vertraulichkeit der Inhalte auf dem Transportweg - je nach gewählter Vorgehensweise und Vereinbarung zwischen den Kommunikationspartner auch am Speicherort - gewährleistet ist.

Rohde & Schwarz ermöglicht eine kryptographisch gesicherte, externe Kommunikation mit dem anerkannten und standardisierten Verfahren S/MIME<sup>1</sup> und PGP<sup>2</sup>. Ausgehende E-Mails mit unternehmenskritischen Inhalten werden zwingend verschlüsselt, sofern vertrauenswürdiges, öffentliches Schlüsselmaterial des Empfängers vorliegt. Dem Verfahren S/MIME wird hierbei gegenüber PGP bevorzugt.

Sollte bei unternehmenskritischen Informationen kein vertrauenswürdiges Schlüsselmaterial des adressierten Empfängers vorliegen, werden diese vorerst nicht zugestellt. Stattdessen werden die Informationen für eine bestimmte Zeit am Rohde & Schwarz Secure E-Mail Webinterface zur Einsicht und Abholung vorgehalten.

Der Rohde & Schwarz Absender teilt dem externen Empfänger hierzu auf einem alternativen Kommunikationskanal (out-of band, z.B. SMS oder Telefon) ein initiales Passwort mit. Über das Rohde & Schwarz Secure E-Mail Webinterface kann durch den Empfänger zudem gültiges, öffentliches S/MIME oder PGP Schlüsselmaterial an Rohde & Schwarz übermittelt werden. Bevorzugt sollte jedoch eine signierte E-Mail an einen Rohde & Schwarz Empfänger gesendet werden, aus der das Schlüsselmaterial entsprechend extrahiert und auf Vertrauenswürdigkeit geprüft wird.

---

<sup>1</sup> Wikipedia: S/MIME (Secure/Multipurpose Internet Mail Extensions) ist ein Standard für die Verschlüsselung und Signatur von MIME-gekapselter E-Mails durch ein hybrides Kryptosystem. S/MIME ist ein hierarchisches Zertifizierungsmodell, bei dem die Echtheit öffentlicher Schlüssel von einer übergeordneten Instanz bestätigt wird.

<sup>2</sup> Wikipedia: PGP (Pretty Good Privacy) ist ein von Phil Zimmermann entwickeltes Programm zur Verschlüsselung und zum Unterschreiben von Daten. PGP benutzt ein sogenanntes Public-Key-Verfahren unter Einsatz eines eindeutig zugeordneten Schlüsselpaars. Dieses besteht aus einem öffentlichen Schlüssel, mit dem jeder die Daten für den Empfänger verschlüsseln kann und einem privaten geheimen Schlüssel. Dieser ist durch ein Kennwort geschützt und darf nur dem Empfänger bekannt sein. Nachrichten an einen Empfänger werden mit seinem öffentlichen Schlüssel verschlüsselt und können ausschließlich durch den privaten Schlüssel des Empfängers entschlüsselt werden. Dies wird als asymmetrisches Verfahren bezeichnet, da Sender und Empfänger zwei unterschiedliche Schlüssel verwenden.

Um eine mittels S/MIME oder PGP verschlüsselte E-Mail an eine E-Mail-Adresse bei Rohde & Schwarz zu versenden, kann das Schlüsselmaterial des Empfängers durch Anforderung einer signierten E-Mail (vom R&S Kommunikationspartner) erfolgen oder (sofern das Schlüsselmaterial für diese E-Mail-Adresse bereits erstellt wurde) von unserem Rohde & Schwarz Secure E-Mail Webinterface abgefragt werden.

E-Mails, deren Inhalt nicht als unternehmenskritisch einzustufen ist, können unverschlüsselt ausgetauscht werden.

## 3 Möglichkeiten zur gesicherten Übertragung

Für eine sichere E-Mail Kommunikation mit Rohde & Schwarz stehen Ihnen künftig drei verschiedene Möglichkeiten zu Verfügung. Diese werden in den nachfolgenden Abschnitten kurz erläutert.

### 3.1 Variante 1: Verschlüsselung mittels S/MIME oder PGP

Für die erste Variante benötigen Sie ein S/MIME-Zertifikat oder einen PGP-Schlüssel auf Ihrem Mailclient. Abhängig von Ihrem Mailclient ist gegebenenfalls noch eine Zusatzsoftware zur Ver- und Entschlüsselung notwendig. Microsoft Outlook unterstützt beispielsweise S/MIME, benötigt jedoch für PGP ein zusätzliches Plug-In. Mit dieser Variante können Sie vertrauliche E-Mails direkt in Ihrem Mailclient lesen bzw. Ihrem Rohde & Schwarz Kommunikationspartner schreiben und müssen nicht das Webinterface (siehe Kapitel 7) verwenden.

Sollten Sie nicht im Besitz eines solchen Schlüsselmateriales sein, so empfehlen wir Ihnen, sich ein S/MIME- Zertifikat bei einer öffentlichen Zertifizierungsstelle ausstellen zu lassen oder einen PGP-Schlüssel zu generieren. Schlüssel oder Zertifikate werden immer für eine bestimmte E-Mail-Adresse einer bestimmten Person ausgestellt. Diese ermöglichen die Durchführung einer verschlüsselten E-Mail Kommunikation mit jedem anderen Kommunikationspartner, der ein solches System im Einsatz hat.

### 3.2 Variante 2: Kommunikation über TLS / SMTPS

Für diese Variante muss Ihr E-Mailserver in der Lage sein E-Mailnachrichten entweder über STARTTLS (TCP Port 25) oder per SMTPS (TCP Port 465) zu empfangen und zu versenden. Detaillierte technische Informationen hierzu finden Sie in Kapitel 6.

### 3.3 Variante 3: Web-Mail mit SSL-Verschlüsselung

Für die Nutzung des Web-Mail-Systems benötigen Sie einen Internetzugang und einen aktuellen Browser. Das System ist in der Bedienung vergleichbar mit Webmailern von Anbietern wie GMX oder web.de. Detaillierte Informationen hierzu finden Sie in Kapitel 7.

## 4 Die erste Kontaktaufnahme

### Ausgehend von Ihnen

Falls Sie initial gesichert per E-Mail mit Rohde & Schwarz kommunizieren wollen, können Sie das hierzu notwendige Schlüsselmaterial am Rohde & Schwarz Secure E-Mail Webinterface (siehe Kapitel 9) abrufen oder dieses bei Ihrem Rohde & Schwarz Ansprechpartner. Eine genaue Beschreibung finden Sie unter Kapitel 5 und 6.

