White Paper
Certificate and Trust Management

Requirements for certificates and trust relationships

Version: 1.0
Last revised: 2010-11-12
Classification: öffentlich/public

VDA | Verband der Automobilindustrie

Table of contents

Introduction

Initial context

This document is one of a series of white papers prepared by the Working Group "E-Mail Security" of the IT-ABC. For references, the glossary and additional material, please see the main document "E-Mail Security" [W1].

Simply implementing encryption solutions is not sufficient to make communication secure. The core element is the management and provision of the certificates that are necessary when encryption solutions are applied. Such certificates must be available as needed and easy to use if they are to gain wide acceptance among users and ultimately bring about a high level of security.

In the past, the necessary certificate and trust management was often left to the individual user. This frequently led to a lack of acceptance and to security loopholes relating to the quality of the certificates, encryption itself, and the validation of the certificates.

In the case of server-based solutions, the same deficits are seen regarding trust in the default settings of various products. These default settings include permissible key lengths and algorithms, and certification authorities predefined as trusted.

An example of this would be the use of STARTTLS in opportunistic mode. This mode is frequently accredited with better properties that, however, apply only if STARTTLS is used in a secure high-grade ciphers mandatory mode. This would include the following:

- trusting self-signed certificates only after validation,
- unencrypted transmission is not used as fallback solution [W3],
- restriction to recognized algorithms and key lengths [W1].

In addition, requirements and processes have to be defined for:

- providing certificates,
- validation and maintenance of certificates pursuant to defined standards (trust management),
- configuration and maintenance of policy settings.

General principles of the document

The term “CA” (certification authority) is used both in a hierarchical X.509 PKI (Public Key Infrastructure) and in a PGP PKI.

The management of PGP keys is subject to the same quality requirements in respect of key lengths and algorithms as those for X.509 certificates. To reflect a hierarchical structure that exists only indirectly within the PGP web of trust (similar to an X.509 PKI), it is recommended that the PGP keys of individual users should be signed either with a PGP company key or by a recognized PGP CA.

In the following, X.509 certificates and PGP keys will generally be called certificates.

Roles and responsibilities in secure e-mail communication

A number of roles and assigned responsibilities are necessary to guarantee secure e-mail transmission.

