AUDI AG

Hinweise zur E-Mail-Verschlüsselung mit der AUDI AG

Autor: Audi IT Sicherheit
Version: 1.2
Datum: 06.06.2019

Inhaltsverzeichnis

1 E-Mail-Verschlüsselung bei Audi

1.1 Einleitung

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

Falls Daten per E-Mail mit der AUDI AG ausgetauscht werden, die unter einer der oben beschriebenen Rubriken einzuordnen sind, 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, die als Standardtechnologies vom Verband der Automobilindustrie (VDA) empfohlen werden:

- Transportverschlüsselung zwischen den E-Mail-Systemen (TLS im „mandatory“ Modus) (bevorzugt)
- Verschlüsselung der E-Mails am E-Mail-Verschlüsselungsgateway mittels PGP oder S/MIME (auf Basis von Domain-Keys)
- Ende-zu-Ende Verschlüsselung der E-Mails auf Basis von S/MIME (z. B. für geheime Informationen)

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

Bei den für den E-Mail-Austausch per TLS vorzunehmenden Konfigurationsschritten auf den internetseitigen E-Mail-Gateways (E-Mail-Server) handelt es sich im Wesentlichen um die folgenden:

- Empfang von E-Mails:
    - Aktivierung von TLS beim E-Mail-Empfang.
    - Hinterlegung eines geeigneten Server-Zertifikats. Es wird ein Extended Validation (EV) Zertifikat benötigt.

- Versand von E-Mails: o Aktivierung von TLS beim E-Mail-Versand.
    - Aktivierung einer Policy, aufgrund derer der E-Mail-Versand an Audi Domains ausschließlich per TLS erlaubt wird.
    - Hinterlegung entsprechender CA-Zertifikate zwecks Überprüfung der Audi 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 mit RC4 wird nicht unterstützt. Dies betrifft insbesondere ältere Versionen von Microsoft Exchange.
- 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 namhafte Certificate Authority (CA) sein, deren Zertifikat und Zertifizierungspolicy für uns überprüfbar sind (siehe Anlage).
- Die Validierung des Zertifikatsinhabers darf bei der CA nicht per E-Mail-Robot o.ä. erfolgen, sondern muss anhand von Dokumenten durchgeführt werden (Extended Validation Zertifikat).

- Das von der CA verwendete Zertifikat (Root CA Zertifikat, Issuing CA Zertifikat) darf ausschließlich zur Ausstellung dokumentenvalidierter Zertifikate verwendet werden.
- Das Zertifikat darf nicht auf einen Domain- oder Hostnamen, sondern muss namentlich auf den Zertifikatsinhaber ausgestellt sein.
- Selbstsignierte Zertifikate können nicht unterstützt werden.
- Da derzeit noch nicht auszuschließen ist, dass E-Mails mit Audi Absenderadressen durch Dritte versendet werden, bitten wir Sie, sicherzustellen, dass auch in Zukunft weiterhin E-Mails auf unverschlüsseltem Wege angenommen werden.
- Zu erfüllende Sicherheitsstufe: mindestens Class 3 oder Extended Validation (EV).

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.
- Die Verschlüsselung mit RC4 wird nicht unterstützt. Dies betrifft insbesondere ältere Versionen von Microsoft Exchange.
- 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: o mailin*.audi.de
- Aussteller der Zertifikate bei Audi ist derzeit die VeriSign CA.
- 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 nicht TLS beim Empfang von E-Mails aus Ihrer Domain, so dass Sie auch weiterhin unverschlüsselt E-Mails an uns senden können, z.B. von anderen Standorten aus. Es muss jedoch von Ihrer Seite sichergestellt sein, dass vertrauliche E-Mails nicht über unverschlüsselte Verbindungen gesendet werden.

2.4 Vorgehensweise

Senden Sie bitte ein ausgefülltes Change Request Formular an Ihren Audi Ansprechpartner zurück.

