Options for encrypted e-mail communication with AUDI AG

Release: 04/2023

Options for encrypted e-mail communication with AUDI AG

Confidential and secret information may only be transmitted to and from AUDI AG in encrypted form. We offer our suppliers and partners various options for encrypted e-mail communication with AUDI AG.

1. Permanent transport encryption (Mandatory TLS)

Recommended if a partner company frequently exchanges confidential e-mails with AUDI AG.

Recommended Solution

2. PGP keys or S/MIME certificates

Useful if a partner company only exchanges confidential e-mails with individual employees of AUDI AG.

3. Encrypted HTML file

Necessary if a partner company has not yet implemented either option 1 or option 2. In this case, confidential e-mails from Audi are sent to the partner company using an encrypted HTML file.

3. Microsoft RMS (Rights Management Services)

In addition to options 1-3, Microsoft RMS (Rights Management Services) is used to protect confidential attachments (e.g. documents and files) in e-mails from AUDI AG to the partner company.

For secret information

Only end-to-end encryption of the e-mail using S/MIME certificates is permitted for sending secret information.

1. Permanent transport encryption (mandatory TLS / Transport Layer Security)

› Method: Establishing a permanently active, secure e-mail connection between a partner company and AUDI AG. This is done by forced transport encryption between the e-mail gateways of AUDI AG and the partner company.

› Scope: If confidential e-mails are frequently exchanged between a partner company and AUDI AG.

Advantages	Disadvantages	Costs
➢ **All** e-mail traffic to and from AUDI AG is automatically encrypted for transport without any further effort on the part of the user. ➢ Even if other security measures are used incorrectly (e.g. PGP encryption), e-mails are transmitted securely.	➢ AUDI AG can only ensure that TLS is enforced when sending e-mails from AUDI AG to the e-mail gateway of the partner company. ➢ The partner company must ensure the encrypted transmission of confidential e-mails from the partner company to the e-mail gateway of AUDI AG. ➢ The partner company must ensure that the transport route between the e-mail gateway and the e-mail client is also secured. ➢ AUDI AG must be informed by the partner company of changes to the certificates or the e-mail gateways used.	➢ Certificate costs for securing the e-mail communication ➢ E-mail gateway customization costs

Further information:

› The installation of permanent transport encryption for sending e-mails from AUDI AG to the partner company must be requested from AUDI AG.

› Further information can be found in the document “Notes on e-mail encryption with AUDI AG”.

2. PGP Keys or S/MIME Certificates

- Method: Encryption of individual e-mails based on established cryptographic standards. In order to be able to encrypt and decrypt e-mails, the sender and recipient must have suitable key material or certificates and have published or exchanged this.
- Scope: If the partner company has PGP keys or S/MIME certificates and confidential e-mails are only exchanged with individual employees of AUDI AG.

Advantages	Disadvantages	Costs
➢ Existing PGP keys or S/MIME certificates can be used. ➢ PGP keys or S/MIME certificates can also be used for communication with other companies.	➢ In most cases, requires additional effort for the user when sending / receiving e-mails (key management). ➢ Appropriate software must be installed on the end device and/or the e-mail gateway.	➢ Certificate costs ➢ If applicable, license costs

Further information:

- Further information can be found in the document “Notes on e-mail encryption with AUDI AG”.

3. Encrypted HTML file

- Method: Encryption of individual e-mails by generating an encrypted HTML file. The password for decryption will be communicated to the recipient separately in another way (e.g. by telephone / SMS).
- Scope: If a partner company only spontaneously receives confidential e-mails from AUDI AG and no other secure transmission method exists.

Advantages	Disadvantages	Costs
➢ no investments in IT infrastructure necessary. ➢ Rule-compliant transmission of confidential data is ensured.	➢ High effort for the user when sending / receiving e-mails, since a new password has to be exchanged separately by telephone / SMS for each encrypted e-mail. ➢ High demands on password management, as old e-mails can only be read with the appropriate password.	➢ none

4. Microsoft RMS (Rights Management Services)

- Method: Additional protection of confidential attachments (documents and files) in e-mails from AUDI AG to the partner company using Microsoft RMS.
- Scope: In order to ensure the protection of confidential documents and files when they are stored or further distributed by the recipient, they can also be protected by AUDI AG with Microsoft RMS. In this case, the authorizations for accessing and handling this data are controlled via RMS.

Further information:

- Information on how to deal with RMS-protected confidential information can be found on the ONE.Group Business Platform (https://vwgroupsupply.com/) under Information -> Security in cooperation -> Requirements information security and IT security