



SECURE E-MAIL & WEBMAIL

CONFIDENTIALITY WITHIN E-MAIL COMMUNICATION

WHAT IS SECURE E-MAIL?

Secure e-mail is a service for processing e-mail exchanges between external contacts and Three Rock Capital Management by using a digital signature and encryption to ensure authenticity and security. E-mails from Three Rock Capital Management with a secure e-mail function are always signed by a digital signature guaranteeing the recipient that the e-mail was indeed sent by the indicated sender and has not been modified in transit. Additionally, encryption protects the content of the e-mail. This service is valid for Three Rock Capital Management e-mails with the ending '@threerockcapital.com'.

WHY SECURE E-MAIL?

Greater security and confidentiality in e-mail communications with our clients and partners are important to us. Various events in the past have demonstrated that there is a clear need for more protection from unauthorised third-party access. In order to meet these requirements, Three Rock Capital Management provides secure e-mail as a suitable solution.

WHAT IS PROTECTED BY SECURE E-MAIL AND WHAT IS NOT?

- **Secure e-mail offers**
 - Authenticity: the legitimacy of the sender is ensured. Is the sender really the person shown as the sender (signature)?
 - Integrity: the message is not modified in transit from the sender to the recipient (signature).
 - Confidentiality: the message can only be read by the intended recipient (signature and encryption).
- **Secure e-mail does not protect**
 - Against disclosing the communication relationship; who is communicating with whom remains freely accessible.
 - Against intentional or accidental deletion/destruction of e-mails.

PREREQUISITES FOR SECURE E-MAIL COMMUNICATION

In order to transmit secure, encrypted e-mails, you must use an e-mail program with secure e-mail functionality (S/MIME or PGP standard). The standard installations of most common programs (MS Outlook, Mozilla Thunderbird, etc.) are already equipped with the necessary functionalities.

In order to be able to send and receive signed and/or encrypted e-mails, you need a digital certificate. This corresponds to the authentication of your identity and is confirmed by an independent, accredited third-party authority. A digital certificate is also a kind of electronic document or digital identification that guarantees the accuracy of the data in the certificate. A digital certificate contains a defined pair of keys: a private key and a public key, on the basis of which encryption and decryption take place and a digital signature is created.

Some companies have already set up infrastructures with secure e-mail. If this is not the case with you, for instance on your personal PC, you need a personal certificate. The issuing of qualified certificates may be subject to governmental authorisation. We recommend that you use only certificates issued by a publicly accredited certificate authority.

The Website of the Swiss State Secretariat for Economic Affairs SECO (SECO ADMIN CH) lists all recognised certificate authorities in Switzerland. For international or country-specific certification authorities, please contact your Relationship Manager or the IT Service Centre.

The cost of a personal certificate is currently Approximately CHF 40 annually.

If an external contact has no S/MIME or PGP technology for encrypting e-mails, the encrypted e-mails will be made available in an SSL-secure Web application, hereinafter

referred to as 'Secure Webmail'. An automatically generated notification e-mail will inform the external contact that he/she has received an encrypted e-mail. Using Secure Webmail, he/she can then log in and, after authentication, read all of the encrypted e-mails delivered to him/her.

INFO BOX

S/MIME: Secure Multipurpose Internet Mail Extensions is an encryption standard that defines the structure and configuration of e-mails and other Internet messages. It provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption). S/MIME functionality is built into the vast majority of modern e-mail software and interoperates between them.

PGP Standard: Pretty Good Privacy is a program for encrypting and signing data. PGP uses a so-called public key process, i.e. there is a clearly allocated key pair. The pair consists of a public key, which anyone can use to encrypt data for the recipient, and a secret private key, which only the recipient possesses and which is protected by a password. Messages sent to the recipient are encrypted with his/her public key and can then only be decrypted by the recipient's private key.

CASE 1: S/MIME CERTIFICATE OR PGP KEY IS AVAILABLE

The following scenarios describe the secure e-mail communication between Three Rock Capital Management and an external user when the user is already able to encrypt or add signatures to e-mails using S/MIME or PGP technology.

1. A Three Rock Capital Management employee sends an external recipient a signed e-mail that is to be encrypted.
2. The e-mail is routed internally to the SecureMail system.
3. The SecureMail system verifies whether the external partner is already registered

and whether his/her public key (S/MIME or PGP) is available.

4. If no S/MIME certificate or public PGP key is available for the external contact, or if one cannot be found via the associated indexing services or key servers, the encrypted e-mail will be temporarily stored in the SecureMail system and the external contact will be sent a notification e-mail in the following form:

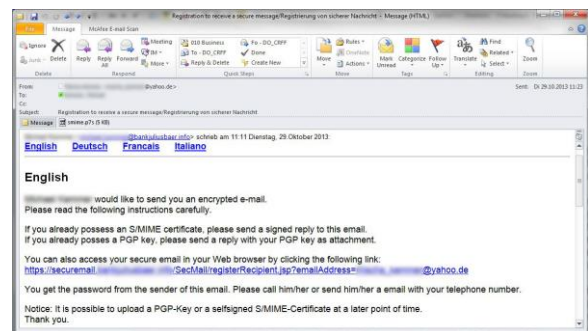


Figure 1: Notification for first-time registration

CASE 2: NEITHER AN S/MIME CERTIFICATE NOR A PGP KEY IS AVAILABLE

The following scenarios illustrate secure e-mail communication between a Three Rock Capital Management employee and an external user who does not yet have e-mail encryption technology (S/MIME or PGP) available.

