E-Mail-Sicherheit

Whitepaper

Version: 1.2
Datum: 2010-11-12
Klassifizierung: öffentlich/public

VDA | Verband der Automobilindustrie

Vorwort

Auf Initiative einiger deutscher Automobilhersteller wurde 2009 begonnen, eine Whitepaper-Reihe „E-Mail-Sicherheit“ zu erstellen.

Diese Dokumente wurden erstellt. Es handelt sich dabei um

- ein einleitendes Dokument **„E-Mail-Sicherheit“,** welches den Leser in die Thematik „Schutz der Vertraulichkeit im E-Mail-Austausch“ einführt,
- ein Whitepaper **„Verschlüsselung des E-Mail-Transports“,** welches eine pragmatische und für den Anwender weitestgehend transparente Grundabsicherung durch eine Transportverschlüsselung beschreibt,
- ein Whitepaper „**E-Mail-Verschlüsselung durch Ende-zu-Ende und E-Mail-Verschlüsselungsgateways**“ sowie
- ein Whitepaper „**Zertifikats- und Trust-Management - Anforderungen an Zertifikate und Vertrauensbeziehungen**“

Die erstellten Dokumente geben der Automobilindustrie eine Orientierung auf Basis bereits bestehender technischer Ansätze. Dabei spielen die Anwenderfreundlichkeit und die Verwendung von industrieüblichen Vertraulichkeitsstufen und daraus abgeleiteter Maßnahmen eine wesentliche Rolle.

Der VDA empfiehlt seinen Mitgliedern, sich an den erstellten Dokumenten zu orientieren und in den Unternehmen die beschriebenen Maßnahmen umzusetzen.

Inhalt

Einleitung 4
Motivation 4
Ausgangslage und Architektursicht 4
Einordnung der Whitepaper-Dokumente 5
Verschlüsselung des E-Mail-Transports 5
E-Mail-Verschlüsselung 5
Zertifikats- und Trust-Management 6
Zusätzliche Rahmenbedingungen 6
Informationsklassifizierung und Anwendung 7
Sicherheitsziele 7
Gegenüberstellung Vertraulichkeitsstufen – abgeleitete Maßnahmen 7
Persistenz der Informationsklassifizierung 8
Kennzeichnung mittels des E-Mail-Headers „Sensitivity“ 8
Absicherung des vertraulichen E-Mail-Verkehrs 10
Übertragung unter Verwendung von bestehenden Standards 10
Absicherung der E-Mail auf Transportebene 10
Absicherung der E-Mail auf Inhaltsebene 10
Kombination verschiedener Methoden 11
Interimskommunikation (optional) 12
Maßnahmen bei fehlender Absicherung 12
Beispiele und Risiken zur Interimskommunikation 13
Anhang 15
Spezifikationen 15
Glossar 17
Autorenverzeichnis 21

Einleitung

Motivation

E-Mail-Verkehr birgt im heutigen Geschäftsleben zahlreiche Risiken. Neben unerwünschten Massen-E-Mails (Spam) und Verbreitung von Schadsoftware besteht bei geschäftlichem E-Mail-Verkehr zusätzlich das Risiko der Preisgabe oder Verfälschung der ausgetauschten Daten.

Unter europäischen Automobilherstellern hat sich ein Arbeitskreis „E-Mail-Sicherheit“ gebildet, der sich zum Ziel gesetzt hat, Best Practices zur E-Mail-Sicherheit zu beschreiben. Diese Best Practices dienen der Absicherung von E-Mails, die zwischen Organisationen ausgetauscht werden. Somit geben das vorliegende Dokument und die mit geltenden Whitepaper Lösungen vor, mit dem Ziel den Automobilherstellern und ihren Partnern eine sichere E-Mail-Kommunikation zu ermöglichen.

Fokus dieser Dokumente ist der Schutz der Vertraulichkeit durch Verschlüsselung, nicht das Schaffen von Verbindlichkeit wie zum Beispiel durch Signieren.

