Bundesamt
für Sicherheit in der
Informationstechnik

VS – Anforderungsprofil Sichere Übertragung von E-Mails und Dateien

Zum Schutz von „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Daten

Version: 1.0.1

Datum: 30.08.2019

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
E-Mail: vs-anforderungsprofile@bsi.bund.de
Internet: https://www.bsi.bund.de

GRP: VS-Anforderungsprofile

Digital unterschrieben von GRP: VS-Anforderungsprofile
Datum: 2019.09.24 12:09:56 +02'00'

Änderungshistorie

Version	Datum	Beschreibung
1.0	05.12.2018	Finale Version
1.0.1	30.08.2019	Finale Version

Allgemeiner Hinweis:

Bei diesem Dokument handelt es sich um ein VS-Anforderungsprofil des BSI an einen (oder mehrere) Produkttyp(en). Produkte dieses Typs dienen dazu, eingestufte Informationen sicher zu verarbeiten und zu übertragen. Somit handelt es sich dabei um ein informationssicherndes System (ISS) im Sinne der VSA.

Dieses Dokument vermittelt zulassungsrelevante Anforderungen an Produkte, welche zum in dem Anforderungsprofil genannten Produkttyp gehören. Die Bewertung für die prinzipielle Eignung solcher Produkte für den vom Bedarfsträger gewünschten Einsatzzweck wird sich u.a. darauf abstützen, inwiefern die Anforderungen von einem Produkt erfüllt werden.

Auch Hersteller eines Produktes können das VS-Anforderungsprofil nutzen, um einen ersten Eindruck von den Anforderungen an einen Produkttyp zu gewinnen. Abweichungen bei der Umsetzung der hier definierten Anforderungen in einem Produkt sind, sofern mit dem BSI abgestimmt, in begründeten Fällen möglich. **Eine Prüfung der Erfüllung dieses Anforderungsprofils ersetzt jedoch nicht den Prozess der Zulassung eines Produktes durch das BSI.** Diese erfolgt gemäß dem Nachweiskatalog [1].

Inhalt

1 Beschreibung des Produkttyps

Dieses Kapitel dient dazu, dieses Dokument eindeutig zu identifizieren (siehe Kapitel 1.1), den Produkttyp kurz zu beschreiben und dazu insbesondere seine grundlegenden Sicherheitsfunktionen zu nennen (siehe Kapitel 1.2).

1.1 Identifizierung des VS-Anforderungsprofils

Titel:	VS-Anforderungsprofil Sichere Übertragung von E-Mails und Dateien
Identifikationskennung:	BSI-VS-AP-0014-2018
Version:	1.0.1
Datum:	30.08.2019
Geeignet für:	VS - Nur für den Dienstgebrauch
Status:	Finale Version

1.2 Beschreibung des Produkttyps E-Mail- und Dateiverschlüsselung

1.2.1 Kurzbeschreibung

Vorbemerkung: In diesem Kapitel wird der Produkttyp beschrieben. Der Produkttyp, der eine sichere Übertragung von E-Mails und Dateien gewährleistet, heißt E-Mail- und Dateiverschlüsselung (EDV). Bei der E-Mail- und Dateiverschlüsselung handelt es sich genau genommen um zwei Produkttypen (E-Mail-Verschlüsselung einerseits und Dateiverschlüsselung andererseits). Beide Produkttypen sollen hier aus Sicht des zu betrachtenden Anwendungsfalles – der sicheren Übertragung bzw. dem sicheren Austausch sensibler Daten – beschrieben werden. Insofern werden sie zur sprachlichen Vereinfachung auch oft als ein „gemeinsamer“ Produkttyp „E-Mail- und Dateiverschlüsselung“ bezeichnet. Wenn Unterschiede der beiden Produkttypen herauszustellen sind, wird auf diese entsprechend eingegangen.

Eine E-Mail- und Dateiverschlüsselung ist ein Produkttyp, der dazu dient, zwischen Nutzern sensible Daten so austauschen zu können, dass deren Vertraulichkeit, Integrität als auch Authentizität sichergestellt ist. Die E-Mails bzw. die Dateien sollen von einem Nutzer (Absender) zu einem anderen Nutzer (Empfänger) so übertragen, versendet bzw. transportiert werden, dass folgende Ziele erreicht werden können, sofern der Nutzer die von der E-Mail- und Dateiverschlüsselung angebotenen Sicherheitsfunktionen entsprechend nutzt:

Vertraulichkeit der Daten: Die sensiblen Daten, die ausgetauscht werden, sind vertraulich und dürfen nur für den Absender und den Empfänger lesbar sein. Dazu werden die Daten von einem Nutzer (Absender) verschlüsselt und können von einem (anderen) autorisierten Nutzer (Empfänger) entschlüsselt werden.

Integrität der Daten: Die sensiblen Daten, die ausgetauscht werden, dürfen auf dem Weg vom Absender zum Empfänger nicht unbemerkt manipuliert werden können. Dazu werden die Daten vom Absender mit einem Integritätsschutz versehen. Der Empfänger wiederum prüft die Integrität.

Authentizität der Daten bzw. des Absenders der Daten: Die Echtheit der Daten bzw. des Absenders der Daten ist gewährleistet, das heißt der Absender ist wirklich diejenige Person, die als Absender angegeben ist und die sensiblen Daten versendet hat. Der Empfänger prüft die Authentizität der Daten bzw. des Absenders der Daten.

Die E-Mail- und Dateiverschlüsselung stellt für den Nutzer ein Schlüsselmanagement bereit.

Die klassische E-Mail-Verschlüsselung erfolgt von Client zu Client (Ende-zu-Ende-Verschlüsselung). Eine Server-basierte E-Mail-Verschlüsselung soll in diesem Anforderungsprofil nicht betrachtet werden, da die

dafür zu formulierenden Sicherheitsanforderungen über das klassische Modell hinausgehen können. In diesem Anforderungsprofil wird nur eine Client-basierte E-Mail-Verschlüsselung betrachtet. Bei der Client-basierten E-Mail-Verschlüsselung verschlüsselt und signiert das entsprechende Produkt auf dem Client-Rechner des Absenders die E-Mail vor dem Versenden. Das Entschlüsseln und die Signaturprüfung übernimmt das entsprechend auf dem Client-Rechner des Empfängers installierte Produkt nach dem Empfang der E-Mail.

Bei der E-Mail-Verschlüsselung handelt es sich um ein Softwareprodukt. Eine E-Mail-Verschlüsselung wird in der Regel als Plugin (d. h. als Zusatzprogramm) für verschiedene E-Mailsysteme entwickelt. Dabei kommt fast immer einer der folgenden zwei Standards zum Einsatz: S/MIME (Secure/Multipurpose Internet Mail Extensions) oder OpenPGP (Open Pretty Good Privacy). Bei beiden Standards können Dateien, welche ebenso verschlüsselt und signiert werden, als Anhänge einer E-Mail versendet werden.

Auch die Dateiverschlüsselung ist ein auf dem Client-Rechner installiertes Softwareprodukt, mit der es möglich ist, einzelne Dateien oder gesamte Ordner zu verschlüsseln und mit einem Integritäts- und Authentizitätsschutz zu versehen. Derartig verschlüsselte und geschützte Dateien können dann beispielsweise als Anhang einer unverschlüsselten E-Mail oder über einen Daten-Server ohne weitere Sicherheitsvorkehrungen versendet bzw. ausgetauscht werden.

Die E-Mail- und Dateiverschlüsselung bietet Funktionen für verschiedene Nutzungsszenarien an. Diese Nutzungsszenarien werden im Folgenden beschrieben und erläutert.

Bei der klassischen E-Mail-Verschlüsselung und -Signatur von Client zu Client (Ende-zu-Ende-Verschlüsselung) übernimmt die E-Mail-Verschlüsselung auf dem Client vom Absender die Verschlüsselung und das Signieren der zu übertragenden Nachricht, die E-Mail-Verschlüsselung auf dem Client vom Empfänger die Entschlüsselung und die Signaturprüfung der übertragenen Nachricht. Dazu benötigen sowohl der Absender als auch der Empfänger ein asymmetrisches Schlüsselpaar, das jeweils aus einem privaten Schlüssel (geheim) und einem öffentlichen Schlüssel (nicht geheim) besteht. Zum Verschlüsseln wird der öffentliche Schlüssel des Empfängers verwendet. Das Signieren erfolgt mit dem privaten Schlüssel des Absenders. Das Entschlüsseln erfolgt dann mit dem privaten Schlüssel des Empfängers und die Signaturprüfung mit dem öffentlichen Schlüssel des Absenders.

Hinweis: In der Praxis wird - wie beispielsweise derzeit beim S/MIME-Standard - zum Verschlüsseln der zu übertragenden Nachricht ein sogenanntes hybrid-asymmetrisches Verfahren eingesetzt. Das heißt, die zu übertragende Nachricht selbst wird im Rahmen eines symmetrischen Verfahrens mit einem generierten, geheimen Sitzungsschlüssel verschlüsselt. Dieser Sitzungsschlüssel wird nun mit dem öffentlichen Schlüssel des Empfängers im Rahmen eines asymmetrischen Verfahrens verschlüsselt und zusammen mit der (symmetrisch) verschlüsselten Nachricht an diesen versendet. Im Folgenden soll aber der Einfachheit halber und zur besseren Lesbarkeit die Beschreibung darauf verkürzt werden, dass die zu übertragende Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt wird. Die konkrete Implementierung eines Produktes kann dann im Detail komplizierter sein. Dies muss vom Hersteller in seiner Dokumentation beschrieben werden.

Der private Schlüssel muss geheim gehalten werden und es muss praktisch unmöglich sein, ihn aus dem öffentlichen Schlüssel zu berechnen. Für den Schutz des geheimen privaten Schlüssels kann dabei auch eine lokale Schlüsselhierarchie auf dem Client beginnend mit einem sogenannten Master-Key etabliert sein. Der Schutz des Master-Key muss dabei hardwarebasiert erfolgen (z. B. mittels Hardware-Token oder Smart-Card). (Hinweis: Ein softwarebasierter Passwortschutz für den Master-Key wird in diesem Anforderungsprofil nicht als ausreichend erachtet.)

Der öffentliche Schlüssel muss jedem zugänglich sein, der eine verschlüsselte Nachricht an den Besitzer des privaten Schlüssels senden will. Dabei muss sichergestellt sein, dass der öffentliche Schlüssel auch wirklich dem Empfänger zugeordnet ist. Inwieweit diese Eigenschaft gewährleistet wird, wird in einem Vertrauensstatus genannten Schlüsselattribut vorgehalten. Zur Ermittlung des Vertrauensstatus können verschiedene Methoden genutzt werden: es kann beispielsweise eine ganze PKI etabliert werden oder der Vertrauensstatus wird vom Nutzer manuell gesetzt, nachdem der Fingerabdruck des Schlüssels persönlich überprüft wurde. Einen „Mittelweg“ zwischen beiden Methoden bietet das sogenannte „Web Of Trust“.