### Ausgehend von Rohde & Schwarz

Sollte Rohde & Schwarz erstmalig mit Ihnen gesichert per E-Mail kommunizieren wollen und uns noch kein vertrauenswürdigen Schlüsselmaterial vorliegen, so erhalten Sie automatische eine signierte Registrierungsemail (siehe Abbildung 1) für das Rohde & Schwarz Secure E-Mail Webinterface. Die eigentliche E-Mail an Sie wird dabei von Rohde & Schwarz vorerst zurückgehalten. Damit diese nicht übersehen wird oder im Papierkorb landet, finden Sie nachfolgend zwei relevante Informationen zur Registrierungsemail:

- Subject / Titel: *“Register to Receive an Encrypted Email”*
- From / Sender: Die E-Mail Adresse Ihres Rohde & Schwarz Kommunikationspartners

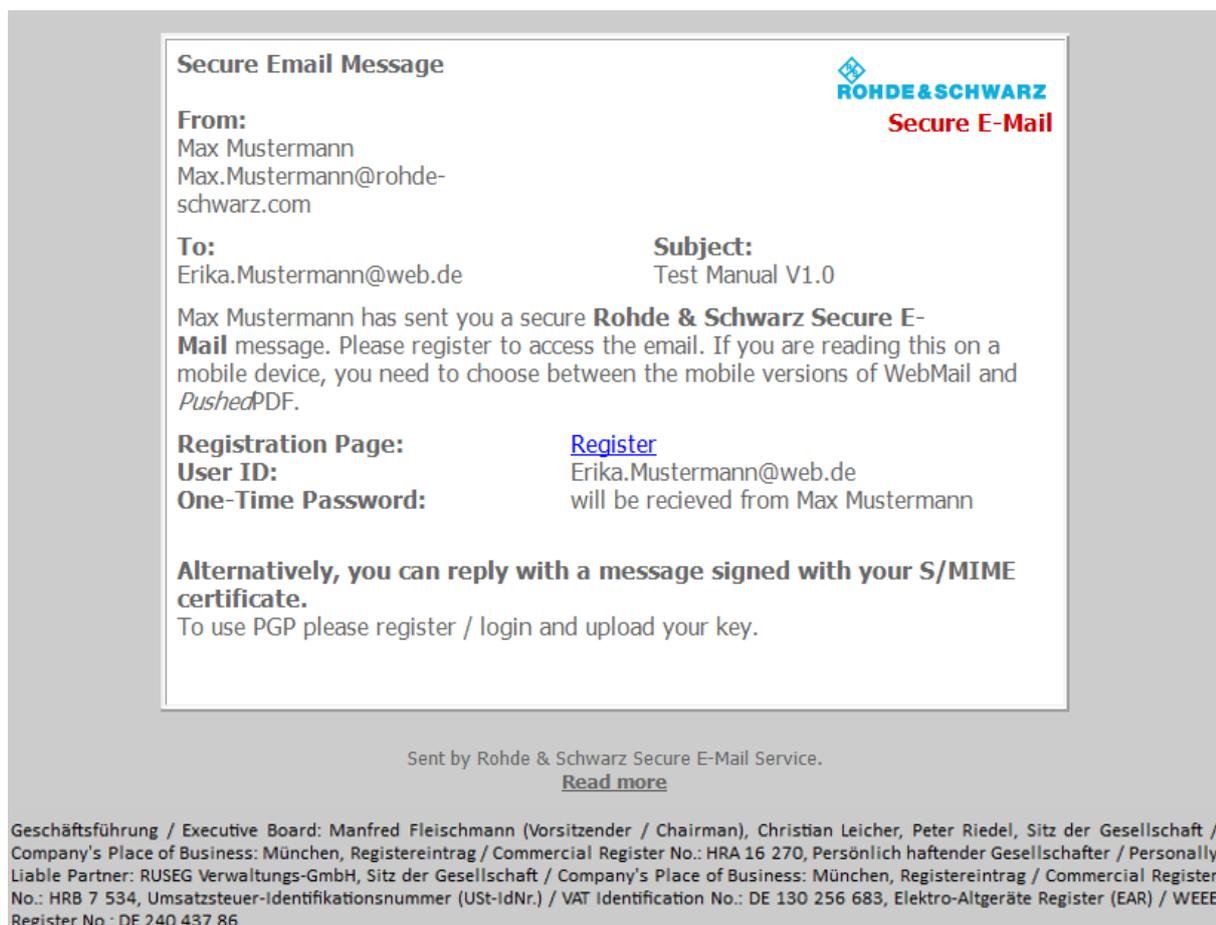


Abbildung 1: Rohde & Schwarz Secure E-Mail - Registrierungsemail

Das in der Registrierungsemail erwähnte Initialpasswort erhalten Sie von Ihrem Kommunikationspartner bei Rohde & Schwarz. Hierzu ist – zu Ihrer Sicherheit – ein anderer Weg, als der per E-Mail (z.B. Telefon, Brief) vorgesehen. Das Initialpasswort benötigen Sie,

**Leitfaden - Sichere E-Mail Kommunikation bei Rohde & Schwarz V1.1.10**

um sich am Rohde & Schwarz Secure E-Mail Webinterface zu registrieren und dort Ihre vertrauliche E-Mail lesen zu können

Diese Registrierungsemail ist signiert mit einem Schlüssel, ausgestellt durch die bei Rohde & Schwarz verwendete Quovadis Zertifizierungsstelle.

Sollten Sie bereits in der Lage sein verschlüsselte E-Mails per S/MIME zu versenden, so können Sie auf die Registrierungsemail mit einer signierten E-Mail Nachricht antworten. Das Verschlüsselungsgateway von Rohde & Schwarz greift Ihren öffentlichen Schlüssel aus der signierten Nachricht ab, validiert diesen und stellt Ihnen die vertraulichen Informationen verschlüsselt per E-Mail zu. Bei Einsatz von PGP registrieren Sie sich bitte am Rohde & Schwarz Secure E-Mail Webinterface und laden Ihren öffentlichen PGP Schlüssel hoch (siehe Kapitel 8).

# 5 Variante 1: Verschlüsselung mittels S/MIME oder PGP

Falls Sie die E-Mail-Verschlüsselung mittels S/MIME-Zertifikat oder PGP-Schlüssel vornehmen, erhalten Sie die E-Mails immer direkt an Ihr persönliches E-Mail-Programm (z.B. Mozilla Thunderbird oder Microsoft Outlook). Die Ver- und Entschlüsselung der Nachrichten erfolgt hierbei automatisch zwischen Ihrem E-Mail-Programm und dem Verschlüsselungsgateway der Rohde & Schwarz.

Um diese Variante nutzen zu können benötigen Sie zwingend ein elektronisches Zertifikat von einem Drittanbieter oder einen PGP-Schlüssel. Bitte beantworten Sie zur Einrichtung die Registrierungsmail und signieren diese Antwort mit Ihrem S/MIME-Zertifikat. Dadurch wird der Austausch der öffentlichen Schlüssel beider Kommunikationspartner vollzogen. Das Rohde & Schwarz Verschlüsselungsgateway prüft Ihre Signatur und Ihren öffentlichen Schlüssel. Sind diese valide, so wird Ihnen die vertrauliche Nachricht umgehend als S/MIME verschlüsselte Nachricht zugestellt.

Sollte Ihr S/MIME Zertifikat von einer nicht öffentlichen PKI stammen, so wird vor Aktivierung eine zusätzliche Prüfung des Schlüsselmaterials durch Rohde & Schwarz erfolgen. Bei der Verwendung von PGP Schlüsseln ist dies immer der Fall.

In diesen Fällen besteht die Möglichkeit, Ihr Zertifikat/Ihren Schlüssel am Rohde & Schwarz Secure E-Mail Webinterface unter dem Menüpunkt Einstellungen - Zertifikate selbst zu hinterlegen (siehe Kapitel 8).

