AUDI AG

Hinweise zur E-Mail-Verschlüsselung mit der AUDI AG

Autor: AUDI AG IT-Security
Version: 3.1
Stand: 04/2023

Inhaltsverzeichnis

1 E-Mail-Verschlüsselung bei Audi

1.1 Einleitung

Die Übertragung von E-Mails über das Internet ist ab der Stufe „vertraulich“ von und zur AUDI AG nur verschlüsselt zulässig. Die Beurteilung, ob derartige Daten vorliegen, erfolgt durch den Anwender selbst. Es ist dabei ein strenger Maßstab anzulegen.

Falls als „vertraulich“ oder höher eingestufte Daten per E-Mail mit der AUDI AG ausgetauscht werden, ist ein geeignetes Verschlüsselungsverfahren einzusetzen.

1.2 Eingesetzte Technik bei der AUDI AG

Die AUDI AG bietet zur sicheren Übertragung von vertraulichen E-Mails folgende Verfahren an. Diese sind als Standardtechnologien vom Verband der Automobilindustrie (VDA) empfohlen.

Für **vertrauliche** E-Mails **von Audi zum externen Partner**

- Transportverschlüsselung zwischen den E-Mail-Gateways mittels TLS im „mandatory“ Modus (bevorzugt)
- Verschlüsselung der E-Mails am E-Mail-Gateway der AUDI AG mittels PGP auf Basis von User- und Domain-Keys
- Verschlüsselung der E-Mails am E-Mail-Gateway der AUDI AG mittels S/MIME auf Basis von User- und Domain-Zertifikaten
- Ende-zu-Ende Verschlüsselung der E-Mails auf Basis von S/MIME User-Zertifikaten

Zusätzlich können als vertraulich klassifizierte Anlagen in E-Mails (z.B. Dokumente oder Dateien) durch Microsoft RMS (Rights Management Services) geschützt sein.

Informationen zum Umgang mit RMS geschützten vertraulichen Informationen finden Sie auf der ONE.Konzern Business Plattform (https://vwgroupsupply.com/) unter Informationen -> Sicherheit in der Zusammenarbeit -> Anforderungen Informationssicherheit und IT-Sicherheit.

Für **vertrauliche** E-Mails **vom externen Partner zu Audi**

- Transportverschlüsselung zwischen den E-Mail-Systemen mittels TLS im „mandatory“ Modus (bevorzugt)
- Verschlüsselung der E-Mails mittels PGP auf Basis von User- und Domain-Keys und Entschlüsselung am E-Mail-Gateway der AUDI AG
- Verschlüsselung der E-Mails mittels S/MIME Domain-Zertifikat und Entschlüsselung am E-Mail-Gateway der AUDI AG
- Ende-zu-Ende Verschlüsselung der E-Mails auf Basis von S/MIME User-Zertifikaten

Für die Übertragung **geheimer** E-Mails ist ausschließlich eine Ende-zu-Ende Verschlüsselung auf Basis von S/MIME User-Zertifikaten zulässig.

2 TLS

2.1 Überblick

Bei TLS handelt es sich um ein Verfahren zur Verschlüsselung der Kommunikation zwischen zwei E-Mail-Gateways (MTA, Mail Transfer Agent) auf Applikationsebene (Transportverschlüsselung). Die Verbindung zwischen den E-Mail-Gateways wird unverschlüsselt auf Port 25 aufgebaut und zur Laufzeit auf verschlüsselte Kommunikation umgeschaltet.

Da TLS auf das SMTP-Protokoll aufbaut, bleiben ggf. vorhandene Redundanzlösungen, z.B. in Form mehrerer E-Mail-Gateways und Internetanbindungen, weiterhin voll nutzbar.

Zu beachten ist dabei jedoch, dass das E-Mail-Gateway des Kommunikationspartners in dessen Geschäftsräumen aufgestellt sein sollte. Bei Verwendung des E-Mail-Gateways eines Providers (z.B. Microsoft 365) muss sichergestellt sein, dass entsprechende vertragliche Vereinbarungen mit dem Provider zum Schutz der Daten abgeschlossen sind.

