[redacted]

[redacted]

Untersuchung TrueCrypt

Arbeitspaket 2

Use Cases (Anwendungsfälle)

[redacted]

Version:	1.2
Datum:	16. November 2010

VS – NUR FÜR DEN DIENSTGEBRAUCH

Historie

Version	Autor	Kommentar	Datum
0.1	[redacted]	Initiale Dokumentenversion erstellt	09.08.10
0.5		Überarbeitung nach KickOff-Meeting	26.08.10
0.6		Kleine Änderungen, UML als Beispiel	30.08.10
0.7		Komplett überarbeitet, neue Struktur	03.09.10
0.8		Änderungen nach Telko vom 6.9.2010	08.09.10
0.85		Änderungen nach Meeting vom 10.09.2010 Anwendungsfall 1 aufgeteilt in zwei Fälle	15.09.10
1.0		Änderungen Rückmeldung vom BSI	22.09.10
1.01		Schreibweisen angepasst	28.09.10
1.02		ASE_SPD aus AP3 übernommen	02.11.10
1.1		Final Review	03.11.10
1.11		Kommentare aus Review eingearbeitet	04.11.10
1.2		Version zur Abnahme von AP3	16.11.10

Inhaltsverzeichnis

1 Einleitung....4
1.1 Definitionen....4
2 Anwendungsfälle....6
2.1 Schutz von VS an einem stationären VS-Arbeitsplatz....6
2.2 Schutz von VS an einem Mehrbenutzer-VS-Arbeitsplatz....9
2.3 Schutz von VS an einem mobilen VS-Arbeitsplatz....11
2.4 Schutz inaktiver VS-Datenträgern bei Verbringung....13
2.5 Schutz der VS bei Verlust durch Abhandenkommen / Diebstahl....15
2.6 Sicheres Löschen von Datenträgern mit VS....16
3 ASE_SPD.NfD....17
3.1 Annahmen Operational Environment....17
3.2 Organisatorische Sicherheitsrichtlinien....18
3.3 Erläuterungen....20
3.4 Bedrohungen....21

1 Einleitung

In diesem Dokument werden die grundsätzlichen Anwendungsfälle einer Partitions- bzw. Festplattenverschlüsselung beschrieben.

Hierbei wird der Anwendungsfall kurz beschrieben und dann, falls anwendbar, die folgenden Punkte dargestellt:

1. Wer das Produkt in dem Anwendungsfall einsetzen kann (Akteure).
2. Unter welchen Rahmenbedingungen es eingesetzt werden kann (Vorbedingungen).
3. Welche Schutzziele erreicht werden.
4. Wie es eingesetzt werden kann (Zusammenspiel der Vorbedingungen, der Akteure, von Ereignissen sowie der Umgebung und der Nachbedingungen) als Standardablauf und der möglichen Alternativen.
5. Welche Sicherheitsleistungen von einem Produkt Festplattenverschlüsselung in dem Anwendungsfall erbracht werden müssen, um die Schutzziele zu erreichen.
6. Welche Einschränkungen gelten und welche Sicherheitsleistungen nicht erbracht werden (können), obwohl diese von einem Laien (bezüglich IT-Sicherheit) erwartet würden.
7. Welche Nachbedingungen gelten.
8. Welche anderen Anwendungsfälle in diesem Anwendungsfall verwendet werden.

1.1 Definitionen

aktiv	Bezeichnet den Systemstatus der Festplattenverschlüsselung: • Das Betriebssystem ist gestartet. • Der Benutzer ist authentisiert. • Die verschlüsselte Partition / Festplatte wird von der Festplattenverschlüsselung transparent entschlüsselt.
inaktiv	Bezeichnet den Systemstatus der Festplattenverschlüsselung: • Die verschlüsselte Partition / Festplatte wird zur Zeit nicht von der Festplattenverschlüsselung entschlüsselt.
Verschlusssache (VS)	Mit Verschlusssache sind hier immer Inhalte bis höchstens der Geheimhaltungsstufe „VERSCHLUSSSACHE - NUR FÜR DEN DIENSTGEBRAUCH" gemeint.
Innentäter	Ein Innentäter hat einen Zugang auf dem System, allerdings mit einem eigenen Passwort.
Außentäter	Ein Außentäter hat lediglich physikalischen Zugriff auf das System.
Diensträume	Eine Umgebung, die für das Bearbeiten von VS geeignet ist. Sie zeichnet sich wie folgt aus: • Geschlossener Benutzerkreis • Abschließbare Räume und Schränke