Personenbezogene Rohde & Schwarz Schlüssel (S/MIME oder PGP) können Sie unter der folgenden URL abrufen: <https://securemail.rohde-schwarz.com>

## 5.1 Einsatz von Domainzertifikaten

Sollten Sie ein E-Mail-Verschlüsselungsgateway verwenden, so kann eine Verschlüsselung der Nachrichten auch auf Basis von S/MIME Domainzertifikaten oder PGP Domainschlüsseln erfolgen. Hierzu lassen Sie uns bitte Ihren entsprechenden Domainschlüssel (S/MIME oder PGP) zukommen. Die Informationen zu den Domainschlüssel (S/MIME und PGP) der Rohde & Schwarz GmbH & Co. KG finden Sie in den folgenden beiden Abschnitten 5.1.1 und 5.1.2.

### 5.1.1 S/MIME Domainzertifikat

Bitte fragen Sie Ihren Ansprechpartner bei Rohde & Schwarz nach dem Domainzertifikat.

Der S/MIME Domainschlüssel ist ausgestellt von

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

Und lautet auf

E = secureemailgw-admin-mu@rohde-schwarz.com  
CN = S/MIME DOMAIN CERTIFICATE  
OU = Secure E-Mail  
O = Rohde & Schwarz GmbH & Co. KG  
C = DE

Der öffentliche Schlüssel trägt den 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 Domainschlüssel

Bitte fragen Sie Ihren Ansprechpartner bei Rohde & Schwarz nach dem Domainkey.

Der PGP Domainschlüssel lautet auf „Secure E-Mail Gateway PGP domain key (Rohde & Schwarz) <SecureEmailGW-Admin-MU@rohde-schwarz.com>“ und ist vom PGP CA Schlüssel des Rohde und Schwarz Secure E-Mail Gateways (Rohde-Schwarz-SecureEMailGW-CA (rohde-schwarz.com) <secureemailgw-admin-mu@rohde-schwarz.com>) unterschrieben.

Der Fingerprint des PGP Domainschlüssels lautet:

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

## 6 Variante 2: Kommunikation über TLS / SMTPS

Falls Sie eine Verschlüsselung der E-Mails zwischen Ihren E-Mail Domains und den E-Mail Domains von Rohde & Schwarz auf Transportebene wünschen, so ist diese Variante die passende.

Hierzu muss Ihr Mailgateway in der Lage sein, E-Mails per STARTTLS oder SMTPS senden und empfangen zu können. Die TLS / SMTPS Verschlüsselung erfolgt zwischen Ihrem Mailgateway und dem TLS Mailgateway von Rohde & Schwarz auf Applikationsebene (Transportverschlüsselung).

Da auf Rohde & Schwarz Seite hierzu eigene Mailsysteme verwendet werden, müssen E-Mails an die Rohde & Schwarz Domains an Ihrem System nicht an den im DNS vorhandenen MX Record<sup>3</sup>, sondern an dedizierte Rohde & Schwarz Mailserver geschickt werden. Dieser ist securemail.rohde-schwarz.com (IP: 80.246.41.42)

Gegebenenfalls können auch von Rohde & Schwarz Seite aus die E-Mails an Ihre Domains zu dedizierten Mailsystemen verschickt werden.

---

<sup>3</sup> Wikipedia: Der MX Record einer Domain ist ein Eintrag im Domain Name System, welcher sich ausschließlich auf den SMTP Dienst bezieht. Dieser gibt an, unter welchem Fully Qualified Domain Name (FQDN) der Mail-Server zu einer Domäne oder Subdomäne erreichbar ist.

Für die gesicherte Kommunikation per TLS / SMTPS erwarten wir die folgenden Rahmenbedingungen:

- Bei STARTTLS erfolgt die Kommunikation über TCP Port 25. Hierbei muss sichergestellt werden, dass beide Seiten die TLS Verschlüsselung erzwingen.
- Bei SMTPS erfolgt die gesicherte Kommunikation über TCP Port 465.
- Die für das TLS Protokoll eingesetzten SSL Zertifikate müssen von einer öffentlichen Zertifizierungsstelle ausgestellt sein.
- Es werden keine selbstsignierten Schlüssel akzeptiert.
- Die Schlüssellänge muss mindestens 2048 Bit betragen.
- Der RC4 Verschlüsselungsalgorithmus wird nicht unterstützt.
- Session Keys müssen mindestens 128 Bit betragen.
- Die Common Names (CN) der verwendeten Zertifikate müssen den Hostnamen der jeweiligen E-Mail Gateways entsprechen.
- Der Mailserver muss in Ihrem Netzwerk betrieben werden und darf nicht extern gehostet sein.

Der Rohde & Schwarz TLS Schlüssel ist auf:

```
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
```

ausgestellt und von der folgenden Instanz unterschrieben:

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

Der dazugehörige Fingerprint lautet:

