E-Mail Security

White Paper

Version: 1.2
Date: 2010-11-12
Classification: öffentlich/public

VDA
Verband der
Automobilindustrie

Foreword

On the initiative of a group of German vehicle manufacturers, in 2009 work started on preparing a series of white papers on “E-Mail Security.”

These documents have now been drawn up. They are:

- an introductory document entitled **“E-Mail Security”** which introduces the reader to the topic of “maintaining confidentiality when exchanging e-mail,”
- a white paper entitled **“Encryption of E-Mail Transport”** which describes, in generally transparent terms, pragmatic basic security achieved with transport encryption,
- a white paper entitled **“E-Mail Encryption Using End-to-End Encryption and Mail Transfer Agents”** and
- a white paper entitled **“Certificate and Trust Management - Requirements for certificates and trust relationships”.**

These documents provide the automotive industry with an orientation based on existing technical approaches. Two major factors here are usability, and application of the classification levels customary in the industry along with measures derived from them.

The VDA recommends its members to use these documents for orientation and to implement the measures described in their companies.

Contents

Introduction

Motivation

E-mail traffic harbors numerous risks in today’s business world. Alongside unwanted mass e-mails (spam) and the spread of malware, with commercial e-mail traffic there is also a risk that the data being exchanged could be revealed or falsified.

The European vehicle manufacturers have formed a Working Group “E-Mail Security” that aims to describe best practices for e-mail security. These best practices serve to ensure that e-mail messages are exchanged securely between organizations. This document and the other applicable white papers therefore present solutions with the aim of enabling the vehicle manufacturers and their partners to engage in secure e-mail communication.

These documents focus on protecting confidentiality by means of encryption, and not on creating trust by signing the mail.

Context and architecture

Several levels of e-mail security are presented below, followed by brief descriptions of the use cases. We also refer to the further information in the other white papers.

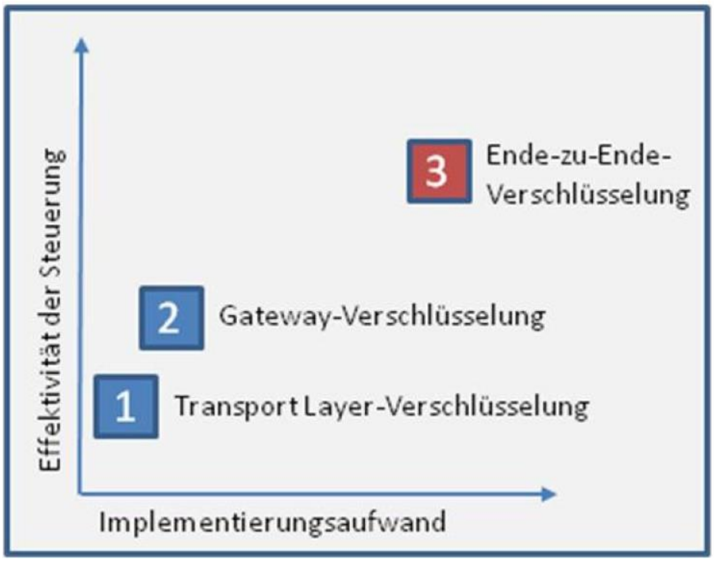
3 Ende-zu-Ende-Verschlüsselung
2 Gateway-Verschlüsselung
1 Transport Layer-Verschlüsselung
Effektivität der Steuerung
Implementierungsaufwand

*Figure 1: Initial context and architecture*Legenden:

Legenden: Effectiveness of control Input for implementation

1 End-to-end encryption 2 MTA encryption 2 Transport layer encryption

The solutions described here differ in their complexity, the input required for implementation, and the effectiveness of the control measures. The objective of all the solutions is to provide an appropriate degree of security for exchanging e-mail.

All the proposed solutions were selected with the aim of generally protecting investments already made, being interoperable and increasing acceptance among users.

End-to-end encryption offers the highest level of security that is theoretically possible, although numerous projects in the industry have not reached the desired level of maturity because they are highly complex and implementation involves a huge amount of input. Furthermore, experience shows that end-to-end encryption does not meet with sufficient user acceptance.