3 Verschlüsselung am E-Mail-Verschlüsselungsgateway

3.1 Versand von Audi zum externen Partner

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

3.2 Versand vom externen Partner zu Audi

Für die E-Mail-Verschlüsselung nutzen Sie bitte unseren PGP-Domain-Key oder S/MIME-Zertifikat (User oder Domain). Userbezogene S/MIME Zertifikate für Mitarbeiter des VW Konzerns können Sie unter der URL https://certdist.volkswagen.de/requestCert.jsp?mode=usercert

3.2.1S/MIME Domain Zertifikat

3.2.2PGP Domain Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: CryptoEx OpenPGP Engine Version 2.1
Comment: AUDI AG securEmail <http://www.audi.de>
mQENBExRbHkBCACDv1WF6kWu8Sa3AZuzsyYa3RjT1RXFU62XN4yBEwULjy9j/7+V
P1o0777/YtyCwPYqBCGQrG2oHKT1+tvVXst+UvDoeKNK8tQ0weYfT8474GQgrAvT
TkB4It7XqNMHn7SqRoWryazK/f4fM8ZoUXV4TjXCE28YlFizmzuWGI60RoxM/byL
LhaqQpXji5K2t15KbwbkGV6xNogHUZe7Qbna+4SA1W/z6WHO/JAHSz0gT1Q+ZQwW
lf/ettGmna28240Aw4X0wP9kQ3SjKwazB324ylJSx72xajqSfdj0JfLq7R/s2nuh
i6z07m7V+UajA17LvhH2RdvZxo64L1v+WPA5ABEBAAG0S0FVREkgQUcgc2VjdXJF
bWFpbCBQR1AgRG9tYWluIEtleSAoc2VjdXJlbWFpbEBhdWRpLmRlKSA8c2VjdXJl
bWFpbEBhdWRpLmRlPokBHAQTAQIAEAUCTFFseQkQD9xR04c4GSMAAJHRB/4wdx5T
Yebt5Pjw733yo/zw9HPsZ67ANu0/ADq/W+A0II4ViLo6+P1uQQmkTUQfGUBAQwLA
GJ3Hlz3j56+7vbTo5qQsw8A9QmD44w3t/4BpCEk52UufqTDqmynyiQR2DaShuSdo
5r7daiurzPJPoOAO0DkYqOUZ8ifn9f+AwCYfWTVF7lutlWYdNd9xjgx+G+pWfIsx
M3vb3Czsj3bWqLhPzZzgggggkZWi1iD7a0nhcj2IO2SJnhXw5E0pvpFTHxkXJxfL5
f1m5sUcRnkkx0SA5tJZZm77PuETYqTmspzMrl6UjsZolEdbB/ur+uCUrJSc4FpP3
6cgvucZYnY2k5lzTiQEcBBMBAgAQBQJMUWx5CRC34DH/HghktgAAZWUH/i+pLRJJ
C6f+6wgSjw6UvGtTSpheM4gVMs2K+yMesnFRdTPVufpfjohWXrjEaEHhcghksCgU
Q+3X1AnZG2AaP+lxyQzTmZWKYBAcLiZ0lSyOcN8xn0yitbZqaSYbJY0B8p4kOPED
BxV5e0ECGy6HWCItIa6q7ZQ4z7+ZMHU+DBFowMn5ErKUTxML/nqOTGn+VZOlPfCZ
dMYiqziy9Z5i+33KFIGfu7zlBFEV3w2mujtHWUnpEa8pfBLYXZcWd8hS50Ly0Q+T