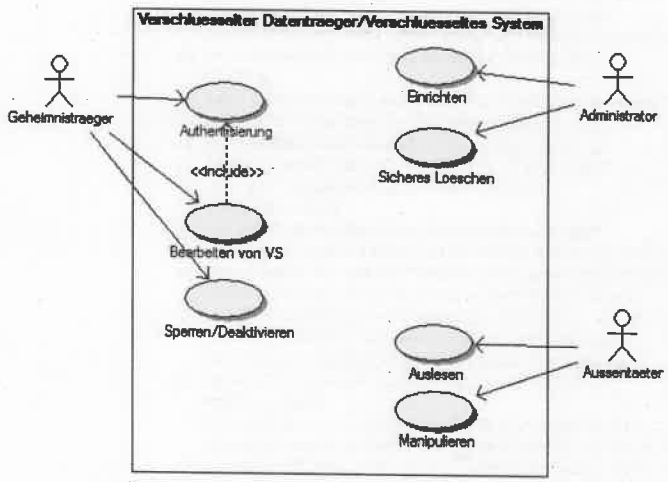
	(Zugangskontrolle) • Der Zugriff auf Systeme in diesen Räumen wird für externe Angreifer organisatorisch verhindert • Der Zugriff auf Systeme durch Innentäter ist möglich

2 Anwendungsfälle

2.1 Schutz von VS an einem stationären VS-Arbeitsplatz

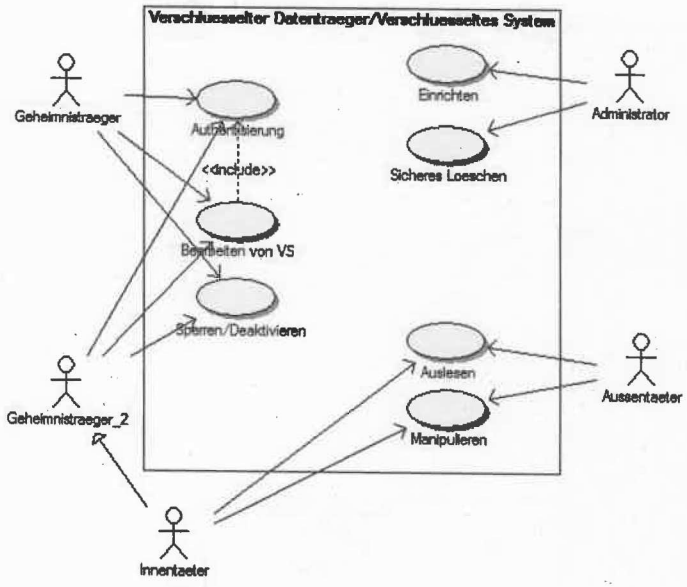
Schutz von VS an einem stationären VS-Arbeitsplatz (Dedicated)	
Beschreibung:	Ein System (z.B.: PC), welches sich in Diensträumen befindet und benutzt wird, um VS zu bearbeiten. Alle Benutzer haben dieselbe Sicherheitsfreigabe und denselben Kenntnisbedarf (Need-to-know-Prinzip) .
Akteure:	1. Geheimnisträger, der mit der Bearbeitung von VS betraut ist. 2. Administrator 3. Angreifer: Außentäter (z.B. Wartungspersonal)
Vorbedingungen:	1. Der Nutzer muss im Umgang mit dem System und den Sicherheitsmaßnahmen entsprechend geschult sein. 2. Die Regelungen des BSI Grundschutzhandbuches für Passworte werden angewendet. 3. Das BIOS muss durch ein Passwort geschützt sein 4. Das Booten von anderen Medien außer der Systemplatte darf nicht möglich sein. 5. Der PC muss gegen Manipulation gesichert sein, insbesondere gegen Öffnen oder Herausnehmen der Systemfestplatte (z.B. durch Siegel) und gegen das Anbringen eines Keyloggers. Dieses gilt auch für den Servicefall bei dem entsprechende Maßnahmen zu ergreifen sind. 6. Ein entsprechender Schutz (z.B.: Firewall) ist einzurichten, wenn das System direkt oder über ein internes Netzwerk mit dem Internet verbunden ist. 7. Geräte mit Funkübertragung (z.B.: Tastaturen) dürfen nur genutzt werden, wenn Sie vom BSI zugelassen sind. 8. Das System und die Datenträger sind regelmäßig auf den Befall von Viren mit einer geeigneten Software zu prüfen. 9. Die Festplattenverschlüsselung muss vom BSI zugelassen sein. 10. Das Betriebssystem ist aktuell zu halten. 11. Das Betriebssystem kontrolliert die Schnittstellen. 12. Die Festplattenverschlüsselung verschlüsselt die Systempartition sowie alle Datenpartitionen, dies war auch schon vor dem ersten Kontakt des Systems mit VS der Fall. 13. Ist es erforderlich, die VS später außerhalb der Diensträume zu verbringen, so ist entweder die VS oder der Datenträger mit einer vom BSI zugelassenen Verschlüsselungssoftware zu verschlüsseln. Hierzu kann z.B. eine Partitions- / Festplattenverschlüsselung auf den