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

Die Firma Rohde & Schwarz unterstützt derzeit die nachfolgenden Cipher Suites für 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
```

Die Firma Rohde & Schwarz behält sich vor diese Liste anzupassen. Daher sollte Ihr System aus Kompatibilitätsgründen mehrere der genannten Suites unterstützen. Hierdurch wird sichergestellt, dass bei einer Anpassung der zu Verfügung stehenden Varianten die verschlüsselte Kommunikation zwischen Ihnen und Rohde & Schwarz weiterhin funktioniert.

Diese Variante benötigt eine Abstimmung zwischen dem IT Personal, welches Ihre Mailserver betreibt und dem IT Personal von Rohde & Schwarz. Nehmen Sie hierzu bitte Kontakt mit Ihrem Ansprechpartner bei Rohde & Schwarz auf.

# 7 Variante 3: Rohde & Schwarz Secure E-Mail Webinterface (SSL)

Sollten Sie keine Möglichkeit besitzen, um vertrauliche Nachrichten per S/MIME, PGP oder TLS verschlüsselt zu übertragen, so können Sie das Rohde & Schwarz Secure E-Mail Webinterface verwenden.

Das Registrierungspasswort, welches Sie von Ihrem Ansprechpartner bei Rohde & Schwarz erhalten, funktioniert nur für die Erstanmeldung an unserem System, weshalb Sie dieses Passwort bei der ersten Anmeldung zwingend in ein individuelles Passwort ändern müssen. Das neue Passwort muss folgenden Richtlinien entsprechen:

- Mindestens 9 Zeichen, maximal 20 Zeichen
- Mindestens ein Groß-, ein Kleinbuchstabe und eine Zahl

Dabei ist das Passwort alle 90 Tage zu ändern. Die E-Mails bleiben für die Dauer von 90 Tagen im Rohde & Schwarz Secure E-Mail System gespeichert. Sie können in dieser Zeitspanne jederzeit über einen Browser mit Ihrem Benutzernamen (Ihre E-Mail-Adresse) und Passwort darauf zugreifen. Wenn eine neue E-Mail in Ihrem Rohde & Schwarz Secure E-Mail Postfach eintrifft, erhalten Sie eine Benachrichtigung.

## 7.1 Anmeldung am Rohde & Schwarz Secure E-Mail Webinterface

Öffnen Sie mit Ihrem Browser die Seite <https://securemail.rohde-schwarz.com>, woraufhin folgendes Anmeldefenster erscheint (Abbildung 2):



Abbildung 2: Rohde & Schwarz Secure E-Mail Webinterface - Login

**Geben Sie bitte in das Feld Benutzer ID Ihren Benutzernamen (Ihre E-Mail-Adresse) ein. In das Feld Passwort geben Sie beim ersten Anmelden Ihr Initialpasswort ein (bei jedem weiteren Login Ihr individuell gewähltes Passwort). Nach Eingabe und Bestätigung erhalten Sie folgende Nachricht (siehe Abbildung 3), welche Sie zum Fortfahren auffordert.**

## Willkommen bei Rohde & Schwarz Secure E-Mail

Sie können Ihre vertrauliche Nachricht über Rohde & Schwarz Secure E-Mail lesen.

Rohde & Schwarz Secure E-Mail

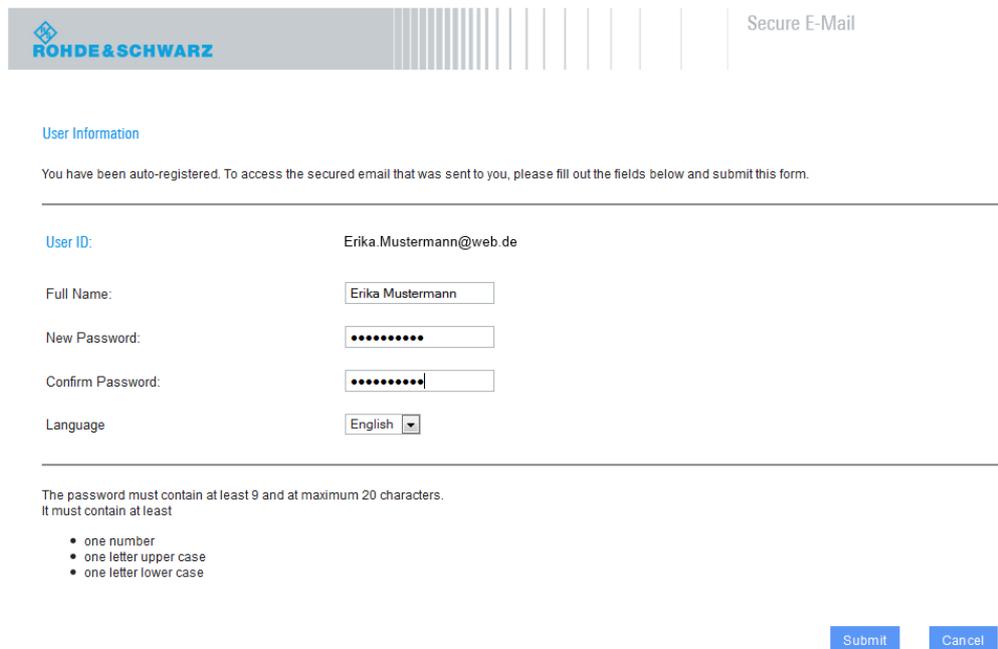
Bitte klicken Sie auf Fortfahren um mit der Registrierung für Rohde & Schwarz Secure E-Mail zu beginnen.

Fortfahren

Abbildung 3: Rohde & Schwarz Secure E-Mail Webinterface - Begrüßung

## 7.2 Eingabe der Benutzer-Informationen

Geben Sie im folgenden Schritt Ihren Namen und Ihr neues Passwort ein (siehe Abbildung 4).



The screenshot shows the registration form for Rohde & Schwarz Secure E-Mail. At the top, there is a header with the Rohde & Schwarz logo and the text 'Secure E-Mail'. Below the header, the section is titled 'User Information'. A message states: 'You have been auto-registered. To access the secured email that was sent to you, please fill out the fields below and submit this form.' The form contains the following fields:

- User ID:** Erika.Mustermann@web.de
- Full Name:** Erika Mustermann
- New Password:** A text box with 9 dots representing a password.
- Confirm Password:** A text box with 9 dots representing a password.
- Language:** English (with a dropdown arrow)

Below the form, there is a password requirement notice: 'The password must contain at least 9 and at maximum 20 characters. It must contain at least' followed by a bulleted list:

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

At the bottom right of the form, there are two buttons: 'Submit' and 'Cancel'.

Abbildung 4: Rohde & Schwarz Secure E-Mail - Username / Passwort setzen

## 7.3 Definieren der Sicherheitsfragen / -antworten

Sie werden nun aufgefordert, zwei vordefinierte und eine frei zu definierende Sicherheitsfrage auszuwählen und zu beantworten. Die Antwort auf diese Sicherheitsfragen benötigen Sie, falls Sie Ihr Passwort vergessen haben sollten. Um einen Missbrauch Ihres Accounts zu vermeiden, sind die in Abbildung 5 aufgeführten Regeln zwingend zu beachten!

The screenshot shows the 'Sicherheitsfragen' (Security Questions) setup page. At the top left is the Rohde & Schwarz logo. The page title is 'Sicherheitsfragen: Erika.Mustermann@web.de'. Below the title, there is a paragraph of introductory text and a list of hints for choosing good security questions. The hints include: choosing questions you can remember easily, avoiding questions from social media or public sources, and ensuring questions are unique. Below the hints, there are three sections for defining questions, each with a dropdown menu for the question and a text input for the answer. The first two sections are pre-defined questions, and the third is for a custom question. At the bottom, there are 'Senden' and 'Abbrechen' buttons.

Abbildung 5: Rohde & Schwarz Secure E-Mail – Sicherheitsfragen definieren

## 7.4 Login

Nach erfolgreicher Registrierung werden Sie auf die Anmeldeseite (Abbildung 6) weitergeleitet. Hier müssen Sie sich mit Ihrer E-Mail Adresse und dem gerade festgelegten Passwort anmelden.