Sowohl die Schlüsselgenerierung als auch der sichere Schlüsselaustausch einschließlich Export und Import von Schlüsseln müssen im Rahmen des Schlüsselmanagements geregelt sein. Sicherer Schlüsselaustausch bedeutet, dass die Schlüssel auf ihrem Weg nicht kompromittiert oder manipuliert werden können (vgl. dazu auch den in Kapitel 2.2 beschriebenen Schutzbedarf kryptographischer Schlüssel und Schlüsselattribute).

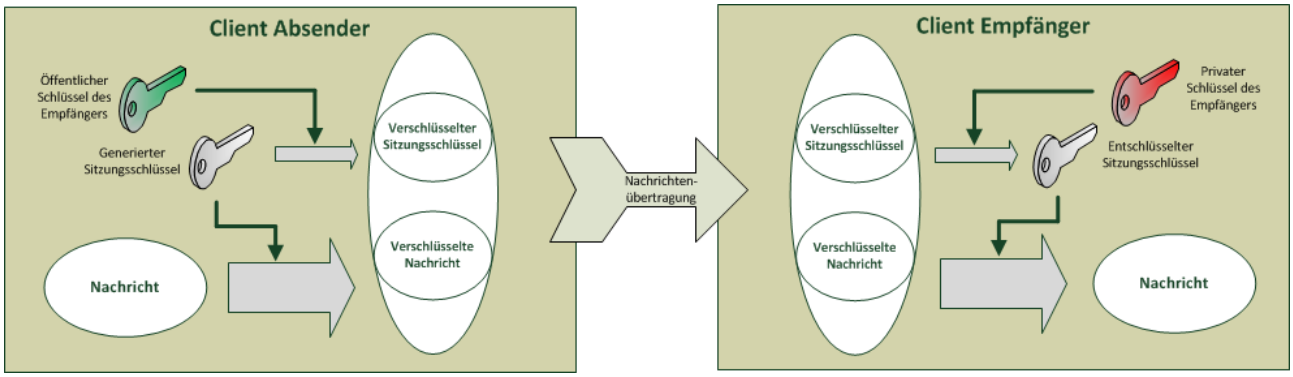

Abbildung 1: Beispiel für eine E-Mail-Verschlüsselung

Für die Dateiverschlüsselung soll hier ein Nutzungsszenario basierend auf einem symmetrischen Verschlüsselungsalgorithmus beschrieben werden. Jeder Nutzer der Dateiverschlüsselung muss dazu im Besitz des notwendigen symmetrischen Schlüssels sein. Dieser Schlüssel ist geheim und muss entsprechend geschützt und sicher gespeichert werden. Ferner muss der Austausch des Schlüssels auf sicherem Wege erfolgen. Es können dann alle Nutzer, die im Besitz des geheimen Schlüssels sind, Dateien bzw. Ordner sowohl verschlüsseln als auch entschlüsseln. Die Datei (oder mehrere Dateien bzw. Ordner) werden mit dem symmetrischen Schlüssel auf dem Client eines Absenders verschlüsselt und auf dem Client eines Empfängers wieder entschlüsselt. Um die Integrität der Datei zu gewährleisten, wendet man zusätzlich typischerweise entweder MACs (Message Authentication Codes) oder digitale Signaturen an. Erstere basieren auf symmetrischen, letztere auf asymmetrischen Verfahren. Praktisch wird bei einer Integritätsprüfung in der Regel auch gleichzeitig die Authentizität der Nachricht mit Bezug auf den Absender verifiziert. Bei authentischen Nachrichten ist sichergestellt, dass sie vom angegebenen Absender erstellt wurden. Mit der Authentizität eines Kommunikationspartners wird die Tatsache bezeichnet, dass er tatsächlich derjenige ist, der er vorgibt zu sein. Es sei darauf hingewiesen, dass bei Verwendung eines MAC nur die Authentizität der Nachricht, nicht die Authentizität des Absenders selbst (im Sinne der Nichtabstreitbarkeit) gewährleistet werden kann. Nichtabstreitbarkeit kann nur bei Verwendung einer digitalen Signatur erreicht werden.

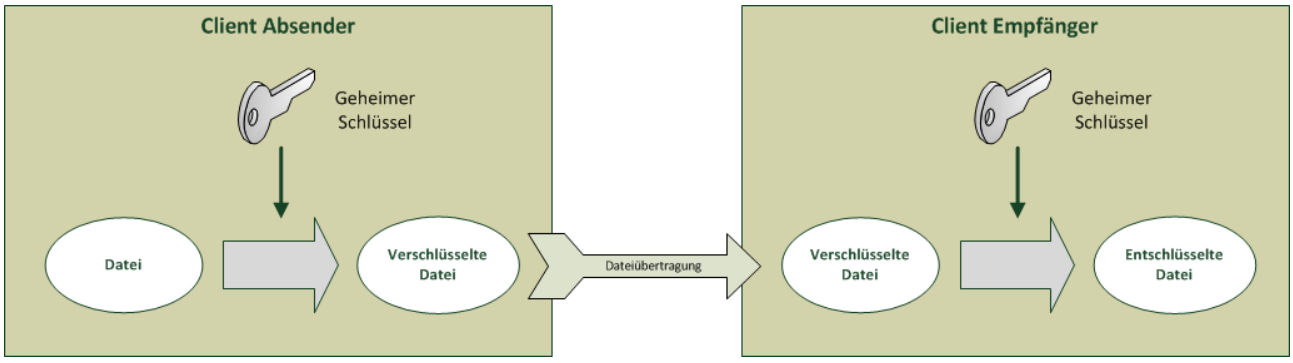

Abbildung 2: Beispiel für eine Dateiverschlüsselung

Eine Dateiverschlüsselung kann auch im Sinne einer Speicherverschlüsselung dazu dienen, sensible Daten sicher auf einem beliebigen Gerät abzulegen. Jedoch sind die Speicherverschlüsselung und die dafür zu erbringende Sicherheitsleistung nicht Gegenstand dieses Anforderungsprofils. Das hier vorliegende Anforderungsprofil betrachtet ausschließlich den Anwendungsfall der Übertragungsverschlüsselung. Der Weg, über den Dateien sicher ausgetauscht werden können, wird hier im Anforderungsprofil nicht

festgelegt. Dateien können, insbesondere wenn es sich um sehr große Datenmengen handelt, auch über einen Server ausgetauscht werden. Der Server erbringt in diesem Fall jedoch keine eigene Sicherheitsleistung. Die Sicherheitsleistung wird ausschließlich von der Software auf dem Client-Rechner erbracht (Ende-zu-Ende-Verschlüsselung). Nur dieser Fall soll hier im Anforderungsprofil betrachtet werden.

Die gesicherte Archivierung von Nachrichten und Dateien im Sinne der Speicherverschlüsselung soll ebenfalls nicht Gegenstand dieses Anforderungsprofils sein. Die Speicherverschlüsselung als solche ist Gegenstand des VS-Anforderungsprofils für eine Festplattenverschlüsselung [10].

1.2.2 Sicherheits-Grundfunktionen

In diesem Kapitel werden die Sicherheits-Grundfunktionen des Produkttyps E-Mail- und Dateiverschlüsselung beschrieben. Sie sollen dem Leser ein erstes Bild der Sicherheitsfunktionalität vermitteln und dienen dem Vergleich mit den Grundfunktionen anderer Produkttypen. Die bei ihrer Formulierung verwendeten Aussagen sind als Erläuterungen der Grundfunktionen zu verstehen und stellen noch keine formal verbindlichen Anforderungen an die Umsetzung im Produkt dar. Verbindliche Sicherheitsanforderungen werden in Kapitel 4 definiert.

Die Sicherheits-Grundfunktionen des Produkttyps E-Mail- und Dateiverschlüsselung, die die Verarbeitung und Übertragung der sensiblen Daten regeln, sind:

- **Vertraulichkeit der übertragenen Daten:** Für die Verschlüsselung und Entschlüsselung der sensiblen Daten sind kryptographische Funktionen erforderlich.
- **Integrität der übertragenen Daten:** Um die Unversehrtheit der übertragenen Daten im Sinne einer gezielten Manipulation zu gewährleisten, sind kryptographische Mechanismen wie zum Beispiel die Verwendung eines MAC oder einer digitalen Signatur, mittels derer die Integrität geprüft werden kann, erforderlich.
- **Authentizität der übertragenen Daten:** Unter Authentizität versteht man sowohl einen Identitätsnachweis des Absenders als auch die Authentizität der eigentlichen Daten. Bei ersterem möchte man sicherstellen, dass der Absender auch der ist, der er vorgibt zu sein. Dafür soll der Absender dem Empfänger seine Identität nachweisen können, ohne dass es Zweifel gibt. Bei der Authentizität der Daten geht es darum, dass die erhaltenen Daten auch tatsächlich vom authentisierten Absender stammen. Beides wird bei einem asymmetrischen Verfahren durch das Signieren der Nachrichten mit dem privaten Schlüssel des Absenders sowie die zugehörige Signaturprüfung unter Verwendung des entsprechenden vertrauenswürdigen öffentlichen Schlüssels des Absenders erreicht. Bei einem symmetrischen Verfahren wird letzteres durch die Berechnung und Prüfung eines MAC unter Verwendung des geheimen Schlüssels, den sowohl Absender als auch Empfänger besitzen müssen, erreicht. Die Authentizität des Absenders selbst lässt sich mit einem MAC jedoch nicht nachweisen. Wenn ein geheimer Schlüssel im Rahmen eines symmetrischen Verfahrens von einer Gruppe verwendet wird, kann nur festgestellt werden, dass ein Mitglied der Gruppe die Nachricht verschlüsselt hat. Ein spezifischer Absender im Sinne der Nichtabstreitbarkeit ist jedoch nicht feststellbar.
- **Zugriffskontrolle:** Die sensiblen Daten müssen vor unberechtigtem Lesen und vor gezielter Manipulation geschützt werden. Dazu erfolgt eine Zugriffskontrolle auf die im Rahmen der kryptographischen Verfahren verwendeten kryptographischen Schlüssel. Eine lokale Schlüsselhierarchie auf dem Client für die verwendeten kryptographischen Schlüssel soll erlaubt sein. Davon ausgehend, dass gegebenenfalls eine solche lokale Schlüsselhierarchie beginnend mit einem sogenannten Master-Key etabliert wird, wird für seine Verwendung mindestens eine Zwei-Faktor-Authentisierung (Besitz und Wissen wie z. B. Hardware-Token und Passwort) gefordert.
- **Schlüsselmanagement:** Verschiedene Funktionen zum Schlüsselmanagement werden bereitgestellt, beispielsweise Funktionen zum Umgang mit Schlüsselattributen (Besitzer, Gültigkeitszeitraum, Vertrauensstatus etc.) sowie Funktionen zum Generieren, zum Import und zum Export von Schlüsseln.