Ausgangslage und Architektursicht

Im Folgenden werden mehrere Ebenen der E-Mail-Sicherheit dargestellt und die Anwendungsfälle nachfolgend kurz beschrieben, sowie auf die weiterführenden Whitepapers hierzu verwiesen.

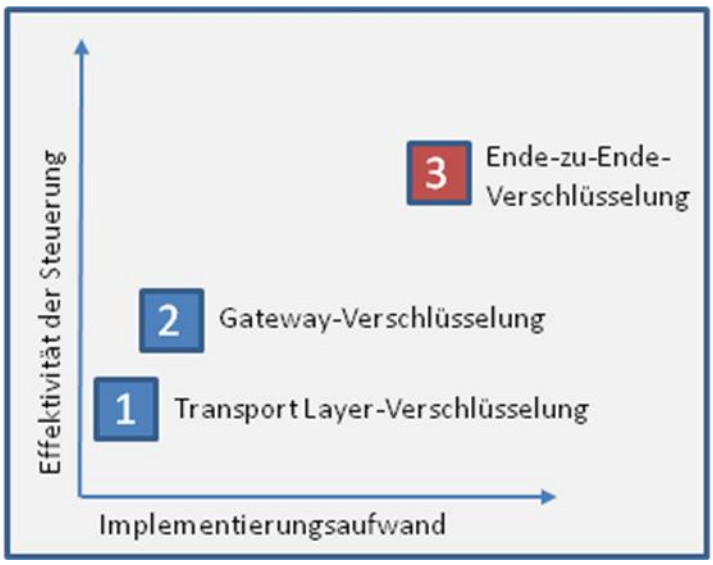

Abbildung 1: Ausgangslage und Architektursicht

Die hier aufgezeigten Lösungen unterscheiden sich in der Komplexität, dem Implementierungsaufwand und der Effektivität der Steuerung. Alle Lösungen haben zum Ziel, ein angemessenes Sicherheitsniveau beim Austausch von E-Mails zu ermöglichen.

Alle vorgeschlagenen Lösungen wurden mit dem Ziel ausgewählt, generell bereits getätigte Investitionen zu schützen, interoperabel zu sein und die Akzeptanz bei den Anwendern zu erhöhen.

Die Ende-zu-Ende-Verschlüsselung bietet die höchste theoretisch erreichbare Sicherheit, allerdings haben zahlreiche Projekte in der Industrie aufgrund der hohen Komplexität den gewünschten Reifegrad nicht erreicht, da der Implementierungsaufwand sehr hoch ist. Darüber hinaus fehlt es der Ende-zu-Ende-Verschlüsselung erfahrungsgemäß an Anwenderakzeptanz.

Sowohl die Gateway- als auch der Transport Layer-Verschlüsselung sind Lösungen, die mit vertretbarem Aufwand implementiert werden können, was laufende Projekte zeigen. Die Transport Layer-Verschlüsselung bietet sich hier besonders an, da sie von vielen E-Mail-Systemen „out-of-the-box“ unterstützt wird.

Einordnung der Whitepaper-Dokumente

Verschlüsselung des E-Mail-Transports

Eine Basis-Absicherung des E-Mail-Verkehrs zwischen beteiligten Unternehmen stellt die Verschlüsselung des Transportweges zwischen den E-Mail-Transportsystemen der einzelnen Unternehmen dar. Dabei wird jede E-Mail über einen sicheren Transportweg gesendet. Auf entsprechende Lösungsszenarien wird im Whitepaper [W3] näher eingegangen.

E-Mail-Verschlüsselung

Die Verschlüsselung der Inhalte einer E-Mail durch eine lokale Client-Komponente oder durch ein serverbasiertes E-Mail-Verschlüsselungsgateway (EVG) sind weitere Möglichkeiten zum Schutz der Vertraulichkeit einer E-Mail. Mögliche Anwendungsfälle werden im Whitepaper [W2] näher beschrieben.