The screenshot shows the 'Anmelden an Secure E-Mail' (Login) page. At the top left is the Rohde & Schwarz logo. The page title is 'Anmelden an Secure E-Mail'. Below the title, there is a link 'zur mobilen Version wechseln'. The login form consists of two input fields: 'Benutzername:' (Username) and 'Passwort:' (Password). The username field contains 'Erika.Mustermann@web.de'. Below the password field, there are links for 'Passwort vergessen?' (Forgot password?) and 'Key-Anforderung' (Request key). At the bottom, there is an 'Einloggen' (Login) button.

Abbildung 6: Rohde & Schwarz Secure E-Mail - Login Maske

## 7.5 Ihr Rohde & Schwarz Secure E-Mail Postfach

Im Anschluss (Abbildung 7) sehen Sie die Übersichtsseite Ihres Postfachs.

The screenshot shows the 'Übersicht' (Overview) page of the Secure E-Mail interface. The header includes the Rohde & Schwarz logo and a 'Logout' button. A sidebar on the left lists navigation options: Übersicht, Neue Nachricht, Posteingang, Entwürfe, Gesendete Nachrichten, Gelöschte Nachrichten, and Einstellungen. The main content area is titled 'Übersicht' and features a table with the following data:

Unterordner	E-Mails	Neue Nachrichten	Grösse
Posteingang	1	1 ( 2.9 KB )	2.9 KB
Gesendete Nachrichten	0	0 ( 0 bytes )	0 bytes
Entwürfe	0	0 ( 0 bytes )	0 bytes
Gelöschte Nachrichten	0	0 ( 0 bytes )	0 bytes
<b>Total</b>	<b>1</b>	<b>1</b>	<b>2.9 KB</b>

Abbildung 7: Rohde & Schwarz Secure E-Mail - Postfach Übersicht

## 7.6 Ihr Rohde & Schwarz Secure E-Mail Posteingang

Die für Sie hinterlegten Nachrichten werden chronologisch im Posteingang (Abbildung 8) aufgelistet. Durch den Klick auf den Betreff bzw. den Briefumschlag können Sie die jeweilige Nachricht öffnen. Ungelesene Nachrichten werden durch einen geschlossenen Briefumschlag hervorgehoben.

The screenshot shows the 'Posteingang' (Inbox) page. The header includes the Rohde & Schwarz logo and a 'Logout' button. A sidebar on the left lists navigation options: Übersicht, Neue Nachricht, Posteingang, Entwürfe, Gesendete Nachrichten, Gelöschte Nachrichten, and Einstellungen. The main content area is titled 'Posteingang' and features a search bar with a 'Löschen' button and a 'Suchen' button. Below the search bar is a table with the following data:

	Von	Betreff	Erhalten	Grösse
	max.mustermann@rohde-schwarz.com	Test Manual V1.1	23.01.2014 17:37	55 KB
	max.mustermann@rohde-schwarz.com	Test Manual V1.0	23.01.2014 17:36	3 KB

Abbildung 8: Rohde & Schwarz Secure E-Mail - Posteingang

Sollte eine E-Mail einen Anhang enthalten, wird dies direkt neben dem Absender durch eine Heftklammer signalisiert. Vorhandene Dateianhänge können Sie auf Ihren Rechner herunterladen. Außerdem besteht die Möglichkeit, die E-Mail als \*.html- oder \*.pdf- Datei auf Ihrer Festplatte zu speichern (siehe Abbildung 9). Auch ein Export als \*.eml-Datei ist möglich, so dass Sie die E-Mails in Ihr E-Mail-Programm (z.B. Mozilla Thunderbird oder Microsoft Outlook) importieren können.

- Übersicht
- Neue Nachricht
- Posteingang
- Entwürfe
- Gesendete Nachrichten
- Gelöschte Nachrichten
- Einstellungen

Mail Von: Max.Mustermann@rohde-schwarz.com Hilfe

Antworten      Löschen      Druckversion  
 Als html speich.    Als eml speichern    Als PDF speichern    Bilder anzeigen

<< Vorherige Nachricht    Nächste Nachricht >>

Von: Max.Mustermann@rohde-schwarz.com  
 An: Erika.Mustermann@rohde-schwarz.com  
 Betreff: Test Manual V1.0  
 Priorität: Normal  
 Gesendet: 20.04.2015 15:10

This information is classified as **COMPANY CONFIDENTIAL**

Best regards,  
 Max Mustermann  
 Rohde & Schwarz GmbH & Co.KG  
 Postfach 80 14 69 - 81614 München  
 Mühldorfstraße 15 - 81671 München  
 mailto: Max.Mustermann@rohde-schwarz.com  
 Phone:  
 Mobile Phone:  
 visit us at <http://www.rohde-schwarz.com>

Geschäftsführung / Executive Board: Manfred Fleischmann (Vorsitzender / Chairman), Christian Leicher, Peter Riedel, Sitz der Gesellschaft / Company's Place of Business: München, Registerintrag / Commercial Register No.: HRA 16 270, Persönlich haftender Gesellschafter / Personally Liable Partner: RUSEG Verwaltungs-GmbH, Sitz der Gesellschaft / Company's Place of Business: München, Registerintrag / Commercial Register No.: HRB 7 534, Umsatzsteuer-Identifikationsnummer (USt-IdNr.) / VAT Identification No.: DE 130 256 683, Elektro-Altgeräte Register (EAR) / WEEE Register No.: DE 240 437 86  
 (\*) Content provided with this E-Mail message is classified as COMPANY CONFIDENTIAL as per the classification policies in effect for the ROHDE & SCHWARZ Group of companies. All E-Mail correspondence related to the sensitive content of this E-Mail must be exchanged encrypted, without exception. Where applicable, please also refer to any related IGDs which may specify further requirements regarding encryption and message handling procedures.

Abbildung 9: Rohde & Schwarz Secure E-Mail Webinterface – E-Mail

## 7.7 Antworten

Über das Webmail Interface können Sie auch gesichert Nachrichten an Rohde & Schwarz verschicken (Abbildung 10). Dies kann eine Antwort auf eine bestehende E-Mail in Ihrem Postfach oder eine neue Nachricht sein. Einer jeden E-Mail können Dateianhänge angefügt werden. In den Feldern „An:“, „Cc:“ und „Bcc:“ werden nur gültige Rohde & Schwarz E-Mail Adressen akzeptiert. Sollten Sie mehrere R&S Personen adressieren wollen, sind deren Adressen entweder durch ein „ , „ oder „ ; “ zu trennen. Das Versenden an eine nicht Rohde & Schwarz Adresse ist nicht möglich und wird folglich zurückgewiesen!

Abbildung 10: Rohde & Schwarz Secure E-Mail Webinterface - Neue E-Mail erstellen

## 7.8 Passwortänderung

Eine Passwortänderung ist jederzeit über das Menü Einstellungen - Passwort ändern möglich. Um dies erfolgreich durchzuführen, müssen Sie zuerst Ihr altes Passwort angeben. Im Anschluss ist die Eingabe eines neuen Passworts notwendig, wobei dieses den Richtlinien in Abbildung 11 entsprechen muss.