- **Zufallszahlengenerator:** Es wird ein Zufallszahlengenerator für die Schlüsselgenerierung und die kryptographischen Verfahren genutzt.
- **Installation und sicheres Update der Software:** Sicherstellung der Integrität und Authentizität des initialen Installationspakets wie auch später heruntergeladener/installierter Aktualisierungen (Updates).
- **Sicherheitsprotokollierung:** Es wird ein sicheres Logging sicherheitsrelevanter Ereignisse durchgeführt.
- **Sicherheitsmanagement (optional)** wie etwa Nutzerverwaltung.

Weitere Grundfunktionen können hinzukommen, wenn die E-Mail- und Dateiverschlüsselung diese zur Verfügung stellt bzw. wenn diese durch einen spezifischen Anwendungsfall erforderlich werden. Es wird dem Hersteller überlassen, dies im Security Target eines spezifischen Produktes zu präzisieren.

2 Definition des Sicherheitsproblems

In diesem Kapitel wird beschrieben, welches Sicherheitsproblem eine E-Mail- und Dateiverschlüsselung lösen soll. Zentral dafür ist die Angabe der **Bedrohungen** (siehe Kapitel 2.3), die durch das Produkt abgewehrt werden sollen. Um diese zu beschreiben, werden vorbereitend die **Rollen** von Personen und anderen IT-Produkten benannt, die mit der E-Mail- und Dateiverschlüsselung interagieren können (siehe Kapitel 2.1) und es werden die **schützenswerten Objekte** definiert (siehe Kapitel 2.2).

Neben der Betrachtung von Bedrohungen kann es auch die Notwendigkeit der expliziten Festlegung sogenannter **Sicherheitspolitiken** (siehe Kapitel 2.4) geben. Dabei handelt es sich um die explizite Festlegung von vorgegebenen Sicherheitsanforderungen, die nicht aus Bedrohungen abgeleitet werden.

In Kapitel 2.5 werden wichtige **Voraussetzungen für die Einsatzumgebung** benannt, um die erforderliche Sicherheitsleistung einer E-Mail- und Dateiverschlüsselung eingrenzen zu können.

Wenn in diesem Dokument Anforderungen definiert werden, werden dabei folgende Verben verwendet:

- „Muss“: Die Anforderung ist zwingend umzusetzen.
- „Sollte“: Es wird empfohlen, die Anforderung umzusetzen.
- „Darf“, „Kann“: Es ist möglich, die Anforderung umzusetzen.

Diese Verwendung entspricht derjenigen, die in Dokumenten des DIN üblich ist.

2.1 Rollen

Die folgenden Personen oder IT-Produkte können mit einer E-Mail- und Dateiverschlüsselung interagieren:

Nutzer

Nutzer/Absender: Der Nutzer (Absender) ist eine Person, die die sensiblen Daten vor dem Austausch verschlüsselt und mit einem Integritäts- und Authentizitätsschutz versieht.

Nutzer/Empfänger: Der Nutzer (Empfänger) ist eine Person, die nach ihrer erfolgreichen Authentisierung Zugriff auf die sensiblen Daten hat und deren Integrität sowie die Authentizität der Daten bzw. des Absenders prüft.

Hinweis: Als Absender und Empfänger sind auch Gruppen möglich, was bedeutet, dass jede Person einer solchen Gruppe zum Umgang mit den sensiblen Daten im Sinne der Sicherheits-Grundfunktionen Vertraulichkeit, Integrität, Authentizität und Zugriffskontrolle berechtigt ist. Dazu müssen die Personen im Besitz der/des entsprechenden kryptographischen Schlüssel/s sein und die Berechtigung für ihre/seine Verwendung haben.

Administrator

Ein Administrator ist eine autorisierte Person, die eine oder mehrere der folgenden Aufgaben wahrnimmt:

- Installation und sicheres Update der E-Mail- und Dateiverschlüsselung,
- Konfiguration der E-Mail- und Dateiverschlüsselung,
- Optional: Managementfunktionen, die für ein konkretes Produkt spezifisch sind.

Hinweis: Die Rollen Administrator und Nutzer sind hier im logischen Sinne voneinander abgegrenzt. Die Kernfunktionalität einer E-Mail- und Dateiverschlüsselung wird hier logisch der Rolle Nutzer zugeordnet. In Abgrenzung dazu werden zusätzliche administrative Aufgaben der Rolle Administrator zugeordnet. Organisatorisch können beide Rollen von derselben Person ausgeübt werden.

Auditor

Ein Auditor ist eine autorisierte Person, die die Einstellung von Logging-Optionen (Festlegung, welche Ereignisse und Details beim Logging aufgezeichnet werden sollen) sowie die Auswertung von Log-Dateien vornimmt.

Hinweis: Die Rollen Administrator und Auditor müssen von verschiedenen Personen ausgeübt werden.

Angreifer

Ein Angreifer ist eine Person oder technische Komponente, die versucht, eine der Bedrohungen zu realisieren oder eine der Sicherheitspolitiken außer Kraft zu setzen. Insbesondere kann eine im Grundsatz vertrauenswürdige, aber für bestimmte Dienste nicht autorisierte Person als Angreifer auftreten.

2.2 Schützenswerte Objekte

Schützenswerte Objekte (im Englischen „assets“) sind Daten und Informationen, deren Vertraulichkeit, Integrität bzw. Authentizität zu schützen sind, aber gegebenenfalls auch Funktionen oder andere Ressourcen, die vor unbefugtem Zugriff zu schützen sind.

Für eine E-Mail- und Dateiverschlüsselung werden hier die folgenden schützenswerten Objekte identifiziert:

Sensible Daten

Sensible Daten sind die eingestuften Daten, deren Vertraulichkeit, Integrität und Authentizität gewahrt werden muss. Der Zugriff auf die sensiblen Daten muss kontrolliert werden und ihre Kenntnisnahme und unbemerkte Manipulation durch Angreifer muss verhindert werden.

Die sensiblen Daten sind das primäre Schutzobjekt. Alle weiteren schützenswerten Objekte sind sekundär in dem Sinne, dass ein Angreifer nur deshalb an ihnen Interesse hat, um an die sensiblen Daten zu gelangen oder zu erreichen, dass von ihm erstellte Daten von einem Nutzer akzeptiert werden. Ein kryptographischer Schlüssel beispielsweise, welcher zur Verschlüsselung der sensiblen Daten verwendet wird, ist ein sekundäres Schutzobjekt.

Hinweis: Während die Liste der primären Schutzobjekte vollständig sein muss, um das Sicherheitsproblem vollständig formulieren zu können, ist eine komplette Liste sekundärer Schutzobjekte in einem VS Anforderungsprofil nicht zwangsläufig notwendig, da zwei verschiedene Produkte auch verschiedene sekundäre Assets haben können. So könnte ein Produkt etwa zusätzliche lokale kryptographische Schlüssel für spezifische Lösungen bestimmter Schutzanforderungen verwenden, die andere Produkte nicht benötigen.

Folgende sekundäre Schutzobjekte lassen sich definieren:

Kryptographische Schlüssel und Schlüsselattribute

Dies sind alle kryptographischen Schlüssel und Schlüsselattribute, die für einen der folgenden Zwecke benötigt werden:

- Verschlüsseln und Signieren der sensiblen Daten,
- Entschlüsseln der verschlüsselten Daten sowie Signatur- und Integritätsprüfung.

Der Begriff Schlüssel wird hier als Oberbegriff für alle im Rahmen der E-Mail- und Dateiverschlüsselung verwendeten Schlüssel benutzt. Falls eine genauere Beschreibung eines Schlüssels notwendig ist, so werden dazu unter anderem die Terme geheimer, privater und öffentlicher Schlüssel bzw. Zertifikat (in Abhängigkeit vom verwendeten kryptographischen Verfahren, welches ein symmetrisches oder asymmetrisches Verfahren sein kann), Master-Key oder Einzelschlüssel (im Kontext einer lokalen Schlüsselhierarchie) oder auch Sitzungsschlüssel im Falle der eigentlichen Ausführung einer kryptographischen Funktion verwendet (siehe auch Glossar).

Für geheime symmetrische Schlüssel und private asymmetrische Schlüssel ist die Authentizität, Vertraulichkeit und die Integrität, für öffentliche asymmetrische Schlüssel ist die Authentizität und Integrität zu schützen.

Ferner sind Schlüsselattribute wie Besitzer, Gültigkeitszeitraum, Vertrauensstatus etc. hinsichtlich Integrität zu schützen.

Es ist erlaubt, auf dem Client eine lokale Schlüsselhierarchie für die verwendeten kryptographischen Schlüssel zu etablieren. Es besteht dann die Möglichkeit, zwischen einem Master-Key sowie durch den Master-Key kryptographisch geschützte Einzelschlüssel für die eigentliche Ausführung kryptographischer Funktionen auf dem Nutzer-Client in Bezug auf die sensiblen Daten zu unterschieden. Wenn keine lokale Schlüsselhierarchie etabliert wird, werden Master-Key und Einzelschlüssel als identisch betrachtet. Das bedeutet, dass hier beschriebene Anforderungen an den Master-Key sich dann automatisch an den oder die verwendeten Einzelschlüssel „vererben“. In diesem Sinne soll im Folgenden die Bezeichnung „Master-Key“ verwendet werden, um die an diesen Schlüssel gestellten Anforderungen entsprechend bündeln zu können.

Für den Master-Key wird ein hardwarebasierter Schutz gefordert: Der Master-Key muss gesichert auf einem Hardware-Token gespeichert werden. Für seine Verwendung wird eine Zwei-Faktor-Authentisierung gefordert. Für die Einzelschlüssel (geheime und private (Sitzungs-)Schlüssel) wird gefordert, dass sie nicht persistent im Klartext auf dem Client gespeichert werden dürfen (im Falle einer lokalen Schlüsselhierarchie werden Einzelschlüssel mit dem Master-Key verschlüsselt).

Authentisierungsdaten

Dies sind beispielsweise die Passwörter, die im Rahmen der Schlüssel-Authentisierung benötigt werden.