Zertifikats- und Trust-Management

Im Rahmen der vorgehend aufgezeigten Möglichkeiten sind verschiedene Festlegungen und Aufgaben rund um die Ausstellung und Verwaltung von Zertifikaten und Schlüsseln notwendig. Nähere Informationen hierzu finden sich im Whitepaper [W4].

Zusätzliche Rahmenbedingungen

Der Versender einer E-Mail bzw. die Organisation haben dafür Sorge zu tragen, dass die versendete E-Mail frei von Viren, Würmern oder ähnlicher Schadsoftware ist. Entsprechende Schutzmechanismen nach aktuellem Stand der Technik sind einzusetzen.

Informationsklassifizierung und Anwendung

Informationsklassifizierung ist Teil der Informationssicherheit und wird angewandt, um daraus abzuleiten, wie die klassifizierte Information organisatorisch und technisch zu behandeln ist.

Sicherheitsziele

Die Informationsklassifizierung hat insbesondere folgende Ziele:

- Angemessenes Schutzniveau für Informationswerte definieren.
- Eindeutige Zuordnung und Kennzeichnung von Informationswerten durch Einordnung in für den Anwender eindeutig vergebbare und erkennbare Vertraulichkeitsstufen.
- Maßnahmen für die Speicherung und den Transport aus den Vertraulichkeitsstufen ableiten.

Gegenüberstellung Vertraulichkeitsstufen – abgeleitete Maßnahmen

Im Folgenden sind die üblichen Vertraulichkeitsstufen und die daraus abgeleiteten Maßnahmen zur Absicherung des E-Mail-Austausches dargestellt.

Vertraulichkeitsstufe ***Classification Level***	**Allgemeine Maßnahmen**	**Abgeleitete Maßnahmen zur Absicherung des E-Mail-Austauschs**
Öffentlich *Public*	Keine Maßnahmen erforderlich	Keine Maßnahmen erforderlich, opportunistic TLS oder weiterreichende Maßnahmen empfohlen.
Intern *Internal*	Need to Know-Prinzip, Zugriffsschutz	Keine Maßnahmen erforderlich, opportunistic TLS oder weiterreichende Maßnahmen empfohlen.
Vertraulich *Confidential*	Need to Know-Prinzip, erweiterter Zugriffsschutz	EVG- oder clientbasierte Verschüsselung mit S/MIME oder PGP, mandatory TLS, VPN.
Geheim *Secret*	Need to Know-Prinzip, erweiterter Zugriffsschutz	Das Medium E-Mail bietet grundsätzlich kein hinreichendes Sicherheitsniveau.

Tabelle 1: Vertraulichkeitsstufen und abgeleitete Maßnahmen

Erläuterungen:

- Need to Know-Prinzip: Sicherstellen, dass auf Informationen einer entsprechenden Vertraulichkeitsstufe nur der berechtigte Personenkreis Zugriff hat.
- Die in der Tabelle konkret aufgeführten Maßnahmen werden in den entsprechenden Whitepapers näher erläutert.
- Eine Ablageverschlüsselung wird für als vertraulich/*confidential* klassifizierte Informationen empfohlen, insofern sie im Einzelfall sinnvoll und anwendbar ist. Auf deren mögliche Ausprägungen wird hier nicht weiter eingegangen.
- Eine als geheim/*secret* klassifizierte Information darf nicht ohne zusätzliche Schutzmaßnahmen als E-Mail versandt oder abgelegt werden, da Maßnahmen zur ganzheitlichen Sicherung der E-Mail nicht allein mit Methoden der hier beschriebenen E-Mail-Sicherheit realisierbar sind. Die Gründe hierfür sind:
    - Methoden der E-Mail-Sicherheit stellen im Allgemeinen keine starke Authentifizierung sicher.
    - Methoden der E-Mail-Sicherheit stellen im Allgemeinen keine adäquate Ablageverschlüsselung sicher.