Übersicht  
Neue Nachricht  
Posteingang  
Entwürfe  
Gesendete Nachrichten  
Gelöschte Nachrichten  
Einstellungen  
Benutzer  
Passwort ändern  
Sicherheitsfragen ändern  
Zertifikate

Secure E-Mail

Logout

### Passwort ändern

Hilfe

Speichern

Altes Passwort:

Neues Passwort:

Passwort bestätigen:

Das Passwort muss aus mindestens 9 und maximal 20 Zeichen bestehen.  
Mindestens

- eine Zahl
- ein Großbuchstabe
- ein Kleinbuchstabe

muss enthalten sein.

Abbildung 11: Rohde & Schwarz Secure E-Mail Webinterface - Passwort ändern

## 7.9 Sie haben Ihr Passwort vergessen?

Die Anmeldemaske des Rohde & Schwarz Secure E-Mail Webinterface (<https://securemail.rohde-schwarz.com>) bietet Ihnen die Möglichkeit, sich selbstständig ein neues Passwort zu setzen. Dazu wählen Sie in der Anmeldemaske den Menüpunkt Passwort vergessen (Abbildung 12). Im Anschluss werden Sie aufgefordert, Ihre vollständige E-Mail Adresse, für welches das Passwort zurückgesetzt werden soll, anzugeben (Abbildung 13). Der darauf folgende Dialog (Abbildung 14) fordert Sie zur korrekten Beantwortung der Sicherheitsfragen auf. Haben Sie diese alle richtig beantwortet können Sie ein neues Passwort setzen (Abbildung 15). Im Anschluss finden Sie sich im Rohde & Schwarz Secure E-Mail Webinterface wieder.

Secure E-Mail

Hilfe

Anmelden an Secure E-Mail

zur mobilen Version wechseln

Benutzername:

Passwort:  [Passwort vergessen?](#) [Key-Anforderung](#)

Einloggen

Abbildung 12: Rohde & Schwarz Secure E-Mail Webinterface - Passwort zurücksetzen 1

## Zurücksetzen des Passworts

Hier können Sie Ihr Passwort mit Hilfe der zuvor definierten Sicherheitsfragen zurück setzen. Bitte geben Sie Ihre E-Mail-Adresse ein.

Ihre E-Mail-Adresse

[Weiter](#)

Abbildung 13: Rohde & Schwarz Secure E-Mail Webinterface - Passwort zurücksetzen 2

## Zurücksetzen des Passworts für die E-Mail-Adresse: *Erika.Mustermann@web.de*

Bitte geben Sie die Antworten auf die von Ihnen festgelegten Sicherheitsfragen ein.

In welcher Strasse haben Sie während der dritten Klasse gewohnt?

Was ist der Mädchenname Ihrer Grossmutter mütterlicherseits?

In welcher Stadt haben Sie Ihren Partner/ihre Partnerin zum ersten mal getroffen?

Falls Sie die Antworten nicht mehr wissen, nehmen Sie bitte mit Ihrem Kommunikationspartner Kontakt auf.

[Zurück](#) [Weiter](#)

Abbildung 14: Rohde & Schwarz Secure E-Mail Webinterface - Passwort zurücksetzen 3

## Passwort ändern

Neues Passwort:

Passwort bestätigen:

[Speichern](#)

Das Passwort muss aus mindestens 9 und maximal 20 Zeichen bestehen. Mindestens

- eine Zahl
- ein Großbuchstabe
- ein Kleinbuchstabe

muss enthalten sein.

Abbildung 15: Rohde & Schwarz Secure E-Mail Webinterface - Passwort zurücksetzen 4

## 7.10 Administration von S/MIME Zertifikaten oder PGP Schlüsseln

Sollten Sie ein S/MIME Zertifikat oder einen PGP Schlüssel zur Verwendung mit E-Mail Verschlüsselung besitzen, so können Sie diese auch für die verschlüsselte E-Mail Kommunikation mit Rohde & Schwarz verwenden. Über das Menü Einstellungen – Zertifikate können Sie Ihre bei Rohde & Schwarz hinterlegten öffentlichen Schlüssel verwalten.

The screenshot shows the 'Meine Zertifikate' (My Certificates) page in the Rohde & Schwarz Secure E-Mail Web Interface. The page is titled 'Meine Zertifikate' and includes a 'Hilfe' (Help) link. The main content area is titled 'Zertifikatverwaltung' (Certificate Management) and contains a 'Löschen' (Delete) button. Below this is a table with the following columns: 'Aussteller' (Issuer), 'Antragsteller' (Applicant), 'Gültig bis' (Valid until), and 'Erstellungsdat.' (Creation date). The table contains one entry with a checkbox, a lock icon, a key icon, and a checkmark. The 'Gültig bis' date is 01.12.2015 and the 'Erstellungsdat.' is 01.12.2014. Below the table are two sections for importing certificates: 'Importieren (S/MIME)' and 'Importieren (PGP)'. Each section has a text input field for the file name, a 'Browse...' button, and an 'Importieren' button.

Abbildung 16: Rohde & Schwarz Secure E-Mail Web Interface – Administration von S/MIME Zertifikaten und PGP Schlüsseln

An dieser Stelle können Sie Ihr öffentliches S/MIME Zertifikat oder Ihren öffentlichen PGP Schlüssel importieren. Über den Button „Löschen“ können Sie abgelaufene oder zwischenzeitlich ungültig gewordene Schlüssel entfernen.

## 7.11 Mobile Login

Für den Zugriff über ein Mobile Device steht Ihnen das Rohde & Schwarz Secure E-Mail Webinterface in abgespeckter Form (siehe Abbildung 17 & Abbildung 18) ebenso zur Verfügung. Dieses erreichen Sie über den Link „Mobile Geräte“ (<https://securemail.rohde-schwarz.com/mobileLogin.jsp>). Hier stehen Ihnen die nachfolgenden Funktionen zur Verfügung:

- Nachrichten lesen / verfassen / antworten
- Nachrichten löschen
- Passwort ändern



Abbildung 17: Rohde & Schwarz Secure E-Mail Webinterface - Mobile Login

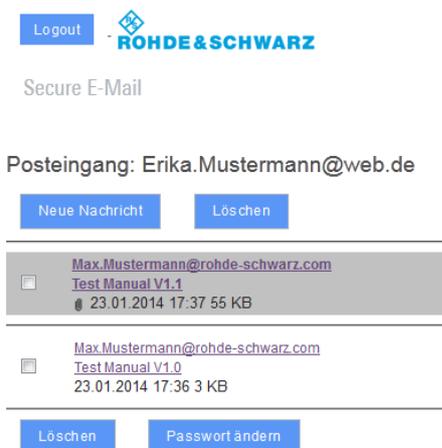


Abbildung 18: Rohde & Schwarz Secure E-Mail Webinterface - Mobile Posteingang

# 8 Änderung der Variante

Sie haben jederzeit die Möglichkeit, die verwendete Zustellmethode über das Rohde & Schwarz Secure E-Mail Webinterface zu verändern (siehe Abbildung 19). Melden Sie sich dazu am Rohde & Schwarz Secure E-Mail Webinterface an und wählen Sie den Menüpunkt Einstellungen - Benutzer aus. Dort können Sie unter Sicherheits Typ die zu verwendende Variante einstellen.

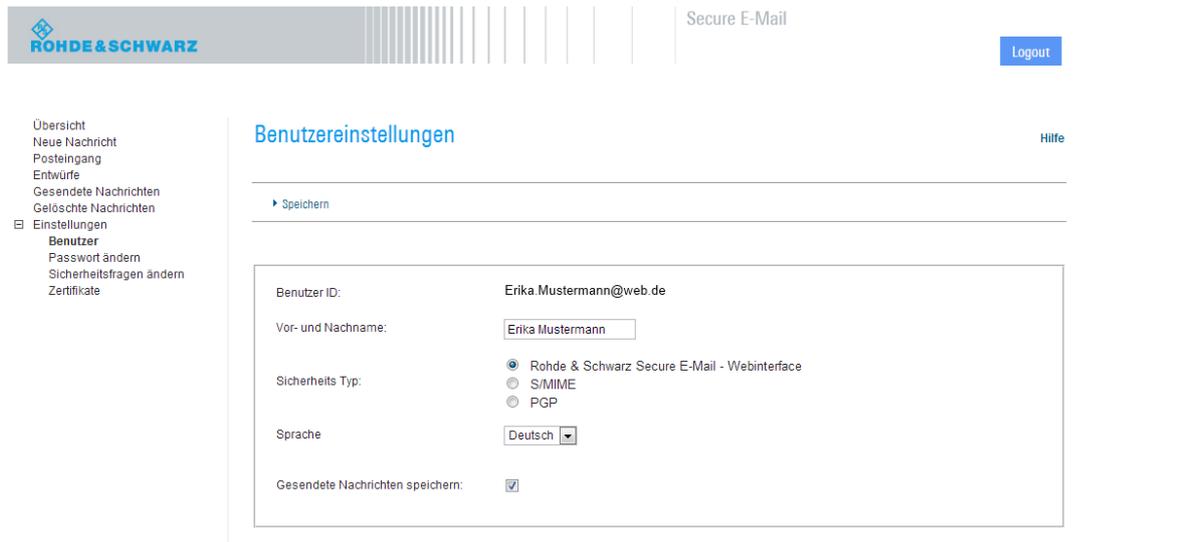