Software der E-Mail- und Dateiverschlüsselung und Konfigurationsdaten

Alle Daten und Komponenten, deren Manipulation die sichere Funktion der E-Mail- und Dateiverschlüsselung gefährden würde, sind bezüglich ihrer Authentizität und Integrität zu schützen.

2.3 Bedrohungen

In diesem Kapitel werden die Bedrohungen der schützenswerten Assets aufgeführt, denen eine E-Mail- und Dateiverschlüsselung im Zusammenwirken mit ihrer Einsatzumgebung begegnen soll.

Bedrohungen werden in der Form T.Name benannt („T“ steht hier als Abkürzung für das englische Wort „Threat“).

Hinweis: Die hier aufgeführten Bedrohungen sind nicht als einzelne Bedrohungen, sondern als Kategorien zu betrachten. Im Zuge der Erstellung eines Security Targets sollen sie als Orientierung zur Ableitung von Bedrohungen, die sich auf ein konkretes Produkt zur E-Mail- und Dateiverschlüsselung beziehen, dienen.

Vorbemerkung: Da die sensiblen Daten das primäre Schutzobjekt sind, werden letztendlich alle Bedrohungen darauf abzielen, unbefugt Kenntnis der sensiblen Daten zu erlangen oder diese zu manipulieren. Alle nachfolgend genannten Bedrohungen lassen sich letztlich aus diesen "Grundbedrohungen" der sensiblen Daten ableiten.

T.Sensible_Daten_Lesen

Einem Angreifer gelingt es ohne die nötige Berechtigung, sensible Daten aus den verschlüsselten Daten zu gewinnen, indem er die Verschlüsselung der Daten bricht oder Schwächen in der Implementierung der Verschlüsselung (einschließlich des zur Übertragung gewählten Datenformates) oder der Handhabung und Speicherung von Schlüsseln ausnutzt.

T.Sensible_Daten_Manipulation

Einem Angreifer gelingt es ohne die nötige Berechtigung, sensible Daten unbemerkt zu manipulieren, indem er Schwächen in der Implementierung des Integritätsschutzes ausnutzt.

T.Identität

Einem Angreifer gelingt es, sich eine gefälschte Identität zu geben oder eine Identität missbräuchlich zu benutzen und damit vertrauliche und integritätsgeschützte Daten zu erstellen oder auf solche Daten zuzugreifen, ohne dass dies vom Empfänger oder dem missbräuchlich benutzten Absender bemerkt wird.

Anmerkung und Beispiel: Die hier beschriebenen Bedrohungen können auch in kombinierter Form auftreten wie beispielsweise bei der Ausnutzung der efail – Sicherheitslücke in den beiden Standards OpenPGP und S/MIME [8]. Die aufgedeckte Sicherheitslücke gestattet die nachträgliche Manipulation verschlüsselter Nachrichten durch einen Angreifer mit dem Ziel, Kenntnis der sensiblen Daten zu erlangen. Eine Abwehr dieser Bedrohung kann beispielsweise mittels konsequenter Verwendung von Prüfcodes wie MDC (Modification Detection Code) oder dem Einsatz von sog. AE/AEAD (Authenticated Encryption/Authenticated Encryption with Associated Data) Modi erfolgen.

2.4 Security Policies

In diesem Kapitel werden Sicherheitspolitiken definiert, die aufgrund einer Festlegung des BSI zum Produkt oder der Einsatzumgebung einzuhalten sind. Bei einer solchen Sicherheitspolitik handelt es sich um eine High-Level-Sicherheitsanforderung, die nicht zwingend aus einer Bedrohung abgeleitet, sondern vorgegeben wird. Ein typisches Beispiel dafür wäre die Anforderung, das Datenschutzrecht einzuhalten.

Die Benennung erfolgt in der Form **OSP.Name** („OSP“ ist dabei die Abkürzung des englischen Terms „Organizational Security Policy“).

OSP.Krypto

Es werden nur vom BSI akzeptierte Kryptoverfahren und -protokolle genutzt. Zu Details siehe Anf.Verschlüsselung in Kapitel 4.

Es wird ein Zufallszahlengenerator benutzt, der die Anforderungen des BSI an die Qualität der Zufallszahlen erfüllen muss. Zu Details siehe Anf.Zufallszahlengenerator in Kapitel 4.

OSP.Zulassung

Es werden neben der E-Mail- und Dateiverschlüsselung zur sicheren Verarbeitung von sensiblen Daten nur zur VS-Verarbeitung geeignete Produkte verwendet.

OSP.Zertifikate

Für die Prüfung von Zertifikaten muss die E-Mail- und Dateiverschlüsselung geeignete Methoden bereitstellen: 1) es kann eine PKI etabliert werden, 2) der sogenannte Vertrauensstatus kann vom Nutzer manuell gesetzt werden, 3) einen „Mittelweg“ zwischen beiden Methoden bietet das sogenannte „Web Of Trust“.

1) Es kann eine PKI etabliert werden:
   Für eine korrekte Prüfung von Zertifikaten kann die die E-Mail- und Dateiverschlüsselung einsetzende Organisation eine vertrauenswürdige Zertifizierungsstelle nutzen bzw. selber betreiben. Dies beinhaltet sowohl das Ausstellen und/oder Signieren von Zertifikaten, als auch die Verwaltung einer oder mehrerer CRLs (Certificate Revocation Lists) oder eines OCSP (Online Certificate Status Protocol) Servers.
   Wenn die Zertifizierungsstelle asymmetrische Schlüsselpaare erstellt und an Benutzer verteilt, muss die Organisation sicherstellen, dass die Verteilung der privaten Schlüssel und deren Schutzinformation (zum Beispiel Passwörter) über Kommunikationskanäle geschieht, die die Vertraulichkeit, Integrität und Authentizität dieser Schlüssel sicherstellt.
   Die zu verwendenden Schlüsselattribute für vom Nutzer neu zu generierende Schlüssel werden von der Organisation mittels Regeln vorgegeben. Solche Regeln beinhalten beispielsweise die Vergabe von E-Mail-Adressen an die Nutzer.

2) Der sogenannte Vertrauensstatus kann vom Nutzer manuell gesetzt werden: der Nutzer überprüft den Fingerabdruck des öffentlichen Schlüssels persönlich und trägt das Ergebnis der Prüfung in dem entsprechenden Schlüsselattribut ein.

3) „Web Of Trust“: Die Echtheit von Zertifikaten wird durch ein Netz von gegenseitigen Bestätigungen kombiniert mit dem individuell zugewiesenen Vertrauen in die Bestätigungen der anderen Netzteilnehmer („Owner Trust“) gewährleistet.

2.5 Voraussetzungen für den sicheren Einsatz

In diesem Kapitel werden Voraussetzungen beschrieben, die die Einsatzumgebung einer E-Mail- und Dateiverschlüsselung erfüllen muss, damit sie sicher betrieben werden kann.

Die Benennung dieser Voraussetzungen erfolgt in der Form **A.Name** ("A" steht dabei für Englisch "Assumption", das hier jedoch bewusst nicht wörtlich mit "Annahme" übersetzt wird, um deutlich zu machen, dass die richtigen Voraussetzungen zum sicheren Betrieb durch verantwortungsvolle Benutzer aktiv geschaffen werden müssen und nicht einfach "angenommen" werden).

A.Sichere_Handhabung

Es wird vorausgesetzt, dass die Umgebung, in der sich der Client mit der E-Mail- und Dateiverschlüsselung befindet, dieselben Anforderungen erfüllt, die gemäß VSA [2] oder GHB [9] für die Verarbeitung von VS der in Kapitel 1.1 definierten Einstufung gestellt werden.

Es wird vorausgesetzt, dass die Nutzer zur Handhabung von VS der in Kapitel 1.1 definierten Einstufung berechtigt sind.

Ferner wird vorausgesetzt, dass durch eine berechtigte Person, z.B. einen Administrator, unter Zuhilfenahme technischer und/oder organisatorischer Maßnahmen geprüft wird, welche Applikationen auf dem Client mit der E-Mail- und Dateiverschlüsselung installiert werden dürfen.

Der Austausch symmetrischer Schlüssel erfolgt so, dass Vertraulichkeit, Integrität und Authentizität dieser Schlüssel sicherstellt sind.

A.Vertrauenswürdiger_Nutzer

Es wird vorausgesetzt, dass die Nutzer der E-Mail- und Dateiverschlüsselung im Rahmen ihrer Autorisierung vertrauenswürdig sind und die E-Mail- und Dateiverschlüsselung gemäß der Anleitung benutzen. Insbesondere ist jeder Nutzer für den Schutz seiner Hardware (Token oder Smart-Card) und seines Passwortes, welches seinen geheimen oder privaten Schlüssel (Master-Key) schützt, verantwortlich. Jeder Nutzer prüft neu erhaltene Schlüssel von Kommunikationspartnern in den in OSP.Zertifikate beschriebenen Szenarien 2) persönliche Prüfung durch den Nutzer und 3) Web Of Trust auf deren Eigenschaften, bevor er diese Schlüssel als authentisiert kennzeichnet.

A.Vertrauenswürdiger_Administrator

Es wird vorausgesetzt, dass ein Administrator der E-Mail- und Dateiverschlüsselung im Rahmen seiner Autorisierung vertrauenswürdig ist und dass er die E-Mail- und Dateiverschlüsselung korrekt installiert und konfiguriert. Es wird vorausgesetzt, dass ein Administrator für seine Aufgaben befähigt und entsprechend geschult ist und er die bereitgestellte Anleitung befolgt.

A.Vertrauenswürdiger_Auditor

Es wird vorausgesetzt, dass ein Auditor der E-Mail- und Dateiverschlüsselung geschult und im Rahmen seiner Autorisierung vertrauenswürdig ist.

A.Plattform

Es wird vorausgesetzt, dass die zugrundeliegende Plattform (das sind hauptsächlich die unterliegende Hardware, das Betriebssystem sowie die Applikation, in die die E-Mail- und Dateiverschlüsselung

gegebenenfalls eingebettet ist) Mechanismen und Funktionen bereitstellt, die die Sicherheits-Grundfunktionen der E-Mail- und Dateiverschlüsselung geeignet unterstützen.

3 Sicherheitsziele

Dieses Kapitel definiert Sicherheitsziele für eine E-Mail- und Dateiverschlüsselung einerseits und für die Einsatzumgebung andererseits. Damit wird dargestellt, in welcher Arbeitsteilung E-Mail- und Dateiverschlüsselung einerseits und die Einsatzumgebung andererseits das im vorigen Kapitel definierte Sicherheitsproblem adressieren.