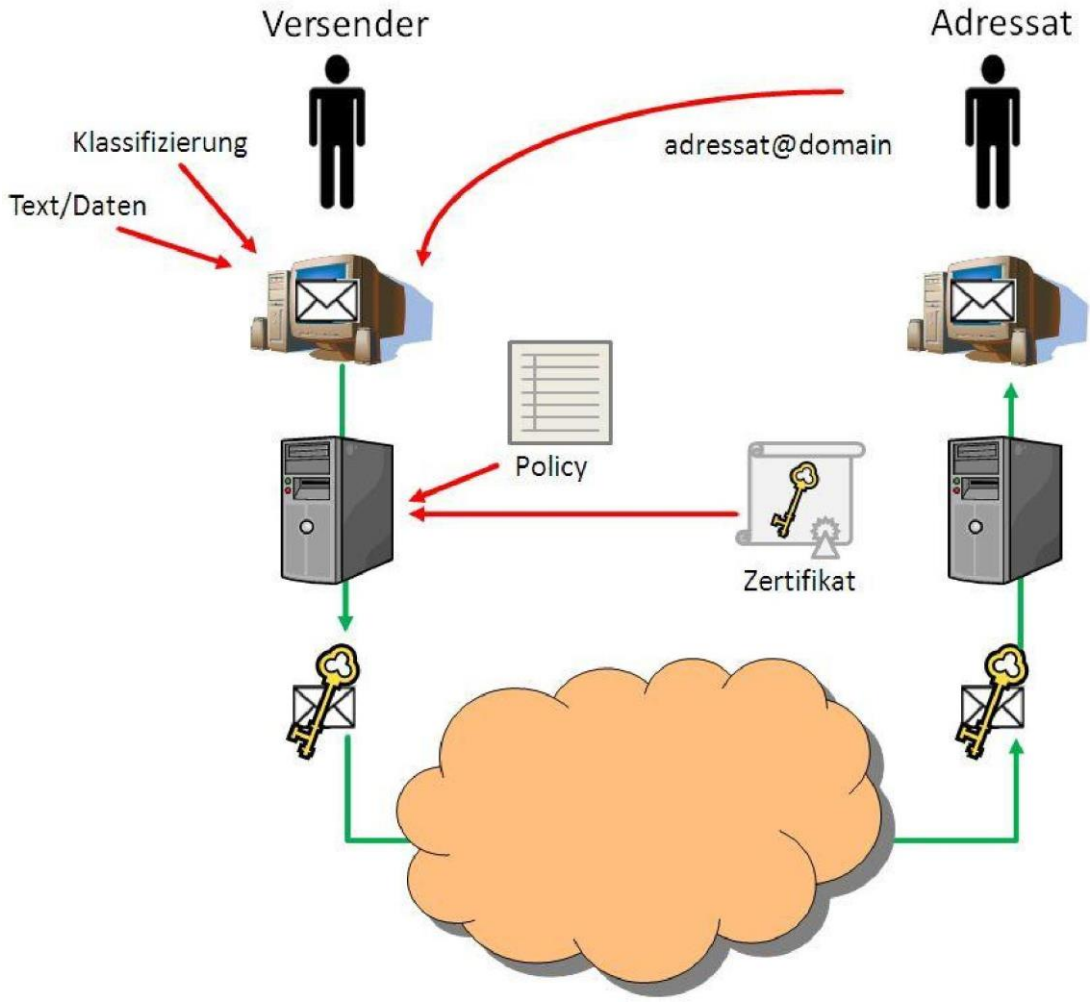

Figure: Schematic diagram of stages in secure e-mail transmission

Legend:

Green: Path the e-mail takes during secure transmission

Red: Control information necessary for secure transmission

Sender	Addressee
Classification	addressee@domain
Text/data	Certificate

Sender's side

Sender

The sender is responsible for:

- selecting the right e-mail address of the addressee,
- classifying the e-mail correctly in accordance with its content.

With the correct control information, the e-mail infrastructure manager is enabled to deliver the information to the correct addressee, and to recognize whether encryption is necessary and if so, which certificate material should be used.

Please note: before confidential information is exchanged, the parties involved should agree on how to handle it, based on an information classification and a non-disclosure agreement (NDA).

E-mail infrastructure manager

The e-mail infrastructure must be set up by the manager so that it performs the following tasks reliably:

- receiving e-mails from the sender via a secure connection,
- implementing measures in accordance with the classification and other guidelines (e.g. domains for which traffic must generally be encrypted),
- using the correct certificate when traffic is encrypted,
- protecting e-mail from unauthorized access,
- providing the required secure e-mail transmission path between the sender's infrastructure and the recipient's infrastructure.

Appropriate measures should be implemented based on the control information. This includes obtaining the necessary certificates of the addressee and obtaining, managing and supplying one's own certificates (certificate management). Here special attention should to be paid to the trustworthiness, validity and quality of the certificates (trust management). Trust management is the responsibility of the trust manager.

Recipient's side

E-mail infrastructure manager

The e-mail infrastructure must be set up by the manager so that it performs the following tasks reliably:

- providing ways of receiving protected e-mails safely,
- obtaining certificates and them making available (certificate management),
- implementing any cryptographic measures [W2],
- delivering the e-mails securely to the addressee,
- protecting the e-mail from unauthorized access.

Addressee

The addressee is responsible for treating information received in accordance with its confidentiality level and not downgrading this confidentiality level. If an e-mail message is not classified otherwise, it is to be treated as "internal" by default.

Just like senders, addressees can be people, groups of people, organizations or IT systems.

Trust management

Some central functions are necessary for e-mail encryption to be effective. These functions moderate and optimize the processes necessary for certificate management, which are used by the e-mail infrastructure managers.

This considerably reduces the input that is required from the sender, the addressee and the e-mail infrastructure manager, as compared with conventional measures.

