AUDI AG

Notes on e-mail encryption with AUDI AG

Author: AUDI AG IT-Security
Version: 3.1
Release: 04/2023

Table of contents

1 E-mail encryption at Audi

1.1 Introduction

The transmission of e-mails classified as “confidential” or higher via the Internet from and to AUDI AG is only permitted in encrypted form. The assessment of whether such data is available is made by the user himself. A strict standard must be applied here.

If data classified as “confidential” or higher is exchanged with AUDI AG by e-mail, a suitable encryption method must be used.

1.2 Technology used at AUDI AG

For the secure transmission of confidential e-mails, AUDI AG offers the following encryption methods, which are recommended as standard technologies by the German Association of the Automotive Industry (VDA):

For **confidential** e-mails **from Audi to an external partner**

- Transport encryption between the e-mail gateways by using TLS in “mandatory” mode (preferred)
- Encryption of e-mails at the AUDI AG e-mail gateway using PGP based on user and domain keys
- Encryption of e-mails at the AUDI AG e-mail gateway using S/MIME based on user and domain certificates
- End-to-end encryption of e-mails based on of S/MIME user certificates

In addition, attachments in e-mails (e.g. documents or files) classified as confidential can be protected by Microsoft RMS (Rights Management Services).

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.

For **confidential** e-mails **from an external partner to Audi**

- Transport encryption between the e-mail gateways by using TLS in “mandatory” mode (preferred)
- Encryption of e-mails using PGP based on user and domain keys and decryption at AUDI AG e-mail gateway
- Encryption of e-mails using S/MIME domain certificate and decryption at AUDI AG e-mail gateway
- End-to-end encryption of e-mails based on of S/MIME user certificates

For transmission of **secret** e-mails only end-to-end encryption based on S/MIME user certificates is permitted.

2 TLS

2.1 Overview

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

Since TLS is based on the SMTP protocol, any existing redundancy solutions, e.g. using multiple e-mail gateways and Internet connections, can still be used without any restrictions. It is important to note, that the e-mail gateway of the communication partner should be set up on their premises. When using a provider's e-mail gateway (e.g. Microsoft 365), it must be ensured that appropriate contractual agreements have been concluded with the provider to protect the data.

Communication to back-end systems or clients must be adequately secured.

At least TLS v1.2 with PFS (Perfect Forward Secrecy) or TLS v1.3 shall be used for encryption[1].

[1] See BSI - Bundesamt für Sicherheit in der Informationstechnik - BSI TR-02102-2

To enable e-mail exchange using TLS the following configuration steps must be implemented on the e-mail gateways connected to the Internet:

- Receiving e-mails:
  - Activation of TLS when receiving e-mails.
  - Provision of a suitable server certificate.

- Sending e-mails:
  - Activation of TLS when sending e-mails.
  - Activation of a policy which enforces TLS when sending e-mails to Audi domains.
  - Provision of CA certificates which are required to verify Audi certificates.

2.2 Sending from Audi to an external partner

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

- SMTP with STARTTLS is used as 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 supports at least TLS v1.2 with PFS or TLS v1.3.
- The common names (CN) of the certificates must correspond to the host names of the e-mail gateways on which they are installed.
- The issuer of the certificates must be a certificate authority (CA), whose certificate and certification policy are verifiable for us (see examples at 7.1 Certificate Authorities).
- Required certificate security level: at least ‘Class 1’ or ‘Domain Validation’ (DV).
- The certificate used by the CA (Root CA Certificate, Issuing CA Certificate) may only be used to issue certificates where the identity of the holder has been validated.
- Self-signed certificates cannot be supported.

2.3 Sending from an external partner to Audi

When sending e-mails to the Audi e-mail gateways, you should note the following:

- SMTP with STARTTLS is used as 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.
- At least TLS v1.2 with PFS or TLS v1.3 is used for encryption.
- The common names (CN) of the certificates used at Audi each correspond to the host name of the e-mail gateway on which they are installed.
- 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:
  - mailin*.audi.de
- The issuer of the certificates used by Audi is currently QuoVadis Global SSL ICA G3 (https://www.quovadisglobal.com/download-roots-crl/).
- Please configure your e-mail server to enforce TLS for all e-mails sent to the Audi domains you use.
- The following list of Audi domains can be used as a basis for a corresponding policy:
  - audi.de
  - audi.hu

Audi does not enforce TLS when receiving e-mails from your domain. However, you must ensure that confidential e-mails are not sent via unencrypted connections.

2.4 Procedure

Please request the corresponding change request form from your Audi contact. Please send the completed form back to your Audi contact.

3 Encryption at the e-mail gateway

3.1 Sending from Audi to an external partner

In order to be able to encrypt all confidential e-mails to you before they are sent, we need your PGP public key (user or domain) or S/MIME certificate (user or domain).