HWfOR4iS/bqnvBJR/c+/rYIxwzdbVxVs7bd3rJq5pZFctNUHNi38qk5ccoXCKTfS
pfCC0WDvJE/Qv2a5AQ0ETFFseQEIAIO/VYXqRa7xJrcBm7OzJhrdGNPVFcVTrZc3
jIETBQuPL2P/v5U/WjTvvv9i3ILA9ioEIZCsbagcpPX629Vey35S8Oh4o0ry1DTB
5h9PzjvgZCCsC9NOQHgi3teo0weftKpGhavJrMr9/h8zxmhRdXhONcITbxiUWLOb
O5YYjrRGjEz9vIsuFqpCleOLkra3XkpvBuQZXrE2iAdRl7tBudr7hIDVb/PpYc78
kAdLPSBPVD5lDBaV/9620aadrbzbjQDDhfTA/2RDdKMrBrMHfbjKUlLHvbFqOpJ9
2PQl8urtH+zae6GLrPTubtX5RqMDXsu+EfZF29nGjrgvW/5Y8DkAEQEAAYkBHAQY
AQIAEAUCTFFseQkQD9xR04c4GSMAACF6B/4oU3Y5ISU8XmGCFyb1MLAR+GtOZV++
qytqtv7Hc8I2TQpj0jPWM6/xf29+UcU7Nht+2Itj7n6ERHbcAkEDo29P0cABnTlF
GTjXPSeOhRVEgC2C19zV2NUKymBeH3JkG/uaroPLXoiw2E/fCyfWXgR3yHZHimcT
P361qRZYJLAZeKcV5D0QjgU4yrH73P3f3Y3oBGoK2wJ1TF9m6g14v+Hxdkm/8nJc
lV9sxDiZvGE6Z3DeN2oMix+QekTuN2n9HezFvyEpyPzk4FQK0hmQqxadlAYw4R9W
I1qyD0Y1u8iQXxOp3EBUiVZWADaXNs5b/tL5TSwVyiOQ6TCqnDizttK6mQENBExR
avoBCACJGc4owyf8QHb9Sa6IphBxfDdkCj8LLo0+innJ1mD2j1vpr+9NGKBoEDRT
Q9qCHZ1N5vgM7fu3GOFj8gjqEsxcjO/n61MpQU44eQ3BSJsVCLO3ppP5mZ1tLkpv
htZY81NruF+mS5MD0kDujOhl3ze+WMgRScf5GruwY6jY4QR2nwp1k++yVcSeR32n
rmKuQWQCByS2HJuLMGPthlE4rqMq+qbl9gY8zJycMUgJmpKq6nxfcCpKQEIk3TCd
jq+o7KtAar2ICjJakLIO/ww0xfNHlHvXf7Q/Yz2EU1uByoeVgy2U1NhTA9jBCM0b
3FCqU38NM5grylhvo/uqVcRZ5S8dABEBAAG0N0FVREkgQUcgc2VjdXJFbWFpbCBQ
R1AgU2lnbmluZyBLZXkgPHNlY3VyZW1haWxAYXVkaS5kZT6JARwEEAECABAFAkxR
avoJELfgMf8eCGS2AADgygf/Y1WCCsMGNt8fuNbHtcWhs+JIDDwZ/7lXOHorqxlG
uwseEFAcIo5K3jIpRuSMWguLo4zYYzKhowKUlRlR1i50dgPSwUlfFHNQu2uo5vFG
30OchjGkhclaMy7sGeg7kqXsBJ6NjavpjhyU5AyFtZa0rPDKBok5E9sZ6wG+5gwZ
m+U0RX8m6Om3UdHt2SQeUPeddcl4ypZx9xJqFTy5xWyN7bQPdhnPXvP3TeYWg54Y
lQtE0dXZAjotFv7use0kQif3OTT2Umq4gNwW6r0S5APLqSNKEcQhyYoV133+O58L
D1KooIdRw1B5Wys3HDNZ/9JGSZJW2tr6jy8Qz8BIaoXMSYkBHAQTAQIAEAUCTFFq
+gkQt+Ax/x4IZLYAABLEB/0bW8pMxcBt7y9cRSMnwTzhQK6gOoaeMAqTX5HX7ZBM
DcIR9osJoZAiq9FeBMmetTlSQgrbZfdFiNgC9IZPEmBMeAUQRvjxRcG1YpSlr2oq
```