Both mail transfer agent (MTA) encryption and transport layer encryption are solutions that can be realized with a reasonable amount of effort, as demonstrated by current projects. Transport layer encryption is especially suitable because it is supported “out-of-the-box” by many e-mail systems.

White paper topics

Encryption of e-mail transport

A basic level of security for e-mail traffic between participating companies is provided by encryption of the transport path between the e-mail transport systems of the individual companies. This means that every e-mail message is sent via a secure transport path. The white paper [W3] gives more details of solution scenarios.

E-mail encryption

Additional options for protecting the confidentiality of an e-mail message are encryption of the message contents by a local client component or a server-based MTA. Possible use cases are described in more detail in the white paper [W2].

Certificate and trust management

The options listed above require various default settings and functions associated with issuing and managing certificates and keys. More detailed information can be found in the white paper [W4].

Additional general requirements

The sender of an e-mail (or the organization) has to ensure that the mail sent is free of viruses, worms and similar malware. Appropriate protection mechanisms should be put in place in line with the latest technology.

Information classification and its application

Information classification is one aspect of information security. Information is classified to determine how it is to be handled, both organizationally and technically.

Security objectives

Information is classified with the following objectives in particular:

- defining an appropriate degree of protection for information assets,
- clear allocation and designation of information assets by assigning them to confidentiality levels that the user can issue and recognize unequivocally,
- deriving measures for storage and transport from the classification (confidentiality) levels.

Summary of classification levels and measures derived

The common classification levels and the measures derived from them for securing e-mail exchange are presented below.

Classification (confidentiality) level	General measures	Derived measures for securing e-mail exchange
Public	No measures required	No measures required, opportunistic TLS or more extensive measures are recommended.
Internal	Need-to-know principle, access protection	No measures required, opportunistic TLS or more extensive measures are recommended.
Confidential	Need-to-know principle, extended access control	MTA-based or client-based encryption using S/MIME or PGP, mandatory TLS, VPN.
Secret	Need-to-know principle, extended access control	The medium of e-mail simply does not offer a sufficient level of security.

Table 1: Classification levels and derived measures

<u>Explanations:</u>

- Need-to-know principle: ensuring that only the authorized group of people has access to information classified at a particular level.
- The measures specifically listed in the table are explained in more detail in the corresponding white papers.
- Storage encryption is recommended for information classified as confidential if it is expedient and practicable in the individual case. The various types available are not described in greater detail here.
- Information classified as secret must not be sent as e-mail or filed without additional protection measures because the methods described here cannot realize complete e-mail security when used on their own. The reasons for this are:
  - methods for e-mail security generally do not ensure strong authentication,
  - methods for e-mail security generally do not ensure adequate storage encryption.

Persistence of information classification

An information classification must not be downgraded or revoked without the consent of the owner of the information.

Designation using e-mail header “Sensitivity”

Most e-mail client products support designation of e-mail messages using the IETF RFC822 mailheader *“**Sensitivity:*** <value>” by the user. This designation is retained when the e-mail is transmitted and is displayed to the recipient by most e-mail clients.

However, there is limited benefit in pairing up the common values for this designation with the above-defined classification levels:

- Designation as “**Sensitivity: Company-Confidential**” corresponds to classification as “confidential” in the sense of this document.

- Any other “Sensitivity” designation (or the absence of one) should be regarded as equivalent to the classification level “internal” for the purposes of automated security for the e-mail exchange.

We urgently recommend using the afore-mentioned e-mail header despite its limitations, because on the one hand it improves clarity and transparency for end users, and on the other it provides an opportunity for automated processing/handling, e.g. by an MTA.

Securing confidential e-mail traffic

Several options exist that ensure confidential e-mail communication. They are listed below.

Responsibility for the secure transmission of an e-mail message classified as “confidential” by the sender ends when the message is successfully transmitted to an MTA that is responsible for the recipient’s domain according to the public list (DNS MX-/A-Record) or bilateral agreement. At this point the responsibility passes to the receiving organization.

Transmission using existing standards

Securing e-mail at the transport level

The Working Group has identified the following technical methods for transport encryption of e-mail messages:

- mandatory TLS,
- ENX,
- VPN

Application of these methods is recommended [W3].