To do this, please send an e-mail with the corresponding PGP public key or a signed e-mail with the corresponding public S/MIME certificate to your Audi contact.

3.2 Sending from an external partner to Audi

For e-mail encryption, please use our PGP domain key or our S/MIME certificate (user or domain).

User-based S/MIME certificates for all employees of VW group can be obtained at https://certdist.volkswagen.de/faces/components/requestCert_USER.xhtml.

3.2.1 S/MIME domain certificate

The Audi S/MIME domain certificate is attached to this document (**Audi_SMIME_Container.p7b**).[2]

3.2.2 PGP domain key

The Audi PGP domain key is attached to this document (**Audi_PGP_Domainkey.asc**).[2]

Key-ID:
87 38 19 23
Fingerprint:
4C23B19F 8CA3BCB3 216E4F5C 0FDC51D3 87381923

[2] Note: Attachments do not appear in all PDF programs. Please use Acrobat Reader if you do not see the attachment.

3.2.3 Supported standards

The key management of the e-mail gateway supports the following standards for encryption and decryption of e-mails:

Assymmetric encryption: RSA, DSA, El Gamal

Symmetric encryption: 3DES, Blowfish, Twofish, Cast5, AES, AES192, AES256, IDEA, Safer-SK128

Hash: SHA-256, SHA-384, SHA-512, RipeMD160, Tiger, Haval

4 Transmission of secret information

4.1 Sending from Audi to an external partner

Encryption with your personal S/MIME certificate is required for the transmission of secret information to you. To do this, you must send your public S/MIME certificate to your Audi contact or make it available for retrieval.

4.2 Sending from an external partner to Audi

Encryption with the S/MIME user certificate of the Audi recipient is required for the transmission of secret information to Audi. In this case, the decryption takes place with the recipient´s personal PKI card.

User-based S/MIME certificates for all employees of VW group can be obtained at https://certdist.volkswagen.de/faces/components/requestCert_USER.xhtml.

5 Sample TLS configuration for Postfix MTA

5.1 Introduction and demarcation

This description of a sample configuration of “mandatory secure high-ciphers STARTTLS” primarily refers to an MTA based on Postfix. It is intended to help administrators who would like to implement mandatory e-mail encryption to partner domains on the basis of STARTTLS. Even if the implementation is to be carried out with an MTA other than Postfix, it may provide useful tips.

This description does not claim to be correct or complete.

5.2 Technology

By default, Postfix supports sending of e-mails by TLS wherever possible (opportunistic encryption).

For remote stations with which communication via mandatory TLS has been agreed, the use of TLS with validation of the server certificate and verification of the common name ("Secure Channel TLS") is enforced by means of a policy. In this case we are talking about certified remote stations.

The identity of the certified remote stations is ensured by maintaining a manually updated compilation of CA certificates. In this regard, only those certificates are acceptable that use the CA exclusively for issuing holder-validated ("strongly validated") certificates.

The use of CA certificates used for domain and/or mail-validated ("weakly validated") certificates (e.g.: "SSL123" from Thawte) is not intended due to the vulnerability to DNS attacks.

5.3 What is Secure Channel TLS?

Secure Channel TLS not only checks whether the certificate is issued by a known CA, but it also ensures that the certificate used is issued to a common name in a specific domain (the destination domain or the domain that hosts the destination domain). This is used to head off a scenario whereby an attacker has a legitimate certificate issued to his own domain by one of the trusted CAs and then, as part of a DNS attack, pretends to the sender to be the e-mail server for one of the destination domains. Further information on this can be found in TLS_README from the Postfix Distribution in section ‘Secure server certificate verification’.

5.4 Key strength and encryption algorithms

At least TLS v1.2 with PFS or TLS v1.3 shall be used as encryption protocol. SSLv2 and SSLv3 are no longer supported due to weakness in the algorithms and in the implementation.

All the algorithms and key lengths that fall into the OpenSSL classification "High" are regarded as being adequately secure. Without exception these use session keys with a minimum length of 128 bit (256 bit recommended), provided that RC4 is not used as an encryption algorithm:

```
openssl ciphers -v -tls1 HIGH
```

5.5 Administration

The administration of the CA certificates and policy rules is controlled centrally via the management server.

5.6 TLS policy

The policy rules for enforcing TLS to certified remote stations are maintained on the management server in file /etc/postfix/tls_policy, e.g.:

```
example.com    secure match=.example.net ciphers=high
```

The syntax of this file is described in TLS_README from the Postfix distribution in section ‘Client TLS security levels’.