Die Kommunikation zu Back-End-Systemen oder Endgeräten muss in adäquater Weise gesichert sein.

Zur Verschlüsselung muss mindestens TLS v1.2 mit PFS (Perfect Forward Secrecy) oder TLS v1.3 eingesetzt werden[1].

Für den E-Mail-Austausch mittels TLS sind folgende Konfigurationsschritte auf den internetseitigen E-Mail-Gateways durchzuführen:

- Empfang von E-Mails:
  - Aktivierung von TLS beim E-Mail-Empfang.
  - Hinterlegung eines geeigneten Server-Zertifikats.

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

- Versand von E-Mails:
    - Aktivierung von TLS beim E-Mail-Versand.
    - Aktivierung einer Policy zur Erzwingung von TLS beim Versand von E-Mails an Audi Domains.
    - Hinterlegung der zur Überprüfung der Audi Zertifikate erforderlichen CA-Zertifikate.

2.2 Versand von Audi zum externen Partner

Beim Versand an Sie als Partner erwarten wir die folgenden Rahmenbedingungen:

- Als Protokoll kommt SMTP mit STARTTLS zum Einsatz.
- Der Versand von E-Mails per SMTPS auf Port 465 wird nicht unterstützt.
- Es wird nur an Gegenstellen ausgeliefert, die Session-Keys mit einer Länge ab 128 Bit unterstützen.
- Die Verschlüsselung unterstützt mindestens TLSv1.2 mit PFS oder TLS v1.3.
- Die Common Names (CN) der verwendeten Zertifikate müssen jeweils den Hostnamen der E-Mail-Gateways entsprechen, auf denen sie hinterlegt sind.
- Aussteller der Zertifikate muss eine Certificate Authority (CA) sein, deren Zertifikat und Zertifizierungspolicy für uns überprüfbar sind (Beispiele siehe 7.1 Certificate Authorities).
- Zu erfüllende Sicherheitsstufe des Zertifikates: mindestens Class 1 oder Domain Validation (DV).
- Das von der CA verwendete Zertifikat (Root CA Zertifikat, Issuing CA Zertifikat) darf ausschließlich zur Ausstellung von Zertifikaten verwendet werden, bei denen die Identität des Inhabers validiert wurde.
- Selbstsignierte Zertifikate können nicht unterstützt werden.

2.3 Versand vom externen Partner zu Audi

Beim Versand von E-Mails an die Audi E-Mail-Gateways sollten Sie folgendes beachten:

- Als Protokoll kommt SMTP mit STARTTLS zum Einsatz.
- Der Empfang von E-Mails per SMTPS auf Port 465 wird nicht unterstützt.
- Es werden nur Session-Keys mit einer Länge ab 128 Bit unterstützt.
- Zur Verschlüsselung wird mindestens TLS v1.2 mit PFS oder TLS v1.3 eingesetzt.
- Die Common Names (CN) der bei Audi verwendeten Zertifikate entsprechen jeweils den Hostnamen der E-Mail-Gateways, auf denen sie hinterlegt sind.
- Die Hostnamen der E-Mail-Gateways und damit auch die CN-Einträge der Zertifikate entsprechen dem folgenden Muster, das Sie bei der E-Mail-Auslieferung prüfen sollten:
    - mailin*.audi.de
- Aussteller der Zertifikate bei Audi ist derzeit QuoVadis Global SSL ICA G3 (https://www.quovadisglobal.com/download-roots-crl/).
- Bitte konfigurieren Sie Ihre E-Mail-Server so, dass der E-Mail-Versand an die von Ihnen verwendeten Audi-Domains zwingend mit TLS erfolgt.
- Die folgende Liste von Audi-Domains kann als Grundlage für die Erstellung einer entsprechenden Policy verwendet werden:
    - audi.de
    - audi.hu

Audi erzwingt kein TLS beim Empfang von E-Mails aus Ihrer Domain. Es muss jedoch von Ihrer Seite sichergestellt sein, dass vertrauliche E-Mails nicht über unverschlüsselte Verbindungen gesendet werden.