Persistenz der Informationsklassifizierung

Eine Informationsklassifizierung darf ohne Zustimmung des Informationseigners nicht herabgesetzt oder entfernt werden.

Kennzeichnung mittels des E-Mail-Headers „Sensitivity“

Die meisten E-Mail-Client-Produkte unterstützen eine Kennzeichnung von E-Mails mittels des IETF-RFC822-Mailheaders „***Sensitivity:*** <Wert>“ durch den Anwender. Diese Kennzeichnung bleibt bei der Übertragung der E-Mail erhalten und wird von den meisten E-Mail-Clients dem Empfänger angezeigt.

Eine Zuordnung zwischen den gängigen Werten dieser Kennzeichnungsmöglichkeit und den oben definierten Vertraulichkeitsstufen ist jedoch nur beschränkt sinnvoll:

- Eine Kennzeichnung mit „**Sensitivity: Company-Confidential**“ entspricht einer Klassifizierung als vertraulich/*confidential* im Sinne dieses Dokuments.

- Jede andere (oder auch eine nicht vorhandene) „Sensitivity“-Kennzeichnung ist für die Zwecke der Erfüllung der automatisierten Absicherung des E-Mail-Austauschs gleichzusetzen mit der Vertraulichkeitsstufe intern/*internal*.

Die Verwendung des genannten E-Mail-Headers wird trotz der genannten Einschränkungen dringend empfohlen, denn sie dient einerseits der besseren Übersichtlichkeit und Transparenz beim Endanwender und andererseits der Möglichkeit zur automatisierten Verarbeitung z.B. durch ein EVG.

Absicherung des vertraulichen E-Mail-Verkehrs

Es existieren mehrere Möglichkeiten, die vertrauliche E-Mail-Kommunikation abzusichern. Diese werden im Folgenden aufgeführt.

Die Verantwortung für die abgesicherte Übertragung einer als vertraulich/*confidential* eingestuften E-Mail durch den Absender endet mit der erfolgreichen Übergabe der E-Mail an einen MTA, der entsprechend der öffentlichen Liste (DNS MX-/A-Record) oder bilateraler Absprache für die Empfängerdomain zuständig ist. An diesem Punkt geht die Verantwortung auf die empfangende Organisation über.

Übertragung unter Verwendung von bestehenden Standards

Absicherung der E-Mail auf Transportebene

Im Arbeitskreis sind folgende technische Methoden zur Transportverschlüsselung von E-Mails identifiziert worden:

- mandatory TLS
- ENX
- VPN

Die Anwendung dieser Methoden wird empfohlen [W3].

Absicherung der E-Mail auf Inhaltsebene

Für die Verschlüsselung von E-Mail-Inhalten haben sich zwei untereinander inkompatible Standards etabliert:

- OpenPGP
- S/MIME

Die Anwendung dieser Standards wird empfohlen [W2].

Bei diesen Verschlüsselungsstandards werden Zertifikate verwendet. In dieser Dokumentenreihe wird mit dem Begriff Zertifikat sowohl X.509- als auch PGP-Schlüsselmaterial bezeichnet.

Die Verwendung dieser Verschlüsselungsstandards bedeutet nicht automatisch das Erreichen einer Ende-zu-Ende-Verschlüsselung, da sie auch auf EVGs zur Entschlüsselung eingesetzt werden können.

Eine verschlüsselte Ablage beim Empfänger kann ebenfalls nicht vorausgesetzt werden.

Die Eigenschaften eines Zertifikats oder die Tiefe seiner organisatorischen Zuordnung (Zuordnung zum Unternehmen, zu einer Organisationseinheit oder einem Individuum) treffen grundsätzlich keine Aussage über

- die Stelle, an der beim Empfängerunternehmen das Zertifikat vorgehalten wird,
- die Stelle, an der es zur Entschlüsselung der E-Mail eingesetzt wird,
- die Form der Schlüsselablage (Software, Hardware oder Hardware Security Module),
- die Verfügbarkeit des Zertifikats auch ohne Mitwirkung der bezogenen Person (z.B. ohne PIN),
- den Weg, den die E-Mail in noch ver- oder bereits entschlüsselter Form im Zielunternehmen zurücklegt.