It is important to note the following here:

- secure enforces Secure Channel TLS for the domain.
- ciphers=high enforces the use of strong key lengths and algorithms. This is not set as the default value in the main.cf to ensure maximum compatibility in the case of opportunistic TLS.
- match=.example.net is used if the e-mail servers are located in a different domain than the mail domain. This match attribute is used when checking the common name.

5.7 CA certificates

The CA certificates are located in the directory /etc/postfix/cacerts.d.
CA certificates in X509 PEM format may only be added here after a thorough check for compliance with guidelines (strong validation).

5.8 Troubleshooting / monitoring

5.8.1 For outgoing e-mails

If the connection setup to a remote station fails, this will be reported by syslog.

```
Syslog message (Facility mail): "Server certificate could
not be verified"

Syslog message (Facility mail):
"smtp\[.*status=deferred..Cannot start TLS"

Syslog message (Facility mail):
"smtp\[.*status=deferred..TLS is required, but was not
offered"
```

Such log messages should lead to the administrators being alerted accordingly.

In the case of remote stations that only support opportunistic TLS, an entry may then be made in the tls_policy, which is used for disabling outgoing TLS for the destination domain in question:

```
example.de                    none
```

In the case of remote stations for which it has been agreed that secure e-mail exchange is a mandatory condition, it is compulsory to clarify why the connection setup fails. Disabling TLS is not permissible and, if TLS is no longer activated, an alternative method of securing the e-mail traffic must be established.

Please note: Outgoing e-mails that cannot be delivered are not bounced immediately if errors occur but remain in the queue up to the maximum holding time (maximal_queue_lifetime) before they are bounced.

5.8.2 For incoming e-mails

If the incoming connection setup fails, this will be reported by syslog.

```
Syslog message (Facility mail): "smtpd\[.*SSL_accept
error"
```

In order not to offer STARTTLS as a protocol option to these remote stations, it is possible to enter the client IP address in /etc/postfix/smtpd_discard_ehlo_keywords using the following format:

```
1.2.3.4                 STARTTLS
```

5.9 Postfix configuration guide

5.9.1 Basic configuration format

```
# TLS settings
smtp_tls_security_level     = may
smtp_tls_policy_maps        = hash:/etc/postfix/tls_policy
smtp_tls_CApath             = /etc/postfix/tls/cacerts.d
smtp_tls_loglevel           = 1
smtpd_tls_security_level    = may
smtpd_tls_cert_file         = /etc/postfix/tls/cert.pem
smtpd_tls_key_file          = /etc/postfix/tls/key.pem
smtpd_tls_loglevel          = 1
```

5.9.2 Sample TLS policy

```
# TLS Policy
#
# In cases where one or more MX host names are not

# within the destination e-mail domain, the entry

# "match=..." is necessary in order to assign the

# corresponding domain or FQHN to the destination domain.
#
hp.com          secure ciphers=high
audi.hu         secure match= .audi.de ciphers=high
mhp.de          secure ciphers=high
```

5.9.3 Generate CSR and key

```
cd /etc/postfix/tls/
export HOST=mailin1.audi.de

export DATE=$(date +%Y%m%d)
touch $HOST-key.$DATE.pem
chmod 600 $HOST-key.$DATE.pem
openssl req -config /etc/postfix/tls/openssl.cnf -newkey \
     rsa:1024 -out $HOST-req.$DATE.pem -nodes -keyout \
     $HOST-key.$DATE.pem
```

6 Sample TLS configuration for Microsoft Exchange (MSX)

6.1 Introduction and demarcation

This description of a sample configuration of “mandatory secure high-ciphers STARTTLS” primarily refers to an MTA of the type ‘Microsoft Exchange’ (MSX). It is intended to help administrators who would like to implement mandatory e-mail encryption to partner domains on the basis of STARTTLS. Even if the implementation is to be carried out with an MTA other than MSX, it may provide useful tips.

This description does not claim to being correct or complete.

6.2 Example

- Install certificate on the Exchange Server.
- Restart Exchange Server.
- After restarting, the available certificates will be visible.
- Open the Exchange System Manager.
- Click on “default SMTP Virtual Server”.
- Open ‘Properties’ and select options “Access” and “Secure Communication”.
- Select the matching certificate in “Certificate Wizard”.
- Accept the certificate, thus allowing Exchange Server to set up connections with and without TLS.
- Subsequently, it is possible to configure mandatory TLS for incoming or outgoing connections. Configuration for outgoing connections is recommended.

7 Attachments

7.1 Certificate Authorities

- Deutsche Telekom AG https://www.telesec.de/
- Entrust.net https://www.entrust.com/
- Equifax https://www.geotrust.com/
- GTE CyberTrust https://www.verizon.com/
- GlobalSign https://www.globalsign.com/
- QuoVadis https://www.quovadisglobal.com/
- Thawte https://www.thawte.com/
- VeriSign https://www.verisign.com/