	Datenträgern eingesetzt werden.
Schutzziele:	1. Vertraulichkeit der VS 2. Schutz vor gezielter Manipulation
Einsatz der Festplatten-verschlüsselung:	1. Der Nutzer authentisiert sich an der Festplattenver-schlüsselung mit einem Passwort und einem Security Token. 2. Verlässt der Benutzer das System, so ist der Zugriff auf das System derart zu sperren, dass Unbefugte keinen Zugriff erlangen können. (z.B.: herunterfahren)
Sicherheitsleistungen der Festplattenver-schlüsselung:	1. Vertraulichkeit der VS in der Zeit, in der die Festplattenverschlüsselung **inaktiv** ist.
Einschränkungen:	1. Die Integrität der Daten wird durch eine Festplattenver-schlüsselung nicht im strikten Sinne gewährleistet. *Hinweise:* *Ein Angreifer kann, wenn er zu zwei Zeitpunkten Zugriff erlangt, zwischen denen Daten durch einen befugten Benutzer geändert wurden, die neuen Daten mit den alten Daten überschreiben, eventuell auch nur teilweise (z.B. Blockweise), ohne dass der Angriff entdeckt würde.* *In der Regel ist es für einen Angreifer aber nicht möglich, Daten gezielt so zu verändern, um einen Nutzen daraus zu ziehen.* *Angreifer (auch Innentäter) können durch Manipulation die Vertraulichkeit erfolgreich kompromittieren, falls die Vorbedingungen nicht eingehalten werden.* 2. *Falls die Schutzziele in Gefahr sind, wenn der Benutzer Administratorrechte erlangen sollte, so muss stattdessen Szenario 2.2 angewandt werden.*
Nachbedingungen:	1. Das Löschen der VS beinhaltenden Datenträgern kann über eine Software erfolgen, welche den Datenträger mindestens zweimal mit zufälligen Werten überschreibt, oder durch die entsprechende Löschfunktion der zugelassenen Festplattenverschlüsselungssoftware, wobei zu beachten ist, dass sämtliche Backups (auch der Header) gelöscht werden müssen. (siehe 2.6)
andere Anwendungsfälle:	1. Sicheres Löschen von Datenträgern mit VS 2. Schutz der VS bei Verlust durch Abhandenkommen / Diebstahl 3. Schutz inaktiver VS-Datenträger bei Verbringung



