Notes on e-mail encryption with HELLA KGaA Hueck & Co.

Table of contents

1. E-Mail encryption at HELLA KGaA Hueck & Co.

1.1 Introduction

The transmission of e-mails of the level "confidential" and above over the Internet from and to HELLA KGaA Hueck & Co. is only permitted in encrypted form. Users themselves are to judge whether they are dealing with data of such a confidential nature. A strict standard is to be applied in this regard.

1.2 Technology used by HELLA KGaA Hueck & Co.

For the secure transmission of confidential e-mails, HELLA KGaA Hueck & Co. offers the following encryption method, which is recommended as standard technology by the German Association of the Automotive Industry (VDA):

- Transport encryption between the e-mail systems (TLS in "mandatory" mode)

2. Transport Layer Secruity (TLS)

2.1 Overview

TLS is a method of encrypting the communication between two e-mail gateways (MTA, Mail Transfer Agent) at the application level (transport encryption). The connection between the e-mail gateways is established in unencrypted form on port 25 and switched to encrypted communication for the duration of the connection.

The STARTTLS keyword is used to tell the SMTP client that the SMTP server is currently able to negotiate the use of TLS. It takes no parameters. Any existing redundancy solutions, e.g. in the form of multiple e-mail gateways and Internet connections, can still be used without any restrictions.

The configuration steps to be implemented in order to permit e-mail exchange by TLS at the e-mail gateways (e-mail servers) on the Internet side are essentially as follows:

- Receiving e-mails from HELLA KGaA Hueck & Co.:
  - Activation of TLS when receiving e-mails.
  - Definition of a suitable server certificate.

- Sending e-mails to HELLA KGaA Hueck & Co.:
  - Activation of TLS when sending e-mails.
  - Activation of a policy on the basis of which the sending of e-mails to HELLA KGaA Hueck & Co. domains is exclusively permitted via mandatory TLS only.
  - Definition of a suitable server certificate.
  - Definition of corresponding public CA certificate chain

2.2 Sending from HELLA KGaA Hueck & Co. to an external Partner

When sending to you as a partner, we expect the following general conditions:

- SMTP with STARTTLS is used as a protocol.
- The sending of e-mails by SMTPS on port 465 is not supported.
- E-mails are only delivered to remote stations that support session keys with a length of 128 bits or more.
- Encryption with RC4 is not supported. In particular, this concerns older versions of Microsoft Exchange.
- The common names (CN) of the certificates used must each correspond to the host names of the e-mail gateways on which they are defined.
- The certificate must not be issued to a domain or host name, but to the named certificate holder.
- The issuer of the certificates must be a well-known certificate authority (CA), whose certificate and certification policy is verifiable for us (see attached).
- The validation of the certificate holder must not be performed at the CA by e-mail robot or the like, but rather on the basis of documents.
- The certificate used by the CA (root CA certificate, issuing CA certificate) may only be used for issuing document-validated certificates.
- Self-signed certificates cannot be supported.
- Since it currently still cannot be ruled out that e-mails with HELLA KGaA Hueck & Co. return addresses are sent by third parties, we would ask you to ensure that e-mails are still accepted in future via unencrypted routes.

2.3 Sending from an external Partner to HELLA KGaA Hueck & Co.

When sending e-mails to the HELLA KGaA Hueck & Co. e-mail gateways, it is important to observe the following:

- SMTP with STARTTLS is used as a protocol.
- The receipt of e-mails via SMTPS on port 465 is not supported.
- Only session keys of 128-bit length or greater are supported.
- Encryption with RC4 is not supported. In particular, this concerns older versions of Microsoft Exchange.
- The common names (CN) of the certificates used at HELLA KGaA Hueck & Co. each correspond to the host names of the e-mail gateways on which they are defined.
- The host names of the e-mail gateways and hence also the CN entries of the certificates correspond to the following format, which you should check when dispatching e-mails:
- The issuer of the certificates at HELLA KGaA Hueck & Co. is currently the GlobalSign CA.
- Please configure your e-mail servers such that e-mails are always forwarded - as a mandatory condition - with TLS to the HELLA KGaA Hueck & Co. domains you use.

HELLA does enforce TLS when receiving e-mails from your domain, meaning that HELLA will not accept unencrypted e-mails from your site.