Zertifikate, die namentlich Endbenutzern zugeordnet sind, können somit an einem EVG vorgehalten und zur automatisierten Entschlüsselung verwendet werden.

Kombination verschiedener Methoden

Die mehrfache Absicherung von E-Mails, z.B. mittels mandatory TLS zusätzlich zu EVG, ist nicht notwendig aber zulässig, sofern sich unterschiedliche Standards nicht gegenseitig ausschließen, wie z.B. S/MIME und OpenPGP oder technische Rahmenbedingungen bei den beteiligten Kommunikationspartnern.

Interimskommunikation (optional)

In der Praxis treten Szenarien auf in denen vertrauliche Informationen ad-hoc zum Empfänger übermittelt werden müssen. Den Kommunikationspartnern wird es nicht immer sofort möglich sein, eines der oben genannten Standardverfahren in der Kürze der Zeit nutzbar zu machen. Wenn hierzu die Verwendung anderer Kommunikationswege als E-Mail nicht sinnvoll möglich ist und eine entsprechende Risikoabschätzung der beteiligten Unternehmen es für den konkreten Fall zulässt, bieten sich verschiedene Maßnahmen an, den Zeitraum bis zur Etablierung standardisierter E-Mail-Sicherheit zu überbrücken. Ein solches zeitlich begrenztes Verfahren ist einer unverschlüsselten Kommunikation vorzuziehen.

Beispiele und damit verbundene Risiken werden im Anhang erläutert.

Maßnahmen bei fehlender Absicherung

Sofern eine verschlüsselte E-Mail-Kommunikation weder nach den bestehenden Standards noch im Sinne der Interimskommunikation verfügbar ist, soll ein E-Mail-System verhindern, dass als vertraulich gekennzeichnete Informationen das versendende Unternehmen verlässt. Dazu eignen sich folgende Strategien:

- Put on Hold: E-Mail in der Warteschlange vorhalten, bis eine Absicherung verfügbar ist (z.B. im Falle einer unterbrochenen Anbindung)
- Return to Sender: E-Mail unmittelbar als unter den gegebenen Bedingungen unzustellbar an den Absender zurücksenden. Dabei ist der Absender über die Gründe der Unzustellbarkeit eindeutig zu informieren.

In einem solchen Fall muss bei entsprechender Dringlichkeit auf andere, als sicher eingestufte Verfahren zurückgegriffen werden. Beispiele hierfür sind:

- Dateiverschlüsselung
- vertrauenswürdiger Kurierdienst
- sichere Dateiaustauschplattform

Beispiele und Risiken zur Interimskommunikation

Beispiele zur Umsetzung von Interimskommunikation sind:

- Zertifikat mit schwacher Verifikation (z. B. Verwendung eines nur auf Basis einer E-Mail-Adresse und Zustellung an diese E-Mail-Adresse ausgestellten Zertifikates)
- Encrypted PDF als Teilfunktion von EVGs (PushedPDF mit getrennter Zustellung der Zugangsdaten)
- HTTPS-Webmail als ergänzende Funktion zum EVG (mit getrennter Zustellung der Zugangsdaten)

Risiken: Es bestehen keine nachvollziehbar etablierten Vertrauensverhältnisse zwischen den an der Kommunikation beteiligten Instanzen. Zertifikate und/oder Zugangsdaten werden nicht über etablierte, abgesicherte Verfahren übertragen.