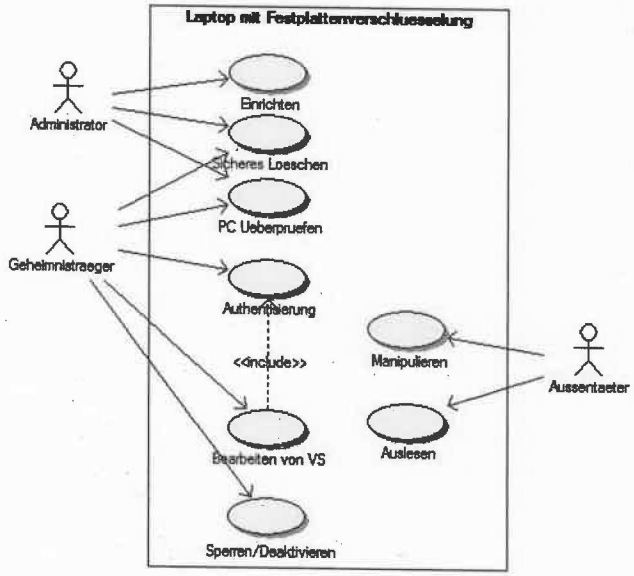
2.2 Schutz von VS an einem Mehrbenutzer-VS-Arbeitsplatz

Schutz von VS an einem Mehrbenutzer-VS-Arbeitsplatz (System High)	
Beschreibung:	Wie bei Szenario 1, aber verschiedene Benutzer haben unterschiedlichen Kenntnisbedarf (Need-to-know-Prinzip)
Akteure:	1. Alle Akteure aus Anwendungsfall 1 2. Geheimnisträger 2 (und eventuell weitere), der mit der Bearbeitung von anderen VS betraut ist (tritt möglicherweise als Innentäter auf)
Vorbedingungen:	1. Alle Vorbedingungen aus Anwendungsfall 1 2. Das Betriebssystem setzt eine Benutzertrennung durch
Schutzziele:	1. Vertraulichkeit der VS 2. Schutz vor gezielter Manipulation
Einsatz der Festplatten-verschlüsselung:	1. Der Nutzer authentisiert sich an der Festplattenver-schlüsselung mit einem Passwort und einem Security Token. 2. Verlässt ein Benutzer das System, so ist der Zugriff auf das System derart zu sperren, dass Unbefugte, auch der jeweils andere Geheimnisträger, keinen Zugriff erlangen können. (z.B.: ausloggen / herunterfahren)
Sicherheitsleistungen der Festplattenver-schlüsselung:	1. Vertraulichkeit der VS in der Zeit, in der die Festplattenverschlüsselung **inaktiv** ist. 2. Aufrechterhalten der Benutzertrennung des Betriebssystems
Einschränkungen:	1. Die **Integrität der Daten** sowie die **Integrität des Systems** wird durch eine Festplattenverschlüsselung nur eingeschränkt gewährleistet (siehe Anwendungsfall 1).
Nachbedingungen:	1. Das Löschen der VS beinhaltenden Datenträgern kann über eine Software erfolgen, welche den Datenträger mindestens zweimal mit zufälligen Werten überschreibt, oder durch die entsprechende Löschfunktion der zugelassenen Festplattenverschlüsselungssoftware, wobei zu beachten ist, dass sämtliche Backups (auch der Header) gelöscht werden müssen. (siehe 2.6)
andere Anwendungsfälle:	1. Schutz von VS an einem stationären VS-Arbeitsplatz 2. Sicheres Löschen von Datenträgern mit VS 3. Schutz der VS bei Verlust durch Abhandenkommen / Diebstahl 4. Schutz inaktiver VS-Datenträgern bei Verbringung