2.4 Vorgehensweise

Bitte fordern Sie das entsprechende Change Request Formular bei Ihrem Audi Kontakt an. Das ausgefüllte Formular senden Sie bitte an Ihren Audi Kontakt zurück.

3 Verschlüsselung am E-Mail-Gateway

3.1 Versand von Audi zum externen Partner

Um alle vertraulichen E-Mails an Sie vor dem Versand verschlüsseln zu können, benötigen wir Ihren PGP-Public-Key (User oder Domain) oder Ihr S/MIME-Zertifikat (User oder Domain).

Senden Sie hierzu bitte eine E-Mail mit dem entsprechenden PGP-Public-Key bzw. eine signierte E-Mail mit dem entsprechenden öffentlichen S/MIME-Zertifikat an Ihren Audi Kontakt.

3.2 Versand vom externen Partner zu Audi

Für die E-Mail-Verschlüsselung nutzen Sie bitte unseren PGP-Domain-Key oder unsere S/MIME-Zertifikate (User oder Domain).

Userbezogene S/MIME Zertifikate für Mitarbeitende des VW Konzerns können Sie über folgende URL abrufen:
https://certdist.volkswagen.de/faces/components/requestCert_USER.xhtml

3.2.1 S/MIME Domain Zertifikat

Das Audi S/MIME Domain Zertifikat ist diesem Dokument als Anlage **Audi_SMIME_Container.p7b** beigefügt.[2]

3.2.2 PGP Domain Key

Der Audi PGP Domain Key ist diesem Dokument als Anlage **Audi_PGP_Domainkey.asc** beigefügt.[2]

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

[2] Hinweis: Anlagen werden nicht in allen PDF-Programmen angezeigt. Bitte verwenden Sie Acrobat Reader, falls Sie die Anlage nicht sehen.

3.2.3 Unterstützte Standards

Das Key Management des E-Mail-Gateways unterstützt für das Ver- und Entschlüsseln von E-Mails folgende Standards:

Asymmetrische Verschlüsselung: RSA, DSA, El Gamal

Symmetrische Verschlüsselung: 3DES, Blowfish, Twofish, Cast5, AES, AES192, AES256, IDEA, Safer-SK128

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

4 Übertragung von geheimen Informationen

4.1 Versand von Audi zum externen Partner

Für die Übertragung von geheimen Informationen an Sie ist eine Verschlüsselung mit Ihrem persönlichen S/MIME Zertifikat erforderlich. Hierzu müssen Sie Ihrem Audi Kontakt Ihr öffentliches S/MIME Zertifikat übermitteln oder zum Abruf bereitstellen.

4.2 Versand vom externen Partner zu Audi

Für die Übertragung von geheimen Informationen an Ihren Audi Kontakt ist eine Verschlüsselung mit dem persönlichen S/MIME Zertifikat des Audi Kontaktes erforderlich. Die Entschlüsselung erfolgt in diesem Fall mit dem persönlichen PKI-Ausweis des Audi Kontaktes.

Userbezogene S/MIME Zertifikate für Mitarbeitende des VW Konzerns können Sie über folgende URL abrufen:
https://certdist.volkswagen.de/faces/components/requestCert_USER.xhtml

5. TLS-Beispielkonfiguration für Postfix MTA

5.1 Einleitung und Abgrenzung

Die hier vorliegende Beschreibung einer Beispielkonfiguration von „mandatory secure high-ciphers STARTTLS“ bezieht sich primär auf einen MTA vom Typ Postfix. Es soll als Starthilfe und Hinweis für Administratoren dienen, die eine zwingende E-Mail-Verschlüsselung zu Partnerdomains auf Basis STARTTLS umsetzen möchten. Auch wenn die Umsetzung mit einem anderen MTA als Postfix erfolgen soll, kann es wertvolle Hinweise liefern.

Diese Beschreibung erhebt weder einen Anspruch auf Richtigkeit noch auf Vollständigkeit.

5.2 Technologie

Postfix verschlüsselt standardmäßig mit TLS, soweit möglich (opportunistische Verschlüsselung).