Securing e-mail at the content level

For encrypting the content of e-mail messages, two standards have become established that are incompatible with each other:

- OpenPGP,
- S/MIME.

Application of these standards is recommended [W2].

Certificates are used for these encryption standards. In this series of documents we use the term “certificate” to refer to both X.509 and PGP key material.

Application of these encryption standards does not automatically result in end-to-end encryption, since they can also be deployed on MTAs for decryption.

Also, it cannot be assumed that the message will be filed in encrypted form at the recipient.

The properties of a certificate and the depth of its organizational allocation (allocation to the company, an organizational unit or an individual) do not indicate anything about:

- the place in the recipient company where the certificate is kept,
- the point at which it is applied for decrypting the e-mail,
- the form in which the key is stored (software, hardware or hardware security module),
- the availability of the certificate even without action by the person to whom it was issued (e.g. without PIN),
- the path the e-mail follows within the target company while it is still encrypted, and after it is decrypted.

Certificates that are allocated to named end users can therefore be stored on an MTA and used for automated decryption.

Combining different methods

Multiple securing of e-mails, e.g. using mandatory TLS in addition to an MTA, is not necessary but is permissible if it is not ruled out by different standards, such as S/MIME and OpenPGP, or the overall technical situations at the communication partners.

Interim communication (optional)

In practice, scenarios occur in which confidential information has to be transmitted ad-hoc to the recipient. It will not always be possible for the communication partners to immediately apply one of the above-mentioned standard procedures. If it is not reasonably possible to use other means of communication than e-mail, and a risk assessment of the companies involved allows in the specific case, there are various measures available for bridging the period until a standardized system for e-mail security can be established. This type of temporary procedure is preferable to unencrypted communication.

The annex gives some examples and explains the associated risks.

Measures in the absence of a secure system

If encrypted e-mail communication is not available, either in accordance with the existing standards or in the sense of interim communication, an e-mail system should prevent information classified as “confidential” from leaving the company. The following strategies may be suitable:

- put on hold: keep the e-mail message in the queue until a secure system is available (e.g. when the connection is interrupted),
- return to sender: send the e-mail message back immediately as undeliverable under current conditions. The sender should be informed of the reasons why the message cannot be delivered.

In such cases, if the matter is urgent other procedures regarded as secure must be applied. Examples would be:

- file encryption,
- trusted courier service,
- secure platform for exchanging files.

Examples and risks of interim communication

Examples of implementation of interim communication are:

- certificate with weak verification (e.g. using a certificate issued on the basis of only an e-mail address and delivery to this email address),
- encrypted PDF as sub-function of MTAs (PushedPDF with access data sent separately),
- HTTPS webmail as a supplementary function to the MTA (with access data sent separately).

Risks: There are no transparently established trust relationships between the communicating entities. Certificates and/or access data are not transmitted using established, secured procedures.

Interim communication is not a long-term replacement for the standard procedures described in section 3.1. Even the temporary application of these measures has inherent weaknesses and generates additional problems:

- Proper exchange of certificates cannot be either assured or tracked. (applies to weakly verified certificate and password transmission when other procedures are used).
- In general the quality of a password cannot be guaranteed.
- It is impossible to rule out repeated use of passwords.
- In general the quality of the encryption cannot be guaranteed in the case of password-dependent procedures.
- Permitting non-standardized procedures gives the user a false sense of security.
- The need for standardized procedures is diluted by deployment of other procedures where a time limit is hard to enforce. (“Nothing lasts longer than a temporary solution.”)
- Procedural regulations that could mitigate these weaknesses may be seen by end users as too complicated and consequently compliance may be poor or non-existent.

This is not an exhaustive list of procedures and risks. Further details are not given at this point.

Interim communication procedures represent an emergency solution, and are generally not recommended like the other procedures.

Given the inherent risks described above associated with these measures, the measures may be used only after bilateral agreement has been reached between two companies.

Annex

The annex applies to all documents in the series on e-mail security.