3.1 Sicherheitsziele für die E-Mail- und Dateiverschlüsselung

Die Benennung der Sicherheitsziele für die E-Mail- und Dateiverschlüsselung erfolgt in der Form O.Name (dabei steht "O" als Abkürzung für das englische "Objective").

Zu jedem Sicherheitsziel werden auch die Bedrohungen und OSP(s) benannt, die es adressiert.

O.Authentisierung

Bedrohung(en): T.Sensible_Daten_Lesen, T.Sensible_Daten_Manipulation, T.Identität

OSP(s): keine

Verwendung eines asymmetrischen Verfahrens:

Es ist eine Zwei-Faktor-Authentisierung des Nutzers erforderlich, bevor dieser Daten unter Verwendung des privaten Schlüssels/Master-Key entschlüsseln darf und damit Zugriff auf die sensiblen Daten erhält.

Es ist eine Zwei-Faktor-Authentisierung des Nutzers erforderlich, bevor dieser Daten unter Verwendung des privaten Schlüssels/Master-Key signieren darf.

Verwendung eines symmetrischen Verfahrens:

Es ist eine Zwei-Faktor-Authentisierung des Nutzers erforderlich, bevor dieser unter Verwendung des geheimen Schlüssels/Master-Key kryptographische Funktionen ausführen darf.

O.Krypto

Bedrohung(en): T.Sensible_Daten_Lesen, T.Sensible_Daten_Manipulation, T.Identität

OSP(s): OSP.Krypto

Die E-Mail- und Dateiverschlüsselung stellt für den Nutzer eine Verschlüsselung bereit, welche die Vertraulichkeit der sensiblen Daten gewährleistet und die BSI-Anforderungen erfüllt.

Die E-Mail- und Dateiverschlüsselung stellt für den Nutzer kryptographische Mechanismen bereit, mittels derer die Integrität der sensiblen Daten sichergestellt werden kann.

Die E-Mail- und Dateiverschlüsselung stellt für den Nutzer kryptographische Mechanismen bereit, mittels derer die Authentizität der sensiblen Daten sichergestellt werden kann.

Die E-Mail- und Dateiverschlüsselung nutzt einen Zufallszahlengenerator, der die Anforderungen des BSI an die Qualität der Zufallszahlen erfüllt.

Zu Details siehe Anf.Verschlüsselung, Anf.Entschlüsselung, Anf.Integrität_und_Authentizität und Anf.Zufallszahlengenerator in Kapitel 4.

O.Schlüsselmanagement

Bedrohung(en): T.Sensible_Daten_Lesen, T.Sensible_Daten_Manipulation, T.Identität

OSP(s): OSP.Zertifikate, OSP.Krypto

Die E-Mail- und Dateiverschlüsselung stellt dem Nutzer Funktionen zur Schlüsselgenerierung bereit. Die generierten Schlüssel genügen den Anforderungen des BSI.

Schlüssel werden so ausgetauscht, dass ihr entsprechender Schutzbedarf erfüllt wird.

Die E-Mail- und Dateiverschlüsselung stellt dem Nutzer Schlüsselmanagementfunktionen zur Verfügung, mittels derer Schlüssel importiert und exportiert werden können.

Der geheime oder private Master-Key wird auf einem sicheren Hardware-Token gespeichert. Der Zugriff auf den Master-Key ist mittels Zwei-Faktor-Authentisierung geschützt.

Geheime und private Einzelschlüssel werden zu keiner Zeit im Klartext persistent auf dem Client mit der E-Mail- und Dateiverschlüsselung gespeichert.

Nicht mehr benötigte geheime und private Schlüssel werden sicher gelöscht.

Ferner können Schlüsselattribute verwaltet und geprüft werden. Die E-Mail- und Dateiverschlüsselung stellt dem Nutzer auch Mechanismen zur Verfügung, mittels derer der Vertrauensstatus von Schlüsseln ermittelt und gegebenenfalls sicher verwaltet werden kann.

O.Administration

OSP(s): OSP.Zulassung

Folgende Managementfunktionen soll ein autorisierter Administrator ausführen können:

- Installation und Update der E-Mail- und Dateiverschlüsselung,
- Konfiguration der E-Mail- und Dateiverschlüsselung.

Managementfunktionen, die für ein konkretes Produkt spezifisch sind.

O.Logging

Bedrohung(en): O.Logging trägt als Maßnahme zur Erkennung und Reaktion auf verschiedene Bedrohungen bei.

OSP(s): keine

Die E-Mail- und Dateiverschlüsselung verfügt über eine Funktion zum sicheren Logging. Logging-Optionen können vom autorisierten Auditor eingestellt werden. Sicherheitsrelevante Ereignisse werden in diesem Fall gemäß vorgegebener Sicherheitspolitiken aufgezeichnet und ausgewertet.

O.Update

OSP(s): OSP.Zulassung

Die E-Mail- und Dateiverschlüsselung verfügt über einen sicheren Software-Update-Mechanismus.

3.2 Sicherheitsziele für die Einsatzumgebung

Die Benennung der Sicherheitsziele für die Einsatzumgebung der E-Mail- und Dateiverschlüsselung erfolgt in der Form **OE.Name** (dabei steht "O" als Abkürzung für das englische "Objective" und E für das englische „Environment“).

Bei jedem Sicherheitsziel wird auch das Sicherheitsproblem benannt, das es adressiert.

OE.Sichere_Handhabung:

OSP(s): OSP.Zulassung

Voraussetzung(en): A.Sichere_Handhabung

Durch geeignete und wirksame Maßnahmen in der Umgebung, in der sich das Gerät mit der E-Mail- und Dateiverschlüsselung befindet, muss sichergestellt sein, dass die Anforderungen erfüllt werden, die gemäß VSA [2] oder GHB [9] an die Verarbeitung von VS der in Kapitel 1.1 definierten Einstufung gestellt werden.

Durch eine berechtigte Person, z.B. einen Administrator, soll verantwortlich geprüft werden, welche Applikationen auf dem Client installiert werden dürfen. Die berechtigte Person soll unter Zuhilfenahme technischer Maßnahmen (z.B. Whitelist im Betriebssystem) und/oder organisatorischer Maßnahmen (z.B. Einhaltung von Richtlinien, Einsatz- und Betriebsbedingungen) dafür sorgen, dass auf dem Gerät nur vertrauenswürdige geprüfte bzw. freigegebene Applikationen laufen.

OE.Nutzer:

Voraussetzung(en): A.Vertrauenswürdiger_Nutzer

Die Nutzer der E-Mail- und Dateiverschlüsselung sind im Rahmen ihrer Autorisierung vertrauenswürdig und kompetent, die Funktionalität der E-Mail- und Dateiverschlüsselung zu nutzen. Sie schützen die von ihnen verwendeten Schlüssel vor unberechtigtem Zugriff und sind insbesondere zur Handhabung von VS der in Kapitel 1.1 definierten Einstufung befugt.

OE.Admin:

Voraussetzung(en): A.Vertrauenswürdiger_Administrator

Ein Administrator der E-Mail- und Dateiverschlüsselung ist im Rahmen seiner Autorisierung vertrauenswürdig und entsprechend geschult.

OE.Auditor:

Voraussetzung(en): A.Vertrauenswürdiger_Auditor

Ein Auditor der E-Mail- und Dateiverschlüsselung ist im Rahmen seiner Autorisierung vertrauenswürdig und entsprechend geschult.

OE.Plattform:

Voraussetzung(en): A.Betriebssystem

Der Hersteller dokumentiert und bewertet, welche Sicherheitsdienste auf dem Client-Rechner vertrauenswürdig realisiert sein müssen, damit diese in geeigneter Weise die Sicherheitsleistungen seines konkreten Produktes unterstützen.

OE.Schlüsselmanagement:

OSP(s), Bedrohung(en): OSP.Zertifikate, T.Sensible_Daten_Lesen, T.Sensible_Daten_Manipulation

Voraussetzung(en): A.Sichere_Handhabung, A.Vertrauenswürdiger_Nutzer

Alle Anteile des Schlüsselmanagements, die außerhalb der E-Mail- und Dateiverschlüsselung ablaufen, sind vertrauenswürdig. Das betrifft insbesondere den Schlüsselaustausch.

Hinweis: Dies betrifft nicht nur die vertrauliche Handhabung geheimer und privater Schlüssel, sondern auch das Sicherstellen der Authentizität öffentlicher Schlüssel.

Der Hersteller beschreibt sein Schlüsselmanagement und nimmt eine Bewertung der Anteile des Schlüsselmanagements, die außerhalb der E-Mail- und Dateiverschlüsselung ablaufen und für sein Produkt erforderlich sind, vor.

4 Sicherheitsanforderungen

In diesem Kapitel werden die funktionalen Sicherheitsanforderungen definiert, die eine E-Mail- und Dateiverschlüsselung erfüllen muss. Die Benennung erfolgt in der Form **Anf.Name.** Dabei steht "Anf" als Abkürzung für Anforderung.

Zu jeder Sicherheitsanforderung werden auch die Sicherheitsziele benannt, die dadurch umgesetzt werden.

Anf.Verschlüsselung

Die E-Mail- und Dateiverschlüsselung muss kryptographische Verfahren anbieten, die geeignet sind, die Vertraulichkeit der sensiblen Daten zu gewährleisten.

Die E-Mail- und Dateiverschlüsselung muss Algorithmen zur Verschlüsselung der sensiblen Daten nutzen, die die Anforderungen der Technischen Richtlinie TR-02102 [3], Teil 1, Kapitel 2 (symmetrische Verfahren) und Kapitel 3 (asymmetrische Verfahren) berücksichtigen. Es müssen insbesondere die folgenden Aspekte bei der Wahl von geeigneten Algorithmen beachtet werden:

- Die verwendeten Algorithmen müssen vom BSI für diesen Zweck als ausreichend sicher betrachtet werden.
- Für die Verschlüsselung müssen Schlüssel verwendet werden, deren Lebensdauer auf geeignete Weise begrenzt ist. Dies muss gemeinsam mit dem BSI abgestimmt werden.

Bezüglich der zu verwendenden kryptographischen Algorithmen ist nicht nur sicherzustellen, dass geeignete Algorithmen gewählt werden, sondern auch, dass diese korrekt implementiert sind. Daher muss nicht nur die Wahl der Algorithmen, sondern auch die zu verwendenden Bibliotheksfunktionen mit dem BSI abgestimmt werden.