Für Gegenstellen, mit denen die Kommunikation per mandatory TLS vereinbart wurde, wird mittels einer Policy-Regel die Verwendung von TLS mit Validierung des Serverzertifikats und Prüfung des Common Name ("Secure Channel TLS") erzwungen. Wir sprechen in diesem Fall von zertifizierten Gegenstellen.

Die Identität der zertifizierten Gegenstellen wird sichergestellt, indem eine von Hand gepflegte Zusammenstellung von CA-Zertifikaten erstellt wird. Akzeptabel sind dabei nur Zertifikate, bei denen die CA ausschließlich zur Ausstellung inhabervalidierter ("stark validierter") Zertifikate verwendet wird.

Die Nutzung von CA-Zertifikaten, die für domain- bzw. mailvalidierte ("schwach validierte") Zertifikate verwendet werden (z.B.: "SSL123" von Thawte), ist aufgrund der Angreifbarkeit durch DNS-Attacken nicht vorgesehen.

5.3 Was heißt Secure Channel TLS?

Bei Secure Channel TLS wird nicht nur geprüft, ob das Zertifikat von einer bekannten CA ausgestellt ist, sondern es wird darüber hinaus sichergestellt, dass das verwendete Zertifikat auf einen Common Name in einer bestimmten Domain (der Zieldomain oder der Domain, die die Zieldomain hostet) ausgestellt ist. Hiermit wird ein Szenario abgefangen, bei dem sich ein Angreifer von einer der vertrauten CAs ein legitimes Zertifikat auf seine eigene Domain ausstellen lässt und dann im Rahmen eines DNS-Angriffs dem Absender vorgibt, er sei E-Mail-Server für eine der Zieldomains. Näheres dazu findet sich in TLS_README aus der Postfix-Distribution unter Secure server certificate verification.

5.4 Schlüsselstärke und Verschlüsselungsalgorithmen

Als Verschlüsselungsprotokoll müssen mindestens TLSv1.2 mit PFS oder TLS v1.3 zum Einsatz kommen. SSLv2 und SSLv3 werden aufgrund von Schwächen der Algorithmen und in der Implementierung nicht mehr unterstützt.

Es werden alle von der OpenSSL-Klassifizierung "High" umfassten Algorithmen und Schlüssellängen als ausreichend sicher betrachtet. Diese verwenden ausnahmslos Session-Keys mit einer Länge von mindestens 128 Bit (empfohlen sind 256 Bit), soweit nicht RC4 als Verschlüsselungsalgorithmus verwendet wird:

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

5.5 Administration

Die Verwaltung der CA-Zertifikate und die Policy-Regeln werden zentral über den Management-Server gesteuert.

5.6 TLS-Policy

Die Policy-Regeln für die Erzwingung von TLS zu zertifizierten Gegenstellen werden auf dem Management-Server in der Datei /etc/postfix/tls_policy gepflegt, z.B.:

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

Die Syntax dieser Datei ist in TLS_README aus der Postfix-Distribution unter dem Punkt Client TLS security levels beschrieben.

Zu beachten ist dabei:

- secure erzwingt Secure Channel TLS für die Domain.
- ciphers=high erzwingt die Verwendung starker Schlüssellängen und -algorithmen. Dies ist nicht als Defaultwert in der main.cf gesetzt, um maximale Kompatibilität bei opportunistischem TLS zu gewährleisten.
- match=.example.net kommt zum Einsatz, wenn die E-Mail-Server sich in einer anderen Domain befinden als die Maildomain. Gegen dieses match-Attribut wird die Überprüfung des Common Name durchgeführt.

5.7 CA-Zertifikate

Die CA-Zertifikate befinden sich im Verzeichnis /etc/postfix/cacerts.d. CA-Zertifikate im X509-PEM-Format dürfen hier ausschließlich nach eingehender Prüfung auf Richtlinienkonformität (starke Validierung) hinzugefügt werden.

5.8 Fehlerbehandlung / Monitoring

5.8.1 Bei ausgehenden E-Mails

Wenn der Verbindungsaufbau zu einer Gegenstelle fehlschlägt, wird dies per syslog gemeldet.

```
Syslog-Meldung (Facility mail): "Server
certificate could not be verified"
Syslog-Meldung (Facility mail):
"smtp\[.*status=deferred..Cannot start TLS"
Syslog-Meldung (Facility mail):
"smtp\[.*status=deferred..TLS is required, but was
not offered"
```

Derartige Logmeldungen sollten zu einer entsprechenden Alarmierung der Administratoren führen.