1. An employee of Three Rock Capital Management sends an external recipient a (signed) e-mail that is to be encrypted by the SecureMail system.
2. The e-mail is routed internally to the SecureMail system.
3. The SecureMail system verifies whether the external partner is already registered and whether his/her public key (S/MIME or PGP) is available.
4. If no S/MIME certificate or public PGP key is available for the external contact, or if one cannot be found via the associated indexing services or key servers, the encrypted e-mail will be temporarily stored in the SecureMail system and the external contact will be sent a notification e-mail in the following form:

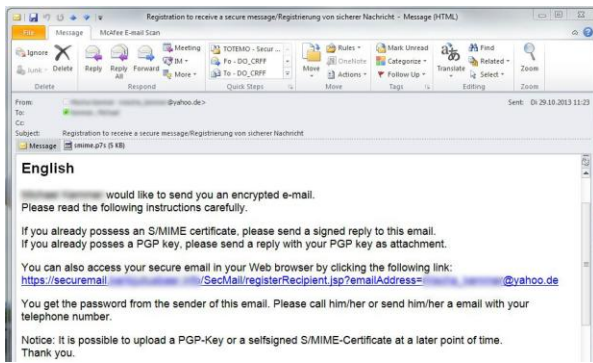


Figure 2: Notification for first-time registration

5. Please get in contact with your Relationship Manager to get your One Time Password (OTP), which is necessary to log in the first time.
6. Navigate, using the URL in the e-mail notification that was sent to you (see figure 2).

The following page will be opened in a web browser:

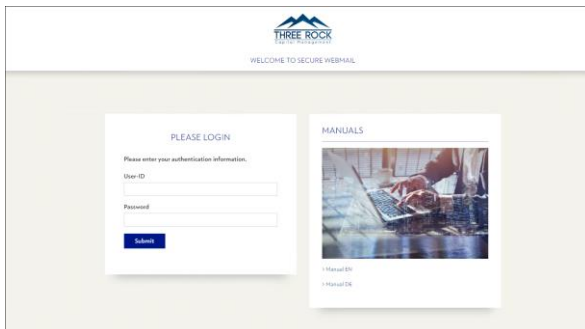


Figure 3: First login 'Secure Webmail'

7. After the first login with the OTP, you have to set a new password. Please note that the following syntax has to be used: minimum 8 but maximum 15 characters as well as special characters like: !"#\$%&'()*+,-./:;<=>@[]^_`{|}~ can be used.
8. You must then login again with the new password, after which you will have access to encrypted mails via the 'Secure Webmail' interface.

ACCESSING DELIVERED E-MAILS VIA SECURE WEBMAIL

Using the 'Secure Webmail' interface, you can read, answer, send or delete e-mails as well as download e-mails to your desktop (HTML, PDF, etc.). The menu in the left column is easy to understand and resembles well-known provider interfaces such as GMX, Hispeed, etc. The options are self-explanatory:

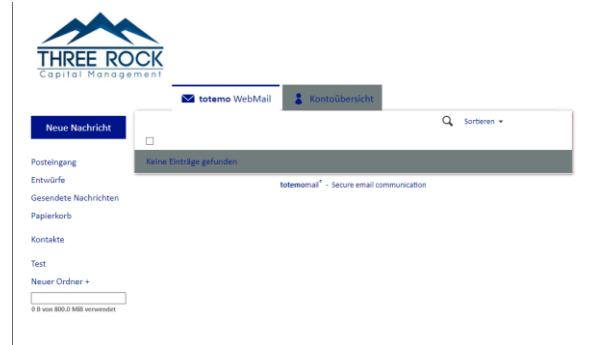


Figure 4: SecureMail interface

As soon as you are registered and get a new, encrypted e-mail from a Three Rock Capital Management employee address, you will receive a notification from the SecureMail system that a new message is waiting in the 'Secure Webmail' system:

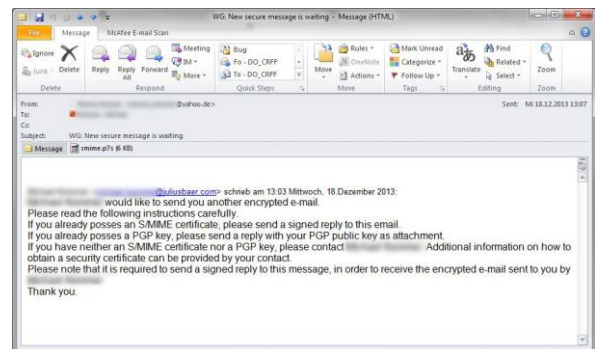


Figure 5: Notification of delivered secure e-mail

PASSWORD RESET

Password resets will always be performed via your Relationship Manager. Please get in touch with him or her to perform this action

THREE ROCK CAPITAL MANAGEMENT LTD

149 Francis Street
Dublin 8
Ireland
Telephone +353 1 440 5183
Mobile +353 87 638 6033
Email: info@threerockcapital.com

Three Rock Capital Management
is a UCITS Management Company
and an Alternative Investment Fund Manager
based in Dublin, Ireland.