More detail on the functions subsumed under the term "trust management" is given under "Trust management."

Use cases

Certificate and trust management forms the basis for the following use cases in e-mail security. They are described in more detail in the corresponding white paper:

■ Transport encryption [W3]

- STARTTLS
  - o opportunistic mode (opportunistic STARTTLS)
  - o secure high-grade ciphers mandatory mode (mandatory STARTTLS)
    - hostname certificate (that correlates with the domain)
    - not automatically correlating hostname certificate
- VPN

  VPN is not covered in this white paper.

■ Content encryption [W2] using S/MIME or OpenPGP

- MTA
  - o domain certificate (organization's certificate)
  - o personal certificate based on the e-mail address
- "End-to-X" encryption
  - o domain certificate (organization's certificate)
  - o personal certificate based on the e-mail address

o End-to-end encryption

- o personal certificate based on the e-mail address

■ Interim communication is dealt with in [W1].

Requirements for using STARTTLS

The basis for securing communication using a transmission tunnel under STARTTLS should be provided by certificates in the format X.509 version 3 or later [W3].

Transport encryption with opportunistic STARTTLS

This is the lowest level of protection, without requiring a trust relationship; transmission is encrypted only in the ideal case, and if there is any doubt it has to be assumed that transmission is not encrypted.

Opportunistic STARTTLS is permissible for use as basic security.

When opportunistic STARTTLS is used, the certificate does not have to satisfy any additional requirements.

It is recommended that as a general principle, only recognized algorithms and key lengths should be used so that basic protection is practicable [W1].

Transport encryption with mandatory STARTTLS

This procedure can provide protection of information classified as "confidential."

In practice, a distinction is made between certificates that are issued in

- the hostname of an MTA that correlates with the target domain,
- the hostname of an MTA that cannot be automatically correlated with the target domain.

When mandatory STARTTLS is applied for transmitting confidential e-mails, any certificate that is used must satisfy the following minimum requirements:

- the CA issuing the certificate is valid and
- considered trustworthy for this use case – based on an individual check by the e-mail infrastructure manager or a listing on the STARTTLS-CA-CTL (standard CA lists, for example of browsers, operating systems or MTAs, are intended for a different use case and are therefore not applicable unless they have been checked),
- the certificate includes at least the purposes "key encryption" and "server authentication",
- if the field "Alternative Requester" is used, it may contain only FQDN as the DNS name.

In addition, one of the following requirements has to be satisfied:

- the MTA identifies itself by means of a certificate that is issued for the target domain of the e-mail (e-mail domain corresponds to the CN (common name) of the field "Requester"), or
- the FQHN of the MTA and the CN of the requester in the certificate are identical and the FQDN can be derived from the target domain, or
- neither the FQDN of the MTA nor the certificate match the target domain. This is the case, for example, when MTAs receive e-mails for several e-mail domains belonging to one company. In this case, additional measures are required to authorize this MTA (hostname and certificate must match and the hostname must be assigned to the domain by a dedicated rule set. This should be regulated individually between the manager of the e-mail infrastructure and the target company, or alternatively taken from a STARTTLS-MX-CTL).

Content encryption

Requirements for using a mail transfer agent

This procedure can protect information classified as confidential.

For server-based e-mail encryption using a mail transfer agent (MTA), X.509 certificates version 3 or later may be used, or alternatively PGP certificates compatible with OpenPGP. In practice, distinctions are made between certificates that are issued for:

- the e-mail domains of the company or group,
- personal e-mail addresses used for corporate communication,
- personal e-mail addresses not used for corporate communication.

Domain certificates

The following applies to X.509 certificates:

- the certificate contains the e-mail address of the MTA or a fictitious e-mail address for the company
    - in the field “Requester” under the entry “CN” and
    - in the field “Requester” under the entry “E” and
    - in the field “Alternative Requester” under the entry “RFC 822 name”,
- the certificate and every element in the certificate chain is valid (for a limited period and not revoked), and
- the issuing authority is classified as trustworthy for this use case. This is ensured through individual examination by the e-mail infrastructure manager or a listing on the MTA-CTL (see glossary).