Specifications

MIME	According to RFC 2045 to RFC 2049 http://www.ietf.org/rfc/rfc2045.txt http://www.ietf.org/rfc/rfc2046.txt http://www.ietf.org/rfc/rfc2047.txt http://www.ietf.org/rfc/rfc2048.txt http://www.ietf.org/rfc/rfc2049.txt
OpenPGP	According to RFC 4880, http://www.ietf.org/rfc/rfc4880.txt and RFC 3156, http://www.ietf.org/rfc/rfc3156.txt
PKCS #6	Extended-Certificate Syntax, http://www.rsa.com/rsalabs/
PKCS #7	Cryptographic Message Syntax, http://www.rsa.com/rsalabs/
PKCS #9	Selected Attribute Types, http://www.rsa.com/rsalabs/
PKCS #10	Certification Request Syntax; according to RFC 2314
PKCS #12	Transfer syntax for personal identity information, http://www.rsa.com/rsalabs/
S/MIME	According to RFC 3851, http://www.ietf.org/rfc/rfc3851.txt RFC 1847, http://www.ietf.org/rfc/rfc1847.txt and RFC 2633, http://www.ietf.org/rfc/rfc2633.txt http://www.ietf.org/html.charters/smime-charter.html
SMTP	According to RFC 2821, http://www.ietf.org/rfc/rfc2821.txt. based originally on RFCs 821 and 822
STARTTLS	According to RFC 3207, http://www.ietf.org/rfc/rfc3207.txt
TLS	According to RFC 2246, http://www.ietf.org/rfc/rfc2246.txt

RFC 821 / 822, RFC 2821	SMTP protocol
RFC 2246	Standardization of SSL 3.0 (forerunner of TLS), now replaced by RFC 4346
RFC 2314	PKCS #10: certificate requests
RFC 3207	Standard for SMTP via StartTLS, replaces RFC 2487
RFC 3280	Standard for digital certificates (X.509 v3)
RFC 4346	Standardization of TLS v1.1 (since 2006, previously SSL), replaces RFC 2246
RFC 4870 / 4871	DKIM
RFC 5280	Standard for digital certificates (X.509 v3), replaces RFCs 3280, 4325, 4630

References

[W1] White Paper “E-Mail-Security,” Version 1.2, Working Group “E-Mail Security”

[W2] White Paper “E-Mail-Encryption Using End-to-End Encryption and E-Mail Transfer Agents,” Version 1.0, Working Group “E-Mail Security”

[W3] White Paper “Encryption of E-Mail Traffic,” Version 1.1, Working Group “E-Mail Security”

[W4] White Paper “Certificate and Trust-Management - Requirements for certificates and trust relationships,” Version 1.0, Working Group “E-Mail Security”

Cryptographic procedures: recommendations and key lengths:

https://www.bsi.bund.de/cae/servlet/contentblob/477256/publicationFile/30924/BSI-TR-02102 V1 0 pdf.pdf

Cryptographic key length recommendation:

http://www.keylength.com/en/

Glossary

Basic security	Sending an e-mail message classified as “internal” via a protected transport path if available.
CA	Certification Authority: entity that issues X.509 certificates.
CA provider	Organization that operates one or more CAs.
CP	Certificate Policy: Document describing the requirements profile for the way a CA operates. It contains core aspects such as registration process, key length, key handling, key creation and technical system protection. This document assists third parties in analyzing trustworthiness and can be integrated into software.
CPS	Certification Practice Statement: Document describing the specific implementation of the requirements profile in the CP.
CSR	Certificate Signing Request – application submitted by the requester to receive a certificate from a CA.
CTL	Certificate Trust List – A signed list of certificates or other security-relevant information in an agreed format that can be validated and evaluated. The creator of the list guarantees with its signature that the certificates or information it contains possess defined properties or are suitable for defined purposes.
DKIM	Domain Keys Identified Mail. Identification protocol for ensuring the authenticity of senders of e-mail messages.
Domain Cert	Also called gateway certificate or organization certificate. A certificate issued for the organization, which contains the MTA’s e-mail domain.
ENX	Special VPN solution. “ENX is the common solution of the European automotive industry for the secure exchange of critical data on development, purchasing and production control.” [Source: http://www.enx.de].