```
HG0Zdjdy1XSFWCj7iyddqsXSuvWIult6U8PRWfTN7Ii4BCEAiRwyPeYNW9gp/zu2
Fa30I5kXVtYwDHVIizViXNWr7xtr4sEvOJKZomrUR9JcjOg4PMmBwl52gx3m9+3d
39lrQLa2PvzvtfH4INDI5LXo4o/T6xX68mqwb/f8I8vF2lh64g1VDy7b1uhNBDqz
BOfxoQpfPXrucdP/sZw9cOyx5GsZaaQKiPTjnIjexK7/iQBKBBARAgAUBQJMUYTh
CRB/Q2eJtAtiPwMFAXgAAF9kAJsGA/VLpJ+q+uJ5mQI/bx7/1B0+eQCfVIOYAXU4
qpYKS+tEQ9sFw5V+7mA=
=+B6E
-----END PGP PUBLIC KEY BLOCK-----
```

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

4 Übertragung der geheimen Information

4.1 Versand vom externen Partner zu Audi

Für die Übertragung von geheimen Informationen ist eine Verschlüsselung mit einem persönlichen Zertifikat des Empfängers erforderlich. Die Entschlüsselung erfolgt in diesem Fall mit dem persönlichen PKI-Ausweis des Empfängers.

Nutzen Sie diese Variante insbesondere bei der Übertragung von geheimen Informationen.

URL:
https://certdist.volkswagen.de/requestCert.jsp?mode=usercert

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.

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.

5.2 Technologie

Der E-Mail-Versand per TLS ist beim Postfix-MTA ab Version 2.3 implementiert. Standardmäßig wird mit TLS verschlüsselt, wo möglich (opportunistische Verschlüsselung).

Für Gegenstellen, mit denen die Kommunikation per 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 gepflegt wird. Akzeptabel sind dabei nur Zertifikate, die die CA ausschließlich zur Ausstellung inhabervalidierter ("stark validierter") Zertifikate verwendet.
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 sollte nur noch TLSv1.2 zum Einsatz kommen. SSLv2 und SSLv3 werden aufgrund von Schwächen der Algorithmen und in der Implementierung nicht mehr unterstützt.

Es werden alle von den 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 Policy-Regeln wird zentral über dem 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.

(Eine Diskussion darüber, warum es kein Problem ist, in der tls_policy auch lokale, selbst gehostete Domains einzutragen (und somit keine unterschiedliche tls_config für die verschiedenen Gateways zu pflegen), findet sich im Postfix-Users-Archiv vom 22.03.2007.)

5.7 CA-Zertifikate

Die CA-Zertifikate befindet 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

5.8.1Bei 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 zwingend 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.

5.8.2Bei 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

5.9.1Basis-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
```

5.9.2TLS-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
```

5.9.3CSR 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.

6.3 Microsoft Exchange RC4 Problem

Die Verwendung der nicht als "High" klassifizierten RC4-Algorithmen ist für diese Zwecke nicht hinreichend.
Microsoft Exchange 2003 unterstützt beispielsweise nur RC4-MD5 und ist daher als MTA in diesem Sinne ungeeignet.
Die Aktivierung des benötigten Algorithmus bei diversen Microsoft Betriebssystemen – und entsprechend aktuellen MSX-MTAs ist jedoch scheinbar möglich und in einem Artikel von MS beschrieben:
http://support.microsoft.com/kb/811833/en-us

7 Anlagen

7.1 Certificate Authorities

- Deutsche Telekom AG http://www.telesec.de/
- Entrust.net http://www.entrust.net/
- Equifax http://www.geotrust.com/
- GTE CyberTrust http://www.verizonbusiness.com/
- GlobalSign http://www.globalsign.com/
- TC TrustCenter http://www.trustcenter.de/
- Thawte http://www.thawte.com/
- VeriSign http://www.verisign.com/