Kryptographische Algorithmen und Abläufe müssen gemäß dem Nachweiskatalog [1] dokumentiert werden. Grundsätzlich ist die benötigte Dokumentation kryptographischer Mechanismen gemäß der "Detailspezifikation kryptographischer Abläufe und Mechanismen" [4] zu erstellen. Im Rahmen der Zulassung wird die Eignung der Implementierung im Hinblick auf das im Security Target beschriebene Bedrohungsszenario gemäß [7] bewertet. Dies schließt die Prüfung von Eigenschaften wie z.B. Seitenkanalresistenz bei Timing Angriffen auf Grundlage der Nachweise des Herstellers ein. Seitenkanalresistenz betrifft hier, also im Fall von VS-NfD, solche Aspekte, die sich durch state-of-the-art-Implementierungen der Kryptoverfahren in Software verhindern lassen. Das BSI empfiehlt den Einsatz von Kryptobibliotheken, zu denen ggf. die entsprechende Dokumentation und Prüfungsergebnisse bereits vorliegen.

Im Security Target muss der Hersteller neben der Auflistung der von ihm verwendeten kryptographischen Verfahren mit allen Eigenschaften auch im Detail die sicherheitsrelevanten Schritte des jeweiligen Nutzungsszenarios beschreiben.

Hinweis: Schwache Algorithmen sollten nicht angeboten werden. Es kann aber beispielsweise für das Lesen von alten E-Mails Ausnahmen geben. Generell soll der Benutzer in Bezug auf die verwendeten Algorithmen so wenige Entscheidungen wie möglich selbst treffen müssen, insbesondere z. B. was die Verwendung schwächerer Algorithmen angeht.

Im Falle der Verwendung eines asymmetrischen Verfahrens erfolgt die Verschlüsselung der sensiblen Daten unter Verwendung des öffentlichen Schlüssels des Nutzers/Empfängers.

Hinweis: Wie bereits in Kapitel 1.2.1 erwähnt kann es sich hier auch um ein sogenanntes hybrid-asymmetrisches Verfahren handeln, bei dem die Verschlüsselung der sensiblen Daten mit einem geheimen Sitzungsschlüssel im Rahmen eines symmetrischen Verfahrens erfolgt. Der geheime Sitzungsschlüssel ist dann wiederum mit dem öffentlichen Schlüssel des Nutzers/Empfängers im Rahmen eines asymmetrischen Verfahrens verschlüsselt.

Im Falle der Verwendung eines symmetrischen Verfahrens erfolgt die Verschlüsselung der sensiblen Daten unter Verwendung des geheimen Schlüssels des Nutzers. Für die Verwendung des geheimen Schlüssels muss eine entsprechende Autorisierung durch den Nutzer gemäß Anf.Authentisierung erfolgen.

Sicherheitsziel(e): O.Krypto

Anf.Entschlüsselung

Die Entschlüsselung ist das Gegenstück zur Verschlüsselung.

Im Falle der Verwendung eines asymmetrischen Verfahrens kann der Nutzer/Empfänger nur unter Verwendung seines privaten Schlüssels die verschlüsselten Daten entschlüsseln. Für die Verwendung des privaten Schlüssels muss eine entsprechende Autorisierung durch den Nutzer gemäß Anf.Authentisierung erfolgen.

Hinweis: Im Falle der Verwendung eines hybrid-asymmetrischen Verfahrens (wie in Kapitel 1.2.1 erwähnt) werden die zuvor mit dem geheimen Sitzungsschlüssel verschlüsselten sensiblen Daten unter Verwendung desselbigen entschlüsselt. Jedoch kann nur der Besitzer des privaten Schlüssels den zuvor mit seinem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssel diesen für die Entschlüsselung der sensiblen Daten im Rahmen eines symmetrischen Verfahrens auch tatsächlich nutzen.

Im Falle der Verwendung eines symmetrischen Verfahrens kann der Nutzer/Empfänger nur unter Verwendung eines geheimen Schlüssels die verschlüsselten Daten entschlüsseln. Für die Verwendung des geheimen Schlüssels muss eine entsprechende Autorisierung durch den Nutzer gemäß Anf.Authentisierung erfolgen.

Im Security Target muss der Hersteller im Detail die sicherheitsrelevanten Schritte des jeweiligen Nutzungsszenarios beschreiben.

Sicherheitsziel(e): O.Krypto

Anf.Integrität_und_Authentizität

Die E-Mail- und Dateiverschlüsselung muss Algorithmen zur Gewährleistung von Integrität und Authentizität der übertragenen Daten bereitstellen, für die dann die folgenden Anforderungen beachtet werden müssen:

- Die Algorithmen zur symmetrischen bzw. asymmetrischen Integritätssicherung und Daten-Authentisierung müssen vom BSI für diesen Zweck als ausreichend sicher betrachtet werden. Entsprechend müssen die Empfehlungen der Technischen Richtlinie TR-02102 [3] berücksichtigt werden. Abweichungen hiervon müssen mit dem BSI abgestimmt werden.
- Für die Sicherung der Integrität und die Daten-Authentisierung müssen Schlüssel verwendet werden, deren Lebensdauer auf geeignete Weise begrenzt ist. Die Lebensdauer solcher Schlüssel kann nicht allgemeingültig festgelegt werden und muss mit dem BSI abgestimmt werden.

Die Integrität und Authentizität der sensiblen Daten kann der Nutzer/Absender beispielsweise mittels Datensignierung unter Verwendung seines privaten Schlüssels schützen. Für die Verwendung des privaten Schlüssels muss eine entsprechende Autorisierung durch den Nutzer gemäß Anf.Authentisierung erfolgen. Die Signaturprüfung (Verifikation) ist das Gegenstück zur Erstellung einer digitalen Signatur. Mittels einer Signaturprüfung kann der Nutzer/Empfänger feststellen, ob die Integrität und Authentizität der übertragenen Daten gewahrt wurde.

Im Security Target muss der Hersteller die von ihm verwendeten kryptographischen Verfahren im Einzelnen mit allen Eigenschaften auflisten und im Detail die sicherheitsrelevanten Schritte des jeweiligen Nutzungsszenarios beschreiben.

Sicherheitsziel(e): O.Krypto

Anf.Authentisierung

Der Zugriff auf den Master-Key muss mittels Zwei-Faktor-Authentisierung (Besitz und Wissen wie z. B. Hardware-Token und Passwort) kontrolliert werden. Bei jeder Nutzung muss eine Gültigkeitsprüfung des Schlüssels durchgeführt werden.

Unter einer Session wird die Aufrechterhaltung der erfolgreichen Authentisierung des Nutzers gegenüber seinem geheimen oder privaten Master-Key verstanden. Die Gültigkeit einer Session muss zeitlich (in Minuten) begrenzt werden.

Sicherheitsziel(e): O.Authentisierung, O.Schlüsselmanagement

Anf.Schlüsselmanagement

Die E-Mail- und Dateiverschlüsselung muss ein Schlüsselmanagement bereitstellen. Dazu zählen insbesondere die gesicherte Speicherung der Schlüssel und ihrer Attribute sowie die Prüfung der Schlüssel.

Folgende Funktionen müssen zur Verfügung stehen:

- Ein geheimer oder privater Master-Key des Nutzers muss gesichert auf einem geeigneten[1] Hardware-Token gespeichert werden.
- Geheime und private Einzelschlüssel dürfen zu keiner Zeit im Klartext persistent auf dem Client mit der E-Mail- und Dateiverschlüsselung gespeichert werden.
- Sicheres Löschen von geheimen und privaten Schlüsseln, wenn diese nicht mehr benötigt werden. (Das Löschen von Schlüsseln hängt vom Status des Schlüssels in der lokalen Schlüsselhierarchie und vom Schlüsselkonzept ab: Das Löschen von Schlüsseln schließt sowohl das automatische Löschen nach dem temporären Gebrauch der Schlüssel (insbesondere Einzelschlüssel) als auch das Löschen von Schlüsseln nach Ablauf ihrer Gültigkeit (insbesondere Master-Keys) ein.)
- Schlüssel-Vertrauensmodell: Die E-Mail- und Dateiverschlüsselung unterstützt den Nutzer bei der Authentisierung öffentlicher Schlüssel. Um die Authentizität dieser Schlüssel sicherzustellen, wird ein sogenanntes Vertrauensmodell (siehe OSP.Zertifikate) für öffentliche Schlüssel umgesetzt, das vom Hersteller beschrieben werden muss. Der Vertrauensstatus öffentlicher Schlüssel muss bei jeder Nutzung abgefragt werden. Der Nutzer muss über das Ergebnis informiert werden. Wenn der Vertrauensstatus als Schlüsselattribut durch die E-Mail- und Dateiverschlüsselung verwaltet wird, muss dazu ein sicherer Mechanismus verwendet werden.
- Es müssen Schlüssel generiert werden können. Die Schlüssel werden in diesem Fall mit einem vom BSI akzeptierten Verfahren erzeugt oder abgeleitet. Für die Verwendung von Zufallszahlen bei der Schlüsselgenerierung gelten die entsprechenden Anforderungen (siehe Anf.Zufallszahlengenerator).
- Es müssen Schlüssel importiert und exportiert werden können. Für den Import und Export muss dann ein sicherer Mechanismus verwendet werden.

Weitere Schlüsselmanagementfunktionen können erforderlich sein. Alle Schlüsselmanagementfunktionen müssen so gestaltet sein, dass Unbefugte keine Kenntnis von geheimen oder privaten Schlüsseln erlangen können.

Sicherheitsziel(e): O.Schlüsselmanagement

Anf.Zufallszahlengenerator

Die E-Mail- und Dateiverschlüsselung nutzt für die Erzeugung kryptographischer Schlüssel und weiterer notwendiger Zufallszahlen einen Zufallszahlengenerator, der die Anforderungen des BSI an die

1 Ein Hardware-Token wird als geeignet angesehen, wenn es sich beispielsweise um eine zertifizierte Smartcard handelt. Insbesondere soll das Hardware-Token aus dem Client herausnehmbar sein.

Qualität der Zufallszahlen erfüllen muss. Es gibt eine Spezifikation von Anforderungsklassen von Zufallszahlengeneratoren. Zu finden ist diese Spezifikation in den Dokumenten AIS20 [5] und AIS31 [6]. Es gelten bzgl. dieser Spezifikation die unten aufgeführten Anforderungen an einen Zufallszahlengenerator. Perspektivisch muss ein PTG.3 bzw. DRG.4-Generator eingesetzt werden.