Abbildung 19: Rohde & Schwarz Secure E-Mail Webinterface - Ändern der Zustellmethode

Im Falle einer Änderung - zum Beispiel von Webmail auf S/MIME - muss auch das entsprechende Schlüsselmaterial vorhanden sein. Gegebenenfalls, muss dieses vorab am Rohde & Schwarz Secure E-Mail Webinterface unter dem Menüpunkt Einstellungen - Zertifikate hinterlegt werden (siehe Abbildung 20).



Abbildung 20: Rohde & Schwarz Secure E-Mail Webinterface - Zertifikat Upload

## 9 Anforderung öffentlicher Schlüssel

Sofern Sie selbst eine S/MIME oder PGP Verschlüsselung einsetzen, so benötigen Sie für den Aufbau einer verschlüsselten Kommunikation den öffentlichen Schlüssel Ihres Kommunikationspartners bei Rohde & Schwarz. Hierzu können Sie die öffentlichen Schlüssel von Rohde & Schwarz über den folgenden Link anfordern:

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

Das genaue Vorgehen kann beispielhaft der nachfolgenden Abbildung 21 entnommen werden. Das angeforderte S/MIME Zertifikat und der PGP Schlüssel ihres Rohde & Schwarz Kommunikationspartners wird Ihnen im Anschluss per E-Mail zugestellt (siehe Abbildung 22).

Anfordern eines öffentlichen Schlüssels

Um eine E-Mail verschlüsselt an einen Empfänger senden zu können, müssen Sie sich den notwendigen "Schlüssel" besorgen.

Bitte befolgen Sie hierzu die beschriebenen Schritte:

- Geben Sie Ihre exakte E-Mail-Adresse in das Feld "Ihre E-Mail-Adresse" ein.
- Geben Sie die exakte E-Mail-Adresse der Person, welche Sie suchen, in das Feld "E-Mail-Adresse des Schlüsselbesitzers" ein.
- Klicken Sie auf "Key-Anforderung".
- Die Schlüssel werden Ihnen per E-Mail zugesendet.

Ihre E-Mail-Adresse

E-Mail-Adresse des Schlüsselbesitzers

Abbildung 21: Rohde & Schwarz Secure E-Mail Webinterface - Public Key anfordern

Von Max Mustermann <Max.Mustermann@rohde-schwarz.com> ✉

Betreff **Anforderung des öffentlichen Schlüssels** 15:42

An Erika.Mustermann@web.de ✉

Andere Aktionen ▾

Sie haben den öffentlichen Schlüssel von **Max.Mustermann@rohde-schwarz.com** angefordert.

Mit diesem Email erhalten Sie sowohl den öffentlichen PGP Schlüssel, als auch das X.509 Zertifikat. Mit Hilfe dieser Schlüssel haben Sie nun die Möglichkeit eine verschlüsselte Email an **Max.Mustermann@rohde-schwarz.com** zu senden. Dazu müssen Sie vorher den Schlüssel in Ihr E-Mail Programm importieren.

- im Falle von **S/MIME**:  
Fügen Sie den Absender dieses Emails einfach in Ihr Adressbuch ein, anschliessend können Sie ihm mit S/MIME verschlüsselte Nachrichten schicken.
- im Falle von **PGP**:  
Importieren Sie den im Anhang befindlichen PGP Schlüssel in Ihr Email Verschlüsselungsprogramm, anschliessend können Sie ihm mit PGP verschlüsselte Nachrichten schicken.

---

[Read More](#)

Geschäftsführung / Executive Board: Manfred Fleischmann (Vorsitzender / Chairman), Christian Leicher, Peter Riedel, Sitz der Gesellschaft / Company's Place of Business: München, Registereintrag / Commercial Register No.: HRA 16 270, Persönlich haftender Gesellschafter / Personally Liable Partner: RUSEG Verwaltungs-GmbH, Sitz der Gesellschaft / Company's Place of Business: München, Registereintrag / Commercial Register No.: HRB 7 534, Umsatzsteuer-Identifikationsnummer (USt-IdNr.) / VAT Identification No.: DE 130 256 683, Elektro-Altgeräte Register (EAR) / WEEE Register No.: DE 240 437 86

Abbildung 22: Rohde & Schwarz Secure E-Mail Webinterface - Public Key E-Mail

# 10 Hinweise

**Bitte beachten Sie die folgenden Informationen:**

## **Rohde & Schwarz Secure E-Mail Webinterface:**

- Bei dem Rohde & Schwarz Secure E-Mail Webinterface Postfach handelt es sich nicht um ein Dauerarchiv. Bitte speichern Sie Ihre Nachrichten und deren Anhänge auf Ihrem Rechner. Alte E-Mails werden aus dem Postfach nach 90 Tagen gelöscht. Konten werden bei 180 Tagen Inaktivität regelmäßig gelöscht.
- Der maximale Speicher für Ihr Rohde & Schwarz Secure E-Mail Webinterface Konto beträgt 50 MB.

## **S/MIME / PGP:**

- Die öffentlichen Schlüssel von Rohde & Schwarz Mitarbeitern können über <https://securemail.rohde-schwarz.com> abgerufen werden.
- Eine Verschlüsselung auf Basis von Domainschlüsseln per PGP oder S/MIME ist möglich.

## **TLS / SMTPS:**

- Die Kommunikation für TLS / SMTPS erfolgt nicht per MX Record zu Rohde & Schwarz, sondern über das dedizierte Mailsystem securemail.rohde-schwarz.com (IP: 80.246.41.42).
- Bei STARTTLS erfolgt die Kommunikation über TCP Port 25. Hierbei muss sichergestellt werden, dass beide Seiten die TLS Verschlüsselung erzwingen.
- Bei SMTPS erfolgt die gesicherte Kommunikation über TCP Port 465.
- Die für das TLS Protokoll eingesetzten SSL Zertifikate müssen von einer öffentlichen Zertifizierungsstelle ausgestellt sein.
- Es werden keine selbstsignierten Schlüssel akzeptiert.
- Die Schlüssellänge muss mindestens 2048 Bit betragen.
- Der RC4 Verschlüsselungsalgorithmus wird nicht unterstützt.
- Session Keys müssen mindestens 128 Bit betragen.
- Die Common Names (CN) der verwendeten Zertifikate müssen den Hostnamen der jeweiligen E-Mail Gateways entsprechen.
- Der Mailserver muss in Ihrem Netzwerk betrieben werden und darf nicht extern gehostet sein.

# 11 FAQ

- F01:** Ich kann die Registrierungs-E-Mail nicht finden.
- A01:** Bitte schauen Sie auch in Ihrem Unbekannt- oder Spam Ordner nach.
- F02:** Wie lautet der Benutzername?
- A02:** Der Benutzername ist Ihre persönliche E-Mail Adresse.
- F03:** Wie soll sich das Passwort zusammensetzen?
- A03:** Die Passwortlänge beträgt mindestens 9 Zeichen, max. 20 Zeichen und muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Zahl enthalten.
- F04:** Ich will mich am Rohde & Schwarz Secure E-Mail Postfach anmelden, habe aber die E-Mail mit dem Link nicht mehr.