It should be remembered that to provide maximum compatibility with various implementations the e-mail address should appear in several fields of the certificate.

PGP certificates should include a valid e-mail address and thus the sender domain. This domain must be contained as either a primary or a secondary PGP User ID. The trust relationship is ensured by transfer of the public key via trusted channels or by cross-certification of the PGP corporate keys between the owner of the key and the manager of the e-mail infrastructure, or else via an MTA-CTL

Certificates based on personal e-mail addresses

The following applies to X.509 certificates:

- the certificate contains the owner's e-mail address
  - in the field "Requester" under the entry "E" or
  - in the field "Alternative Requester" under the entry "RFC822 name"
- the certificate and every element in the certificate chain is valid (for a limited period and not revoked), and
- the issuing authority is classified as trustworthy for this use case. This is ensured through individual examination by the e-mail infrastructure manager or a listing on the MTA-CTL (see glossary).

The following applies to PGP certificates:

- the e-mail address must be given in the field "User ID",
- the owner's name should be contained in the field "User ID".

The trust relationship can be ensured by the following process:

- transferring the public key or its "fingerprint" via trusted channels from the owner of the key to the manager of the e-mail infrastructure, or
- the public key, in conjunction with the recipient's e-mail address, has been signed by a PGP certificate classified as trusted for this purpose (signing key or trusted introducer), or
- the trustworthiness of individual PGP certificates can also be ensured via an MTA-CTL.

The trust relationship must be examined once again in particular for the e-mail addresses added to an existing key, before they are used.

Requirements for using “end-to-X” solutions

The applicable requirements are analogous to those for using MTAs. In this scenario it should be emphasized that various types of infrastructures for decryption may be used on the recipient’s side. Therefore, it must always be assumed that decryption is carried out by an MTA.

Please note: not all common products have technical support for certain combinations.

Requirements for end-to-end use

With solutions like these, it is possible to achieve a higher level of security than is the case when using MTAs, by applying personal key material (Soft PSE, smartcard). This could provide security up to the confidentiality level of “secret.” Since the sender cannot technically rule out decryption by an MTA on the recipient’s side, additional organizational agreements are necessary (e.g. that both parties use smartcards) [W1].

In the absence of an additional agreement, the requirements apply as specified in “Requirements for using a mail transfer agent.”

Requirements for interim communication

This procedure can protect information classified as confidential only provisionally. As a rule certificates are not used, and instead symmetrical key material is frequently used.

You can find a description in [W1].

Certificate management

Application of encryption technologies is based on the use of certificates. Certificates are issued by a trusted authority to confirm that a key pair belongs to an identity.

Certificates are issued with a specific lifetime, during which they have to satisfy certain requirements relating to allocation to an identity, secure transport to the requester, and safekeeping.

Requirements for certificates

Identification of the requester

Identification is a process for unequivocally recognizing a person or system. One can prove one's own identity by means of certain knowledge, possession of certain items or by appearing in person.

Commercial certificate providers generally classify the certificates they issue by identification features demanded of the requester. In this context, the most commonly used renowned providers usually distinguish the following classes:

Class	Features	Quality class
Class 1	Verification of the requester's identity by e-mail, for personal and server certificates. In the case of server certificates, validation of the domain name owner via e-mail contacts of the NIC handles, in individual cases possibly telephone verification that the requester belongs to the company, using the information from electronic corporate registries.	Low
Class 2	Transmission in writing (by fax or letter) of official ID as proof of identity. In the case of personal certificates, a copy of the person's identity card or a similar document. In the case of server certificates, an excerpt from the commercial register, D-U-N-S number (Dun & Bradstreet), business license or similar documentation of the company's owner.	Medium
Class 3	Personal identification at an authority named by the CA manager to function as a notary, via a procedure such as Postident.	High
Extended Verification (EV)	Extended form of Class 3, with additional proof of the authorized legal representative of the requester, extensive written application procedure and in-depth examination of the data submitted.	High

Depending on the level of confidentiality, the certificates issued by commercial CAs contain as attributes only an e-mail address or a DNS name (Class 1), and for the higher levels of confidentiality they contain the additional information from the application verified by the issuing authority – such as the company name, department, etc. This information varies from one provider to another.