HSM Hardware Security Module. A specially secured piece of hardware for storing confidential key material.

IRM Information Rights Management. Procedure for protecting electronic documents.

Mandatory TLS See STARTTLS.

MIME Multipurpose Internet Mail Extensions. E-mail file format standard thatenables an e-mail message to be divided into various text parts and/or attachment parts with differing properties (file types, forms of presentation, presentation alternatives, fonts, etc.).

MTA Mail Transfer Agent. Component of the e-mail infrastructure, which receives e-mails using SMTP and forwards them in accordance with certain rules.

MTA-CTL See CTL.

MX Mail Exchange. Synonym for MTA.

NDA Non-Disclosure Agreement – Secrecy agreement.

NIC Network Information Center – (here) a place for registering domain names. The NIC handle is the contact address entry in the NIC for a registered organization.

OCSP Online Certificate Status Protocol: An internet protocol enabling checks on the validity of certificates in real time.

Opportunistic TLS See STARTTLS.

OpenPGP File format standard for files that are encrypted and/or signed using PGP key material. The main application is for e-mail, whereby PGP/Inline and PGP/MIME are the most frequently used versions.

PGP Pretty Good Privacy. Here PGP means both the products of the PGP Corporation (http://www.pgp.com), GNU Privacy Guard (GnuPG, http://www.gnupg.org/) and International PGP (http://www.pgpi.org/). See OpenPGP.

PKI Public Key Infrastructure is the name used in cryptology to refer to a system that can issue, distribute and check electronic certificates. [Source: Wikipedia]

PKCS Public Key Cryptography Standards. A series of standard documents making recommendations for topics such as certificate requests and secure certificate transport. See also RFC 2314.

SCVP Server-based Certificate Validation Protocol: An internet protocol enabling the creation of chains of certificates and their validation.

Self-Signed-Cert A certificate that has not been certified by a recognized CA. As a rule, this type of certificate has been generated by the owner itself (possibly within a PKI).

S/MIME Secure Multipurpose Internet Mail Extensions. Extension of MIME for encryption and signing using key material contained in X.509 certificates.

SMTP Simple Mail Transfer Protocol. Standard for transmitting internet e-mail.

Soft-PSE Software Personal Security Environment. Unlike hardware PSE, in this case key material is not stored in special hardware, but in a symmetrically encrypted file.

SSL Secure Socket Layer. Technology for secure data exchange on a specific layer (transport layer) of the TCP / IP ISO-OSI layer model.

STARTTLS SMTP extended by the addition of TLS. Keyword introducing the switch from clear text transmission to TLS encryption in the case of an existing SMTP connection within the protocol sequences. STARTTLS can be selected for all or only for individual e-mail domains either to be used optionally, if it is available at the other party (opportunistic TLS), or as a mandatory requirement for e-mail exchange (mandatory TLS).

STARTTLS-CTL See CTL.

TCP/IP Transmission Control Protocol/Internet Protocol. Family of network protocols, also known collectively simply as “Internet Protocol” owing to their great importance for the internet.

TLS Transport Layer Security. Securing of data transmission on the transport layer. See STARTTLS.

TSP Trust Management Service Provider. An organization that tackles topics concerning the management of keys and certificates and the accreditation of certification authorities according to certain defined criteria, as a service. See [W4].

Tunnel In this context: an encrypted data connection from one system to another with an insecure network as the transport medium.

VDA German Association of the Automotive Industry.
See http://www.vda.de/

VPN Virtual Private Network. Means of securing data transmission on the network layer.

List of Authors

Name	Company	E-mail address
Frölich, Jens	AUDI AG	jens.froelich@audi.de
Ionescu, Michael	Porsche-Information Kommunikation-Services GmbH	michael.ionescu@porsche.de
Klingel, Jan-Arendt	BMW Group	jan-arendt.klingel@bmw.de
Liebe, Michael	Volkswagen AG	michael.liebe@volkswagen.de
Scherr, Carsten	Daimler AG	carsten.scherr@daimler.com

Document and version history:

Version	Date	Status, remarks
1.0	2009-06-08	Final version
11	2009-10-15	Revised version
1.2	2010-11-12	Revised version, glossary added