- A04:** Unter <https://securemail.rohde-schwarz.com> gelangen Sie auf die Anmeldeseite. Die Anmeldung erfolgt mit Ihrer E-Mail Adresse und dem von Ihnen bei der Registrierung definierten Passwort.
- F05:** Wozu dienen die Sicherheitsfragen?
- A05:** Sollten Sie Ihr Passwort vergessen haben, so können Sie durch richtiges Beantworten Ihrer Sicherheitsfragen das Passwort im Self-Service Portal zurücksetzen.
- F06:** Was passiert wenn ich die Sicherheitsfragen falsch beantworte?
- A06:** In diesem Falle wird Ihr Konto gesperrt. Bitte setzen Sie sich dann mit Ihrem Ansprechpartner bei Rohde & Schwarz in Verbindung. Dieser wendet sich an das zuständige IT-Personal. Im Anschluss werden Sie ein neues Registrierungspasswort erhalten. Mit diesem können Sie sich erneut anmelden.
- F07:** Wo sehe / erkenne ich den Absender der E-Mail?
- A07:** Der Absender erscheint immer im Text der Registrierungs-E-Mail beziehungsweise in jeder vom Verschlüsselungsgateway von Rohde & Schwarz erzeugten Benachrichtigung.
- F08:** Kann über das Postfach auch auf E-Mails geantwortet werden?
- A08:** Ja, Sie können auf E-Mails in dem Rohde & Schwarz Secure E-Mail Postfach antworten. Ebenso können Sie dort neue Nachrichten für Rohde & Schwarz Mitarbeiter erstellen um diesen Informationen über den sicheren Kanal zukommen zu lassen.
- F09:** Können auch Anhänge über das Rohde & Schwarz Secure E-Mail Webinterface versendet werden?
- A09:** Ja, analog zu üblichen E-Mail Programmen können Sie auch im Rohde & Schwarz Secure E-Mail Webinterface Anhänge an Ihre E-Mails anfügen.

**F10:** Wie lange ist das Postfach gültig?

**A10:** Nach 180 Tagen Inaktivität wird Ihr Konto gelöscht. Sie werden hierüber informiert. Bitte speichern Sie daher die Nachrichten und ihre Anhänge auf Ihrem Rechner. Eine Archivierung seitens Rohde & Schwarz findet nicht statt!

**F11:** Wie lange ist ein Passwort gültig?

**A11:** Mit Ausnahme des Initialpassworts ist das Passwort alle 90 Tage zu ändern. Dieses darf dabei nicht dem vorangegangenen entsprechen.

**F12:** Wie lauten der Titel und der Absender der Registrierungsemail für das Rohde & Schwarz Secure E-Mail Webinterface?

**A12:** Subject / Titel: „*Register to Receive an Encrypted Email*“  
From / Sender: Ihr Rohde & Schwarz Kommunikationspartner

**F13:** Was mach ich, wenn ich die Mail am Rohde & Schwarz Secure E-Mail Webinterface nicht abrufen kann?

**A13:** Bitte Stellen Sie sicher, dass Sie sich bereits erfolgreich für das Rohde & Schwarz Secure E-Mail Webinterface registriert haben. Sollte dies nicht der Fall sein, setzen Sie sich dann mit Ihrem Ansprechpartner bei Rohde & Schwarz in Verbindung. Dieser wendet sich an das zuständige IT-Personal. Im Anschluss werden Sie ein neues Registrierungspasswort erhalten. Mit diesem können Sie sich erneut anmelden.

**F14:** Wie kann ich als ext. Kommunikationspartner Schlüsselmaterial mit Rohde & Schwarz austauschen, ohne stets über die Mailbox gehen zu müssen?

**A14:** Wenn Sie uns Ihr S/MIME Zertifikat zur Verfügung stellen wollen, senden Sie uns eine signierte E-Mail. Im Falle von PGP können Sie diesen über das Rohde & Schwarz Secure E-Mail Webinterface hochladen. Diese Möglichkeit besteht ebenfalls für Ihr S/MIME Zertifikat. Sollten sie wiederum Schlüsselmaterial von Rohde & Schwarz beziehen wollen, können Sie dies über das Rohde & Schwarz Secure E-Mail Webinterface (<https://securemail.rohde-schwarz.com/>).

**F15:** Kann ich beim Antworten über das Rohde & Schwarz Secure E-Mail Webinterface eine nicht Rohde & Schwarz Person in Kopie setzen?

**A15:** Nein dies ist nicht möglich, da das Rohde & Schwarz Secure E-Mail Webinterface ausschließlich der sicheren Kommunikation zwischen Ihnen und Rohde & Schwarz dient.

## 12 Haben Sie weitere Fragen?

Bei Fragen wenden Sie sich bitte an Ihren Ansprechpartner bei Rohde & Schwarz.

## Rohde & Schwarz

Der Elektronikkonzern Rohde & Schwarz bietet innovative Lösungen auf den Arbeitsgebieten Messtechnik, Rundfunk- und Medientechnik, sichere Kommunikation, Cyber-Sicherheit sowie Funküberwachungs- und -ortungstechnik. Vor mehr als 80 Jahren gegründet, ist das selbstständige Unternehmen in über 70 Ländern mit einem engmaschigen Vertriebs- und Servicenetz präsent.

In seinen angestammten Arbeitsgebieten zählt der Elektronikkonzern zu den führenden Anbietern weltweit. Der Firmensitz ist in München, Deutschland. Ergänzend steuern je ein regionales Headquarter in Singapur sowie in Columbia, USA, die Geschäfte.

## Regional Kontakt

Europa, Afrika, Mittlerer Osten  
+49 89 4129 12345

[customersupport@rohde-schwarz.com](mailto:customersupport@rohde-schwarz.com)

Nord Amerika

1 888 TEST RSA (1 888 837 87 72)

[customer.support@rsa.rohde-schwarz.com](mailto:customer.support@rsa.rohde-schwarz.com)

Lateinamerika

+1 410 910 79 88

[customersupport.la@rohde-schwarz.com](mailto:customersupport.la@rohde-schwarz.com)

Asien Pazifik

+65 65 13 04 88

[customersupport.asia@rohde-schwarz.com](mailto:customersupport.asia@rohde-schwarz.com)

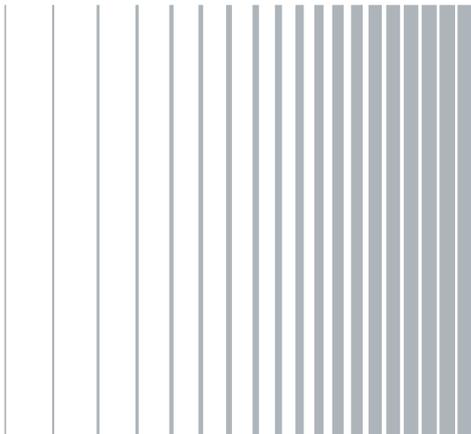
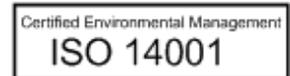
China

+86 800 810 82 28 | +86 400 650 58 96

[customersupport.china@rohde-schwarz.com](mailto:customersupport.china@rohde-schwarz.com)

## Nachhaltige Produktgestaltung

- Umweltverträglichkeit und ökologischer Fußabdruck
- Energie-Effizienz und geringe Emissionen
- Langlebigkeit und optimierte Gesamtbetriebskosten



**Rohde & Schwarz GmbH & Co. KG**

Mühl Dorfstraße 15 | D - 81671 München

Telefon + 49 89 4129 - 0 | Fax + 49 89 4129 - 13777

[www.rohde-schwarz.com](http://www.rohde-schwarz.com)