Die Interimskommunikation bietet keinen dauerhaften Ersatz für die unter 3.1 beschriebenen Standardverfahren. Selbst die nur vorübergehende Verwendung dieser Maßnahmen hat inhärente Schwachpunkte und wirft zusätzliche Problematiken auf:

- Ein ordnungsgemäßer Austausch von Zertifikaten kann nicht sichergestellt oder nachvollzogen werden. (betrifft schwach verifiziertes Zertifikat und Passwortübermittlung bei anderen Verfahren).
- Die Qualität eines Passwortes kann im Allgemeinen nicht sichergestellt werden.
- Die Wiederverwendung von Passwörtern kann nicht ausgeschlossen werden.
- Die Qualität der Verschlüsselung kann bei passwortabhängigen Verfahren im Allgemeinen nicht sichergestellt werden.
- Das Zulassen von nicht-standardisierten Verfahren vermittelt beim Anwender einen falschen Eindruck von Sicherheit.
- Die Notwendigkeit von standardisierten Verfahren wird durch den Einsatz anderer Verfahren aufgeweicht, deren zeitliche Begrenzung zudem schwer durchsetzbar ist. („Nichts hält länger als ein Provisorium.“)
- Verfahrensvorschriften, welche diese Schwachpunkte entschärfen könnten, werden ggf. von Endanwendern als zu aufwendig betrachtet und dementsprechend schlecht oder gar nicht befolgt.

Diese Nennung von Verfahren und Risiken ist nicht abschließend. Auf weitere Details wird an dieser Stelle nicht eingegangen.

Die Verfahren der Interimskommunikation stellen eine Notlösung dar und werden wie andere Verfahren generell nicht empfohlen.

Die oben beschriebenen inhärenten Risiken, die diesen Maßnahmen zugrunde liegen, können nur nach der bilateralen Einigung zweier Unternehmen zum Einsatz kommen.

Anhang

Der Anhang gilt für alle Dokumente der Reihe E-Mail-Sicherheit.

Spezifikationen

MIME	gemäß RFC 2045 bis 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	gemäß RFC 4880, http://www.ietf.org/rfc/rfc4880.txt und 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; gemäß RFC 2314
PKCS#12	Transfer syntax for personal identity information, http://www.rsa.com/rsalabs/
S/MIME	gemäß RFC 3851, http://www.ietf.org/rfc/rfc3851.txt RFC 1847, http://www.ietf.org/rfc/rfc1847.txt und RFC 2633, http://www.ietf.org/rfc/rfc2633.txt http://www.ietf.org/html.charters/smime-charter.html
SMTP	gemäß RFC 2821, http://www.ietf.org/rfc/rfc2821.txt. Basiert ursprünglich auf den RFCs 821 und 822
STARTTLS	gemäß RFC 3207, http://www.ietf.org/rfc/rfc3207.txt
TLS	gemäß RFC 2246, http://www.ietf.org/rfc/rfc2246.txt

RFC 821 / 822, RFC 2821	SMTP-Protokoll
RFC 2246	Standardisierung von SSL 3.0 (Vorgänger von TLS), heute durch RFC 4346 ersetzt
RFC 2314	PKCS #10: Zertifikatsanfragen
RFC 3207	Standard für SMTP via StartTLS, ersetzt RFC 2487
RFC 3280	*Standard für digitale Zertifikate (X.509 v3)*
RFC 4346	Standardisierung von TLS v1.1 (seit 2006, vormals SSL), ersetzt RFC 2246
RFC 4870 / 4871	DKIM
RFC 5280	Standard für digitale Zertifikate (X.509 v3), ersetzt RFC 3280, 4325, 4630

Referenzen

[W1] Whitepaper „E-Mail-Sicherheit“, Version 1.2, Arbeitskreis E-Mail-Sicherheit

[W2] Whitepaper „E-Mail-Verschlüsselung durch Ende-zu-Ende und E-Mail-Verschlüsselungsgateways“, Version 1.0, Arbeitskreis E-Mail-Sicherheit

[W3] Whitepaper „Verschlüsselung des E-Mail-Transports”, Version 1.1, Arbeitskreis E-Mail-Sicherheit