In this white paper, company-specific certificates generated on the basis of a trusted source of data are regarded as equivalent to Class 2. A trusted data source may be a company's personnel master databases since it can be assumed that they are kept updated using secure processes.

Securing transport of the key to the requester

The private key can be sent from the issuing authority to the requester using the following graded paths (listed as examples):

Type	Quality class
Transmission to a specified e-mail address	Low
Transmission to a specified e-mail address within a secure e-mail infrastructure	Medium
Transmission through a service from/to an authenticated requester	Medium
Sending by regular mail	Medium
Retrieval from a secure service by an authenticated requester	High
Forwarding via reliable service providers	High
Forwarding to an authorized representative	High
Transfer in person	High

In practice the key is normally created at commercial certificate providers by the requester, and only in rare cases are private keys created at the provider or security copies of private keys held or sent to the requester. The requester creates a certificate signing request (CSR), usually in PKCS #10 format, and sends it to the provider electronically. The provider also sends the certificates to the requester electronically and this does not pose a significant security risk.

There are exceptions such as various PKI products and smartcard solutions from commercial CAs. Depending on the product variant, transfer is either done in person, or a key protected by a PIN and the relevant PIN itself are dispatched separately.

Physical storage of the private key

The requester can physically store the private key in the following ways:

Type	Quality class
Software PSE (PKCS #12 token or PGP certificate) in the owner's possession	Low
Application (e.g. MTA) has sole access to the software PSE (PKCS #12 token or PGP certificate)	Low
Smartcard or hardware security module (HSM)	High

All forms of storage require access control, e.g. password or PIN.

Physical storage of the certificate using software PSE in the possession of the user or of the MTA is sufficient for securing mails classified as confidential.

Recommendation: private keys should be generated centrally, and should be kept and used in the secure surroundings of the MTA.

Lifecycle

Aspects of the lifecycle such as renewing or revoking certificates are necessary, but this document does not specify additional requirements for them. When a solution is being set up, particular attention should be paid to how private keys are handled.

Summary of requirements for certificates

The following table puts the foregoing quality classes in relation to the points mentioned under the use cases.

Use case	**Requirements for identification**	**Requirements for transport**	**Requirements for storage**
Opportunistic STARTTLS	Low	Low	Low
Mandatory STARTTLS	High	High	Low
MTA with domain certificate	High	High	Low
MTA with certificate based on personal e-mail address	Medium	Low	Low
X-to-end with software PSE	Medium	Low	Low
X-to-end with smartcard	High	High	High

Recommendations for implementation

The requirements for certificates and their technical types are summarized below. A communication partner must satisfy these requirements in order to function as the addressee of secure e-mail communication in the sense of the white paper. The same requirements apply to the sender when assuming the role of addressee.

Use case and implementation recommendation	**Requirements for identification upon certificate creation**	**Requirements for handling the private key**	**Requirements for storing the private key**	**Requirements for validation by the sender of the e-mail**
Opportunistic STARTTLS – ***m****inimum standard*	-	-	-	-
Opportunistic STARTTLS - *recommended*	Class 3	PKCS #10 (standard)	Software PSE (standard)	-
Mandatory STARTTLS – ***m****inimum standard*	Class 3	PKCS #10 (standard)	Software PSE (standard)	CPS (CA) or manual validation
Mandatory STARTTLS – *recommended*	Class 3	PKCS #10 (standard)	Software PSE (standard)	CPS (CA)
MTA with domain certificate – ***m****inimum standard*	Class 2	PKCS #10 (standard)	Software PSE (standard)	CPS (CA) or manual validation
MTA with domain certificate – recommended	Class 3	PKCS #10 (standard)	Software PSE (standard)	CPS (CA) or manual validation
MTA with certificate (personal e-mail address) - ***m****inimum standard*	Class 2	-	Software PSE (standard)	CPS (CA) or manual validation
MTA with certificate based on personal e-mail address – *recommended*	Class 2	PKCS #10 (standard)	Software PSE (standard)	CPS (CA) or manual validation
X-to-end – ***m****inimum standard*	Class 2	-	Software PSE	CPS (CA) or manual validation
X-to-end – *recommended*	Class 2	PKCS #10 (standard)	Software PSE	CPS (CA) or manual validation