- Physikalische Zufallszahlenerzeugung: Wird ein physikalischer Zufallszahlengenerator eingesetzt, so sollte ein PTG.3-Generator im Sinne der AIS31 [6] eingesetzt werden. Übergangsweise kann ein Zufallszahlengenerator der Klasse PTG.2 im Sinne der AIS31 [6] genügen. Dies muss mit dem BSI abgestimmt werden. Ein PTG.2 konformer Zufallszahlengenerator kann durch geeignete kryptographische Nachbearbeitung, etwa durch einen geeigneten deterministischen Zufallszahlengenerator, den Anforderungen der Klasse PTG.3 genügen.
- Deterministische Zufallszahlenerzeugung: Wird ein deterministischer Zufallszahlengenerator eingesetzt, so muss dieser der Anforderungsklasse DRG.4 im Sinne der AIS20 [5] genügen. Übergangsweise kann der Zufallszahlengenerator noch konform sein zur Anforderungsklasse DRG.3 im Sinne der AIS20 [5].

Zusätzliche Informationen zu Zufallszahlengeneratoren und den zuvor genannten Anforderungen finden sich in der Technischen Richtlinie TR-02102 [3], Kapitel 9.

Der Hersteller muss ein Konzept vorlegen, in dem er nachweist, dass er einen Zufallszahlengenerator nutzt, der den hier gestellten Anforderungen genügt. Er kann dabei entweder auf einen bereits zugelassenen Zufallszahlengenerator zurückgreifen oder der Hersteller implementiert einen eigenen Zufallszahlengenerator und erbringt die entsprechenden Nachweise.

Sicherheitsziel(e): O.Krypto

Anf.Zertifikate

Für die Verwendung von Zertifikaten im Rahmen der Sicherheitsfunktionalität der E-Mail- und Dateiverschlüsselung gelten – sofern eine CA (Certification Authority) eingebunden ist - die nachfolgenden Anforderungen:

Grundsätzlich müssen die Einträge der Zertifikate die Policy der ausstellenden CA erfüllen. Es ist festzulegen, welche Einträge die verwendeten Zertifikate mindestens enthalten.

Die Zertifikate müssen hinsichtlich der verwendeten Algorithmen und Schlüssellängen den Anforderungen der Technischen Richtlinie TR-02102 [3] genügen.

Es ist vom Hersteller zu beschreiben, wie die Zertifikate geprüft werden. Die Beschreibung muss ferner darlegen, wie auf das Ergebnis der Zertifikatsprüfung reagiert wird.

Die folgenden Maßnahmen müssen für die Prüfung mindestens ergriffen werden:

- Prüfung der Signaturen der jeweils vollständigen Zertifikatskette;
- es muss sichergestellt sein, dass eine Zertifikatsketten-Verlängerung nicht möglich ist (d.h., dass die Kette der geprüften Zertifikate zwischen dem Root-Zertifikat und dem zu prüfenden Zertifikat eine definierte Maximallänge hat und keine zusätzlichen CA-Zertifikate eingefügt werden können);
- Prüfung der Gültigkeit der Zertifikate;
- Möglichkeit, ausgeschlossene Zertifikate zu erkennen (PKI-aktiver Ausschluss);
- Rollenprüfung.

Sicherheitsziel(e): O.Authentisierung, O.Krypto, O.Schlüsselmanagement

Anf.Administration

Die E-Mail- und Dateiverschlüsselung sollte folgende administrativen Funktionen bereitstellen:

- Installation und Update der E-Mail- und Dateiverschlüsselung,

- Konfiguration der E-Mail- und Dateiverschlüsselung,
- Weitere Managementfunktionen.

Die Managementfunktionen dürfen nur von einem autorisierten Administrator ausgeführt werden.

Sicherheitsziel(e): O.Administration

Anf.Logging

Die E-Mail- und Dateiverschlüsselung muss ein sicheres Logging sicherheitsrelevanter Ereignisse durchführen. Dies können folgende Ereignisse sein:

- Ein- und Ausschalten der Auditfunktion,
- Auslösen eines Alarms im Zusammenhang mit Anf.Selbsttest,
- fehlerhafte Authentisierungsversuche der Nutzer,
- Administratoraktivitäten.

Es sollten dann mindestens die folgenden Angaben aufgezeichnet werden:

- Art des Ereignisses (siehe oben),
- Datum und Zeitpunkt des Ereignisses,
- Detailinformationen zu durchgeführten Operationen.

Es sollten bezüglich der Protokollierung die gemäß des BSI Mindeststandards [11] relevanten Anforderungen erfüllt werden. (Bezüglich der Relevanz wird insbesondere auf die zur Protokollierungsrichtlinie Bund [11] zugehörige technische Dokumentationsdatei [12] verwiesen, die das BSI auf Anfrage zur Verfügung stellt.)

Der Umfang des Logging muss eingestellt werden können.

Die Log-Daten dürfen nur von einem autorisierten Auditor ausgewertet werden.

Sicherheitsziel(e): O.Logging

Anf.Selbsttest

Die E-Mail- und Dateiverschlüsselung muss beim Start und regelmäßig während des Betriebs Selbsttests der sicherheitsrelevanten Funktionen durchführen.

Die Selbsttests müssen unter anderem beinhalten:

- Überprüfung der Authentizität und Integrität der Software einschließlich der Konfigurationsparameter;
- Prüfung der korrekten Ausführung von Kryptoalgorithmen, bevor diese nach dem Laden des Algorithmus oder nach einem Neustart das erste Mal verwendet werden (z.B. Known-Answer-Tests);
- Beim Fehlschlagen von Selbsttests muss die E-Mail- und Dateiverschlüsselung einen sicheren Zustand einnehmen, d. h ein unbefugter Zugriff auf Schlüssel, sensible Daten und Authentisierungsdaten muss verweigert werden;
- Kommandos, Aktionen und Testpunkte, die ausschließlich für die Entwicklungs- und Testphase der E-Mail- und Dateiverschlüsselung benötigt werden, müssen in Produktversionen für den zulassungskonformen Wirkbetrieb entfernt sein.

Sicherheitsziel(e): O.Krypto, O.Logging, O.Update

Anf.Update

Die E-Mail- und Dateiverschlüsselung sollte eine automatisierte und konfigurierbare Update-Prüfung implementieren. Alternativ sollte ein ggf. manueller Prozess in der Umgebung definiert sein, der dieselben Anforderungen erfüllt.

Updates der E-Mail- und Dateiverschlüsselung müssen unverzüglich[2] installiert werden können und vor der Installation mit positivem Ergebnis auf Authentizität und Integrität geprüft werden. Es muss dazu entweder ein sicherer Mechanismus zum Nachladen von Software implementiert sein, sodass nur authentische Software geladen werden kann. Oder alternativ kann ein sicherer Update-Prozess in der Umgebung definiert sein, der dieselben Anforderungen erfüllt.

Durch den Updateprozess sollten keine Konfigurationen verändert werden. Falls dies dennoch erforderlich ist, muss in geeigneter Weise darauf hingewiesen werden.

Für den Fall von Kompatibilitätsproblemen oder auftretender Sicherheitsrisiken sollten Updates rückgängig gemacht und so der vorm Update verwendete Zustand der Software wiederhergestellt werden können.

Der Update-Vorgang sollte so protokolliert werden, dass sicherheitskritische Aktionen nachvollzogen werden können.

Sicherheitsziel(e): O.Update

2 Dass die Installation von Updates *unverzüglich* möglich sein soll, bedeutet hier, dass erstens der Hersteller den Betreiber über ein entstandenes Sicherheitsrisiko umgehend informiert und dass zweitens ein Software-Update in Abhängigkeit von der Höhe des Risikos vom Hersteller so schnell wie möglich zur Verfügung gestellt wird.

5 Hinweise zur Umsetzung der Sicherheitsanforderungen

Dieses Kapitel dient dazu, konkrete Beispiele und Hinweise zur Implementierung einer E-Mail- und Dateiverschlüsselung zu geben. Inwieweit es sich um Beispiele oder Hinweise handelt, ist jeweils durch die Formulierung erkennbar.

Implementierung von kryptographischen Algorithmen

Die vom BSI anerkannten Algorithmen und Protokolle sind detailliert in Standards beschrieben, siehe [3]. Implementierungen dieser Algorithmen und Protokolle, die sich nicht an diese Standards halten, können die Sicherheit beeinträchtigen. Daher ist eine in diesem Sinne korrekte Implementierung der verwendeten Algorithmen und Protokolle zu gewährleisten.

Weiterhin müssen bei der Implementierung unter anderem die folgenden Punkte beachtet werden:

- bei Nonces (z.B. Zufallszahlen), die im Rahmen kryptographischer Protokolle verwendet werden, sind bei Erzeugung und Prüfung die für das jeweilige Protokoll erforderlichen Eigenschaften zu gewährleisten und bei Entgegennahme die vorgesehenen Prüfungen durchzuführen;
- Überprüfung von Rollen;
- Vermeidung von verdeckten Kanälen;
- Härtung gegen Seitenkanalangriffe.

Hinweis: Die dem BSI im Rahmen der Zulassung eines Produktes vom Hersteller vorzulegende Dokumentation muss deutlich machen, wie diese Anforderungen berücksichtigt wurden. In einem an die CC angelehnten Verfahren könnte dies beispielsweise in dem Dokument „Sicherheitsarchitektur“ erläutert sein. Für die Darstellung kryptographischer Abläufe und ihrer Implementierung stellt das BSI in Ergänzung zum Nachweiskatalog [1] ein gesondertes Dokument [4] auf Anfrage zur Verfügung.

Seitens NATO bzw. EU gibt es weitere Anforderungsdokumente [13] und [14], die bei Implementierungen für internationale Zwecke beachtet werden müssen.

Schlüsselmanagement und Umgang mit Zertifikaten

Für die Verwendung von Zertifikaten sollte ferner der Standard [RFC5280] durch die Hersteller berücksichtigt werden. (Hinweis: Die Spezifikation [RFC5280] ist Teil einer Familie von Standards für eine X.509 Public Key Infrastructure (PKI) für das Internet.)

Vom Hersteller ist einerseits zu beschreiben, wie Zertifikate geprüft werden (technisch hart kodiert oder organisatorisch) und ferner, wie auf das Ergebnis der Zertifikatsprüfung reagiert wird. Reaktionen auf eine Zertifikatsprüfung können beispielsweise Warnmeldungen o.ä. sein. Ein Zertifikat muss also nicht in jedem Fall technisch hart kodiert gesperrt werden.

In jedem Fall muss sich der Hersteller jedoch Gedanken machen, wie eine Infrastruktur etabliert wird, die über einen längeren Nutzungszeitraum betreut werden kann. Anteile des Schlüsselmanagements, die außerhalb der E-Mail- und Dateiverschlüsselung ablaufen und für das Produkt erforderlich sind, müssen vom Hersteller beschrieben und bewertet werden.