[W4] Whitepaper „Zertifikats- und Trust-Management, Anforderungen an Zertifikate und Vertrauensbeziehungen“, Version 1.0, Arbeitskreis E-Mail-Sicherheit

Kryptographische Verfahren: Empfehlungen und Schlüssellängen:

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/

Glossar

CA	Certification Authority: Ausgabestelle für X.509 Zertifikate.
CA-Provider	Organisation die eine oder mehrere CAs betreibt.
CP	Certificate Policy: Dokument, welches das Anforderungsprofil an die Arbeitsweise einer CA beschreibt. Es beinhaltet Kernpunkte wie Registrierungsprozess, Schlüssellänge, Schlüsselhandhabung, Schlüsselerzeugung und den technischen Systemschutz. Dieses Dokument dient Dritten der Analyse der Vertrauenswürdigkeit und lässt sich in Software integrieren.
CPS	Certification Practice Statement: Dokument, welches die konkrete Umsetzung des Anforderungsprofils der CP beschreibt.
CSR	Certificate Signing Request – Signierungsantrag des Antragsstellers, um von einer CA ein Zertifikat zu erhalten.
CTL	Certificate Trust List – Eine signierte Liste von Zertifikaten oder anderen Sicherheitsrelevanten Informationen in einem vereinbarten, validierbaren und auswertbaren Format. Der Ersteller der Liste sichert durch seine Signatur zu, dass die beinhalteten Zertifikate oder Informationen definierte Eigenschaften besitzen oder für definierte Zwecke tauglich sind.
DKIM	Domain Keys Identified Mail. Identifikationsprotokoll zur Sicherstellung der Authentizität von E-Mail-Absendern
Domain-Zertifikat	Auch Gateway-Zertifikat und Organisations-Zertifikat genannt. Ein Zertifikat, welches auf die Organisation ausgestellt ist und die E-Mail-Domäne des Gateways enthält.
ENX	Spezielle VPN-Lösung. „ENX ist die gemeinsame Lösung der europäischen Automobilindustrie für den sicheren Austausch kritischer Entwicklungs- Einkaufs-, und Produktions-steuerungsdaten.“ [Quelle: http://www.enx.de].

EVG	E-Mail-Verschlüsselungsgateway.
EVG-CTL	siehe CTL.
Grundsicherheit	Versenden einer als „intern“ gekennzeichneten E-Mail über einen zugriffsgeschützen Transportweg wenn verfügbar.
HSM	Hardware Security Module. Speziell gesicherte Hardware zur Speicherung von vertraulichem Schlüsselmaterial.
IRM	Information Rights Management. Verfahren zum Schützen von elektronischen Dokumenten.
Mandatory TLS	siehe STARTTLS.
MIME	Multipurpose Internet Mail Extensions. E-Mail-Dateiformatstandard, der die Gliederung einer E-Mail in verschiedene Text- bzw. Anhangsteile mit verschiedenen Eigenschaften (Dateitypen, Darstellungsformen, Darstellungsalternativen, Zeichensätzen etc.) ermöglicht.
MTA	Mail Transfer Agent. Komponente der E-Mail-Infrastruktur, welche E-Mails mittels SMTP annimmt und nach bestimmten Regeln weiterleitet.
MX	Mail Exchange. Synonym für MTA.
NDA	Non Disclosure Agreement – Geheimhaltungsvereinbarung
NIC	Network Information Center – hier Registrierungsstelle für Domain-Namen. Der NIC-Handle ist der Kontaktadresseintrag im NIC für eine registrierte Organisation.
OCSP	Online Certificate Status Protocol: Ein Internet-Protokoll, das die Gültigkeitsprüfung von Zertifikaten in Echtzeit ermöglicht.
Opportunistic TLS	siehe STARTTLS.
OpenPGP	Dateiformat-Standard für mittels PGP-Schlüsselmaterial verschlüsselte und/oder -signierte Daten. Die Hauptanwendung liegt bei E-Mail, wobei hauptsächlich die Ausprägungen PGP/Inline und PGP/MIME zum Einsatz kommen.
PGP	Pretty Good Privacy. PGP meint hier sowohl die Produkte der PGP Corporation (http://www.pgp.com) als auch GNU Privacy Guard (GnuPG, http://www.gnupg.org/) als auch International PGP (http://www.pgpi.org/). Siehe OpenPGP.

