Encrypted exchange of E-Mails with MTU

1 Introduction

Dear business partner,

confidential and secure exchange of information is an essential basis for successful cooperation. MTU Aero Engines AG is taking numerous measures to make the exchange of e-mails as secure as possible.

The aim of this document is to provide you with all the information you need to set up a secure e-mail exchange with MTU yourself or together with your IT service provider.

2 Encrypted transmission of e-mails

In many cases, e-mails are transmitted over the Internet unencrypted. An e-mail is therefore comparable to a postcard in the real world. Each intermediate stop during delivery can read the contents of the e-mail. In the case of e-mails, these are the recipients and senders, the technical service providers for the operation of the e-mail systems, and the Internet providers that operate the connection routes. For this reason, unencrypted e-mails are unsuitable for sending confidential content.

To still be able to exchange confidential content, e-mail encryption can be used. MTU Aero Engines uses **TLS infrastructure-to-infrastructure encryption**.

This procedure enables encrypted transmission of e-mails from the sender’s e-mail server to the recipient’s e-mail server. The contents of the e-mails are available on the e-mail servers in a readable form and can for example be checked for viruses. An insight by internet service providers is thus excluded – only the operator of the e-mail server could technically gain insight into e-mails. In the case of MTU and most partners, the e-mail servers are operated either by the company itself or by trusted partners. The use of this type of encryption therefore does not represent a disadvantage for security. Only when using public e-mail servers (e.g. GMX / Web.de / Google Mail) there would be a risk that the operator would gain insight into contents.

Another advantage is the significantly simplified key management. Only the e-mail servers need certificates, but not the individual users. Encrypting e-mails in this way is therefore much easier.

The use of infrastructure to infrastructure encryption is common today on the basis of the TLS standard and is offered by all major public e-mail providers (T-Online / Web.de / Microsoft Office 365). This method is therefore MTU's preferred method for transmitting encrypted e-mails.

Two operating modes are possible at MTU:

- TLS-Preferred
- TLS-Required

2.1 TLS-Preferred

TLS-Preferred is enabled by default for all incoming and outgoing e-mails. As soon as the other side offers a TLS-secured transmission of the e-mail, it will automatically be encrypted. If a transmission can only take place unencrypted, it is carried out unencrypted.

In order to carry out an encrypted exchange of e-mails, your e-mail system needs a valid and trustworthy certificate from an official certificate authority with a good reputation. This certificate must be issued to the hostname of the sending system. Self-generated or expired certificates are not accepted.

You can check your domains settings with the tool https://www.checktls.com/
Only if this test responds positive, a secured exchange is possible.

2.2 TLS-Required

Upon request, MTU may agree with a communication partner for individual domains (e.g. @mtu.de) that e-mails are to be transmitted exclusively in encrypted form. If an encrypted transmission is not possible, the transmission is aborted and the sender is informed. This measure prevents an attacker from specifically blocking encrypted communication in order to force unencrypted transmission.

The measure is only fully effective if the other party also refuses to transmit unencrypted e-mails from/to MTU. Please get in touch with your MTU contact person for further information.

Please note that the requirements listed under 2.1 must be met at all times, otherwise e-mails will not be transmitted if TLS-Required has been agreed and activated.

3 Implementing TLS

In order to implement an encrypted exchange of e-mails via TLS, the mail servers of both partners must be configured accordingly

3.1 Receiving e-mails

- Activation of TLS when receiving e-mails
- Deposit of a suitable server certificate

3.2 Sending e-emails

- Activation of TLS when sending e-mails
- Activation of a policy that only allows sending e-mails to MTU domains via TLS
- Deposit of CA certificates to validate MTU certificates

3.3 Surrounding terms

- The issuer of the certificates must be an official Certificate Authority (CA) whose certificate and certification policy are verifiable by us.
- Self-signed certificates cannot be supported