Composite-Aspekt

Für Teilkomponenten der E-Mail- und Dateiverschlüsselung wie zum Beispiel das verwendete Hardware-Token (Hardware, SC-Middleware) oder den verwendeten Zufallszahlengenerator kann zum Nachweis der Sicherheitseigenschaften auf bereits erteilte CC-Zertifikate oder Zulassungen im Sinne des Composite-Aspektes zurückgegriffen werden. Die vom Hersteller verwendeten Schnittstellen sowie die Eignung der Sicherheitsmechanismen der Teilkomponente müssen dazu detailliert dokumentiert und ihre korrekte Funktion im Rahmen der Zulassung der E-Mail- und Dateiverschlüsselung mit evaluiert werden.

Verfügbarkeit, Performance und weitere funktionale Anforderungen

Im Rahmen der Zulassung durch das BSI werden Anforderungen im Kontext des Geheimschutzes geprüft, so dass das wesentliche dabei geprüfte Sicherheitsziel im Schutz der Vertraulichkeit und Integrität eingestufter Daten besteht. Ein Bedarfsträger oder Betreiber von zugelassenen Geräten und Systemen wird aber weitere Anforderungen haben, etwa die Verfügbarkeit, Performance, Ergonomie und andere. Derartige Ziele werden im Rahmen dieses Anforderungsprofils nicht definiert und geprüft, es wird aber darauf hingewiesen, dass im Rahmen einer Beschaffung und entsprechender Ausschreibungen derartige Anforderungen voraussichtlich gestellt werden. Ein Hersteller sollte also zusätzlich zur Erfüllung der Anforderungen dieses Anforderungsprofils auch prüfen, welche weiteren Anforderungen von Bedarfsträgern und Betreibern er berücksichtigen sollte, damit sein Produkt für deren Zwecke geeignet ist. Er sollte auch potentielle Konflikte im technischen Design beachten, die beispielsweise zwischen Sicherheitsanforderungen einerseits und Performance andererseits häufig auftreten, und beachten, dass auch in Konfliktfällen beide Ziele erreicht werden müssen.

6 Hinweise zum sicheren Betrieb einer E-Mail- und Dateiverschlüsselung

Um eine zugelassene E-Mail- und Dateiverschlüsselung so zu betreiben, dass die Verarbeitung von VS der entsprechenden Einstufung als sicher angesehen werden kann, müssen bestimmte Anforderungen an ihre Einsatzumgebung erfüllt werden.

Verbindlich werden diese Anforderungen im Rahmen der Zulassung eines spezifischen Produktes ausgesprochen. Im Rahmen des Evaluierungs- und Zulassungsverfahren werden die Bedingungen für den sicheren Betrieb in einem Dokument zu Einsatz-und Betriebsbedingungen vom Hersteller verbindlich festgehalten. Dieses Kapitel enthält einige allgemeine Hinweise, die für den Produkttyp E-Mail- und Dateiverschlüsselung gelten:

- Die Einsatzumgebung muss für die Verarbeitung von VS der entsprechenden Einstufung geeignet sein.
- Eine sichere Nutzung der unterliegenden Plattform (das sind i. d. R. die Hardware, das unterliegende Betriebssystem, und eine Softwareapplikation), mit der die E-Mail- und Dateiverschlüsselung verzahnt ist, muss gewährleistet werden; dazu zählen beispielsweise Maßnahmen beim sicheren Start Up der E-Mail- und Dateiverschlüsselung oder das Einrichten einer Zugriffskontrolle, die ggf. mit der der E-Mail- und Dateiverschlüsselung gekoppelt ist, gegebenenfalls Prozessisolierung, Integritätsschutz des Betriebssystems und der Software, Speicherschutzmechanismen, Patch-Management u.a.; vom Hersteller genutzte Mechanismen und Funktionen der unterliegenden Plattform, die die Sicherheitsleistungen seines spezifischen Produktes unterstützen, müssen in der Herstellerdokumentation detailliert beschrieben und bewertet werden.
- Hardware-Token: Es besteht die Möglichkeit, bereits vorhandene Hardware-Token wie elektronischer Dienstausweis, SINA-Card etc., die im Kontext anderer Anwendungen auf dem Nutzer-Client genutzt werden, für die sichere Speicherung des Master-Key zu nutzen. In diesem Fall ist das vorgesehene Nutzungskonzept vom Hersteller detailliert zu beschreiben und vom Hersteller müssen die Nachweise erbracht werden, dass das Nutzungskonzept zur Erfüllung der hier gestellten Sicherheitsanforderungen an die E-Mail- und Dateiverschlüsselung beiträgt und diesen insbesondere nicht widerspricht.
- Der Hersteller muss dem Betreiber bzw. Anwender der E-Mail- und Dateiverschlüsselung eine Regelung anbieten, die dem Betreiber bzw. Anwender zusichert, dass im Fall von aufgedeckten Sicherheitsrisiken ein Update der Software der E-Mail- und Dateiverschlüsselung unverzüglich zur Verfügung gestellt wird.

7 Anhänge

7.1 Glossar

Begriff	Erklärung
Verschlusssache (VS)	Nach § 4 Abs. 1 des Sicherheitsüberprüfungsgesetzes vom 20. April 1994 (BGBl. I S. 867) in der jeweils geltenden Fassung sind Verschlusssachen (VS) im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse unabhängig von ihrer Darstellungsform (z. B. Schriftstücke, Zeichnungen, Karten, Fotokopien, Lichtbildmaterial, elektronische Dateien und Datenträger, elektrische Signale, Geräte, technische Einrichtungen oder das gesprochene Wort). Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung in Geheimhaltungsgrade eingestuft.
Einstufung / Geheimhaltungsgrade	VS sind je nach dem Schutz, dessen sie bedürfen, gemäß § 4 Abs. 2 des Sicherheitsüberprüfungsgesetzes in folgende Geheimhaltungsgrade einzustufen: STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann, GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann, VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann, VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.
Produkttyp	Ein Produkttyp ist ein Menge von Produkten, die ein vorgegebenes Set an Sicherheits-Grundfunktionen umsetzen und zusätzlich für gleiche Einsatzzwecke vorgesehen sind und dafür gegebenenfalls dieselbe Technologie verwenden.
VS-Anforderungsprofil (VS-AP)	Ein VS-Anforderungsprofil ist ein Dokument, das die Anforderungen an einen Produkttyp von ISS festlegt.
VS-Zulassung	VS-Zulassung bezeichnet den Prozess im BSI, der dazu dient die Eignung von ISS-Produkttypen zum Schutz eingestufter Informationen festzustellen.
Kryptographische Schlüssel	Der Begriff Schlüssel wird hier als Oberbegriff für alle im Produkt verwendeten Schlüssel benutzt. Insofern eine genauere Beschreibung eines kryptographischen Schlüssels notwendig ist, werden dazu folgende Terme verwendet: geheim, privat, öffentlich, Zertifikat, Master-Key, Einzelschlüssel und Sitzungsschlüssel. **Geheimer Schlüssel:** Bei symmetrischen Verfahren verwenden beide Kommunikationspartner denselben **geheimen** Schlüssel sowohl zum Ver- als auch zum Entschlüsseln.

Begriff	Erklärung
	Privater/öffentlicher Schlüssel: Bei einem asymmetrischen Verfahren wird ein Schlüsselpaar benutzt, das aus einem geheimen Teil (**privater** Schlüssel) und einem nicht geheimen Teil (**öffentlicher** Schlüssel) besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Besitzer des privaten Schlüssels zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Der private Schlüssel ermöglicht es seinem Besitzer, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren. **Zertifikat:** Public-Key-Zertifikate nach dem Standard X.509 bestätigen die Identität des Inhabers und weitere Eigenschaften eines öffentlichen Schlüssels. **Master-Key:** Master-Keys bilden die Wurzel einer Schlüsselhierarchie. **Einzelschlüssel:** Einzelschlüssel sind mit dem Master-Key verschlüsselte und damit kryptographisch geschützte Schlüssel. **Sitzungsschlüssel:** Ein Sitzungsschlüssel ist ein zufällig generierter Schlüssel, der im Rahmen einer Sitzung einmalig verwendet werden.

Tabelle 1: Glossar

7.2 Abkürzungen

Abkürzung	Bedeutung
AP	Anforderungsprofil
CC	Common Criteria
ISS	Informationssichernde Systeme (wird im VS-Kontext verwendet)
S/MIME	Secure/Multipurpose Internet Mail Extensions
OpenPGP	Open Pretty Good Privacy
PKI	Public Key Infrastructure
IPC	Interprocess communication
MDC	Modification Detection Code
AE/AEAD	Authenticated Encryption/Authenticated Encryption with Associated Data
VS	Verschlusssache
VSA	Verschlusssachenanweisung
VS-AP	Anforderungsprofil für die Sicherheit informationssichernder Systeme im VS-Bereich
VS-NfD	VS-NUR FÜR DEN DIENSTGEBRAUCH
GHB	Geheimschutzhandbuch
MAC	Message Authentication Code

Tabelle 2: Abkürzungsverzeichnis

8 Literaturverzeichnis

[1] Nachweise für eine Evaluierung für eine Zulassung bis VS-NfD, BSI, Version 1.3, August 2015

[2] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), Vom 10. August 2018, BMI, 2018

[3] TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teile 1–4, BSI, 2018

[4] Detailspezifikation kryptographischer Abläufe und Mechanismen, BSI, Version 1.0, 2015
(Das Dokument kann beim BSI https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/FAQ/faq_node.html#faq9734106 angefordert werden.)

[5] AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, BSI, Version 3, 2013

[6] AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, Version 3, 2013

[7] AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, BSI, Version 3, 2013

[8] Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels, https://efail.de/efail-attack-paper.pdf

[9] Geheimschutzhandbuch. Handbuch für Geheimschutz in der Wirtschaft. 2004, Stand 23.08.2017

[10] VS-Anforderungsprofil für eine Festplattenverschlüsselung, BSI, Version 1.0, BSI-VS-AP-0008-2018

[11] Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 15.10.2018
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards_Bund/PDCA/PDCA.html

[12] Auszug aus den technischen Dokumentations- und Konfigurationsdateien der Protokollierungsrichtline Bund (PR-B) bzgl. E-Mail-Systeme/-Plugins [Netzsicht – Stufe 7]
(Das Dokument kann beim BSI über den Kontakt protokollierungsrichtlinie@bsi.bund.de angefordert werden.)

[13] IASP 2, EU Council INFORMATION ASSURANCE SECURITY POLICY ON CRYPTOGRAPHY, 30.05.2011

[14] AC/322-D/0047-REV2, NATO INFOSEC TECHNICAL AND IMPLEMENTATION DIRECTIVE ON CRYPTOGRAPHIC SECURITY AND CRYPTOGRAPHIC MECHANISMS , Revision 2, 11.03.2009