PGP certificates are manually validated or verified and signed by a CA similarly to class 2 or 3. For PGP certificates the standard procedure for generating and signing the certificates is comparable with that for PKCS #10.

Following manual validation of a certificate (end-entity certificate) by an e-mail infrastructure manager, the certificate can be used by the two parties, in line with the quality of the desired validation class – independent of the issue class. This does not result in a more extensive trust relationship between the mailing partners.

Trust management

Trust management is concerned with the validation, provision and management of certificates in accordance with defined standards. These tasks arise regularly for every e-mail infrastructure manager at the mailing partners who provides encrypted e-mail communication. Here encrypted e-mail communication refers to:

- content encryption using PGP,

- content encryption using S/MIME,

- transport encryption using STARTTLS,

whenever information classified as confidential. In this context, however, additional use cases are also conceivable.

The roles and tasks of trust management are described below.

It is planned that the general trust classification tasks will be performed by a central trust management service. This will enable visualization of organizational relationships and of information flows, and a distinction between activities that can be implemented either individually or by a service provider — for a mailing party or centrally for all the mail users.

Roles and tasks

Trust management is divided into several separate areas of responsibility and activities, each with different roles and tasks.

Trust managers

Trust managers are the organizational units of the companies participating in e-mail exchange, which make the technical foundations for encryption available to users (sender and addressee). The trust manager is responsible for the certificates issued to his company and for ensuring that certificates of the communication partners are used for their intended purpose.

The trust manager also assesses the trustworthiness and the services of the CAs operated by the trust center. The assessment depends on the fundamental security requirements.

Trust managers carry out the following tasks:

- obtaining certificates from one or more CAs operated by trust centers or other e-mail infrastructure managers,
- technical validity check and use of certificates from other e-mail infrastructure managers,

- using the services of trust centers (e.g. certificate and key servers),
- providing contact data and technical information for the provision of company certificates to the partners,
- ensuring secure communication with other e-mail infrastructure managers,
- assessing the CAs operated by trust centers and other e-mail infrastructure managers in respect of:
    - CA certificate,
    - CP/CPS,
    - inquiry services (CRL, CTL, etc.),
    - documentation of the assessed CAs,
- providing and updating the documentation,
- ensuring implementation and acceptance of the agreed regulations in their own company?

A CA's classification can change during the period of use. For this reason a CA should be re-assessed at intervals.

Given that addresses should not be passed on to third parties, the trust manager is obligated to treat the certificates issued as confidential and to use them solely for the intended purpose. In this setting, integrated corporate certificate repositories are a type of employee directory. Measures should be instituted to prevent unauthorized bulk queries, in order to maintain data protection.

Trust center

The trust center operates one or more certificate authorities (CAs). The trust center is responsible for the whole lifecycle of the certificates issued by its CAs. The trust center defines a set of requirements for the working practices of each CA (Certificate Policy, CP) and documents its specific implementation in a Certification Practice Statement (CPS). In general the trust center has the following tasks:

- issuing certificates,
- providing central services for automatic public query and for validity checks on self-issued certificates,
- providing the CP/CPS and appropriate action to analyze the trustworthiness of the CA.

In the case of a PGP-CA, the trust center has analogous tasks, such as certifying that existing PGP keys belong to particular owners.

Annex

For specifications, references and the glossary, please see the main document “E-Mail-Security” [W1].

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
Michael Liebe	Volkswagen AG	michael.liebe@volkswagen.de
Scherr, Carsten	Daimler AG	carsten.scherr@daimler.com

Document and version history:

Version	Date	Status, remarks
1.0	2010-11-12	Final version