Bei Gegenstellen, für die nur opportunistisches TLS unterstützt wird, erfolgt dann ggf. ein Eintrag in der tls_policy, mit dem ausgehendes TLS für die gegebene Zieldomain deaktiviert wird:

```
example.de      none
```

Bei Gegenstellen, mit denen der zwingend abzusichernde Austausch von E-Mails vereinbart ist, muss geklärt werden, warum der Verbindungsaufbau fehlschlägt. Eine Deaktivierung von TLS ist nicht zulässig, sondern es muss, falls TLS nicht mehr zum Laufen gebracht wird, eine alternative Methode zur Sicherung des E-Mail-Verkehrs etabliert werden!

Bitte beachten: Ausgehende E-Mails, die nicht zugestellt werden können, werden bei Fehlern nicht sofort gebounced, sondern bleiben bis zur maximalen Haltezeit (maximal_queue_lifetime) in der Queue, bevor sie gebounced werden.

5.8.2 Bei eingehenden E-Mails

Wenn der Verbindungsaufbau eingehend fehlschlägt, wird dies per syslog gemeldet:

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

Um diesen Gegenstellen kein STARTTLS als Protokolloption anzubieten, kann nach folgendem Muster ein Eintrag der Client-IP-Adresse in /etc/postfix/smtpd_discard_ehlo_keywords erfolgen:

```
1.2.3.4 STARTTLS
```

5.9 Konfigurationsleitfaden Postfix

5.9.1 Basis-Konfigurationsmuster

```
# TLS settings
smtp_tls_security_level = may
smtp_tls_policy_maps = ash:/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 TLS-Policy-Beispiel

```
# TLS Policy
#
# In Faellen, wo ein oder mehr MX-Hostnamen nicht
# innerhalb der Ziel-Emaildomain liegen, ist die
Angabe
# "match=..." erforderlich, um die entsprechende
Domain
# oder den FQHN der Zieldomain zuzuordnen.
#
hp.com    secure ciphers=high
audi.hu   secure match= .audi.de ciphers=high
mhp.de    secure ciphers=high
```

5.9.3 CSR und Key generieren

```
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 TLS-Beispielkonfiguration für Microsoft Exchange (MSX)

6.1 Einleitung und Abgrenzung

Die hier vorliegende Beschreibung einer Beispielkonfiguration von „mandatory secure high-ciphers STARTTLS“ bezieht sich primär auf einen MTA vom Typ Microsoft Exchange (MSX). Es soll als Starthilfe und Hinweis für Administratoren dienen, die eine zwingende E-Mail-Verschlüsselung zu Partnerdomains auf Basis STARTTLS umsetzen möchten. Auch wenn die Umsetzung mit einem anderen MTA als MSX erfolgen soll, kann es wertvolle Hinweise liefern.

Es erhebt weder einen Anspruch auf Richtigkeit noch auf Vollständigkeit noch darauf, ein zu jeder Zeit gültiges Beispiel einer Konfiguration im Sinne des oben genannten Dokuments zu sein.

6.2 Beispiel

- Zertifikat auf dem Exchange Server einspielen.
- Exchange Server neu starten.
- Nach dem Neustart sind die verfügbaren Zertifikate sichtbar.
- Öffnen des Exchange System Managers.
- Anklicken von „default SMTP Virtual Server“.
- Eigenschaften öffnen und zum Eintrag “Access” und “Secure Communication” wechseln.
- Auswahl des passenden Zertifikats in „Certificate Wizard“.
- Übernahme vom Zertifikat, danach kann der Exchange Server Verbindungen mit TLS und ohne TLS herstellen.
- Im Anschluss daran kann mandatory TLS für eingehende oder ausgehende Verbindungen konfiguriert werden. Empfohlen ist die Konfiguration für ausgehende Verbindungen.

7 Anlagen

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/