PKI	Mit Public-Key-Infrastruktur bezeichnet man in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. [Quelle: Wikipedia]
PKCS	Public-Key Cryptography Standards. Eine Reihe von Standarddokumenten, die Empfehlungen für Themen wie Zertifikatsanfrage und den sicheren Zertifikatstransport machen. Siehe auch RFC 2314.
SCVP	Server-based Certificate Validation Protocol: Ein Internet-Protokoll, das den Aufbau von Zertifikatsketten und deren Validierung ermöglicht.
Self-Signed-Cert	Ein Zertifikat, das nicht durch eine anerkannte CA zertifiziert wurde. Im Regelfall ist dieses Zertifikat von dem Eigentümer selber generiert worden (ggf. im Rahmen einer PKI).
S/MIME	Secure Multipurpose Internet Mail Extensions. Erweiterung von MIME um Verschlüsselung und -signierung mittels in X.509-Zertifikaten enthaltenen Schlüsselmaterials.
SMTP	Simple Mail Transfer Protocol. Standard zur Übertragung von Internet-E-Mail.
Soft-PSE	Software Personal Security Environment. Im Gegensatz zu Hardware PSE wird Schlüsselmaterial nicht in spezieller Hardware sondern in einer symmetrisch verschlüsselten Datei abgelegt.
SSL	Secure Socket Layer. Technik, um auf einer bestimmten Ebene (Transportebene) des TCP / IP ISO-OSI-Schichtenmodells Daten sicher auszutauschen.
STARTTLS	SMTP-Erweiterung um TLS. Schlüsselwort, das bei einer bestehenden SMTP-Verbindung innerhalb des Protokollablaufs die Umschaltung von Klartextübertragung auf TLS-Verschlüsselung einleitet. STARTTLS kann für alle oder einzelne E-Mail-Domains entweder als optional anzuwenden, sofern beim Gegenüber verfügbar (opportunistic TLS) oder als zwingende Voraussetzung für den E-Mail-Verkehr (mandatory TLS) eingestellt werden.

STARTTLS-CTL	siehe CTL.
TCP/IP	Transmission Control Protocol/Internet Protocol. Familie von Netzwerkprotokollen und wegen ihrer großen Bedeutung für das Internet auch kurz nur zusammengefasst als Internetprotokoll bezeichnet.
TLS	Transport Layer Security. Absicherung der Datenübertragung auf der Transportebene. Siehe STARTTLS.
TSP	Trust-Management Service Provider. Eine Organisation, welche sich Themen um die Schlüssel- bzw. Zertifikatsverwaltung und die Akkreditierung von Zertifizierungsstellen nach festgelegten Kriterien als Dienstleistung annimmt. Siehe [W4].
Tunnel	In diesem Kontext: Eine verschlüsselte Datenverbindung von einem System zum anderen System unter Nutzung eines unsicheren Netzwerkes als Transportmediums.
VDA	Verband der Automobilindustrie. Siehe http://www.vda.de/
VPN	Virtual Private Network. Absicherung der Datenübertragung auf der Netzwerkebene.

Autorenverzeichnis

Name	Unternehmen	E-Mail-Adresse
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

Dokumenten- und Versionshistorie:

Version	Datum	Status, Anmerkungen
1.0	2009-06-08	Finale Version
1.1	2009-10-15	Überarbeitete Version
1.2	2010-11-12	Überarbeitete Version, Ergänzung Glossar