2.3 Schutz von VS an einem mobilen VS-Arbeitsplatz

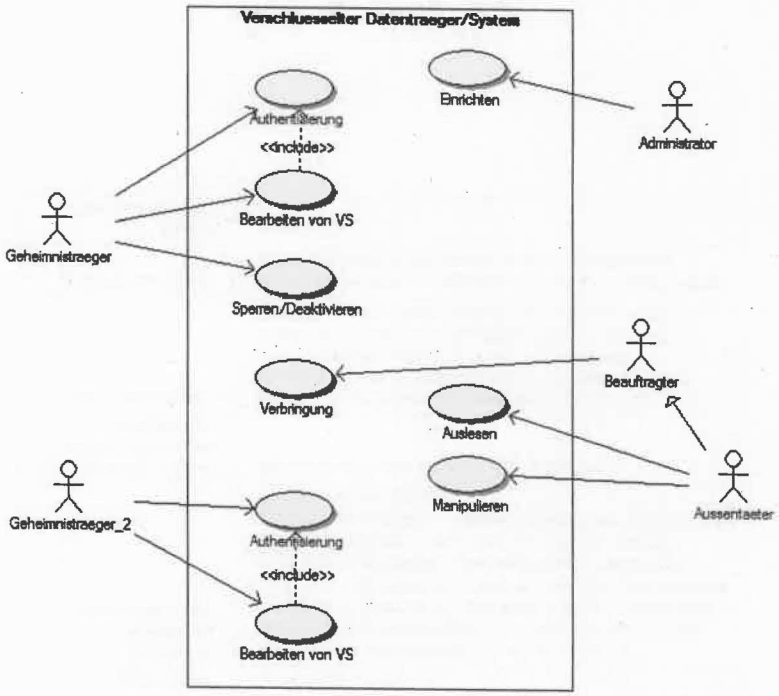
Schutz von VS an einem mobilen VS-Arbeitsplatz	
Beschreibung:	Ein mobiles System (z.B.: Laptop), welches außerhalb von Diensträumen eingesetzt wird, um VS zu bearbeiten.
Akteure:	1. Geheimnisträger, der mit der Bearbeitung von VS betraut ist. 2. Administrator 3. Angreifer
Vorbedingungen:	1. Alle Vorbedingungen aus Anwendungsfall 1 2. Der Benutzer muss sicherstellen, dass er seinen eigenen PC vor sich hat. 3. Ist eine Verbindung in ein internes (Behörden-) Netzwerk nötig, so muss diese über eine vom BSI zugelassene VPN-Lösung erfolgen. 4. Die duchsetzenden Sicherheitsfunktionen (VPN / Festplattenverschlüsselung) müssen separiert sein, hierzu ist eine vom BSI zugelassene Lösung einzusetzen.
Schutzziele:	1. Vertraulichkeit der VS 2. Schutz vor gezielter Manipulation
Einsatz der Festplatten-verschlüsselung:	1. Der Nutzer authentisiert sich an der Festplattenverschlüsselung mit einem Passwort und einem Security Token. 2. Verlässt der Benutzer das System, so ist das System herunterzufahren, bzw. die Festplattenverschlüsselung zu deaktivieren, um Cold-Boot-Angriffe zu verhindern.
Sicherheitsleistungen der Festplattenverschlüsselung:	1. Vertraulichkeit der VS in der Zeit, in der die Festplattenverschlüsselung **inaktiv** ist.
Einschränkungen:	1. Die **Integrität der Daten** sowie die **Integrität des Systems** wird durch eine Festplattenverschlüsselung nur eingeschränkt gewährleistet (siehe Anwendungsfall 1).
Nachbedingungen:	1. Das Löschen der VS beinhaltenden Datenträgern kann über eine Software erfolgen, welche den Datenträger mindestens zweimal mit zufälligen Werten überschreibt, oder durch die entsprechende Löschfunktion der zugelassenen Festplattenverschlüsselungssoftware, wobei zu beachten ist, dass sämtliche Backups (auch der Header) gelöscht werden müssen. (siehe 2.6)
andere Anwendungsfälle:	1. Sicheres Löschen von Datenträgern mit VS 2. Schutz der VS bei Verlust durch Abhandenkommen / Diebstahl 3. Verbringung von Datenträgern mit VS



2.4 Schutz inaktiver VS-Datenträgern bei Verbringung

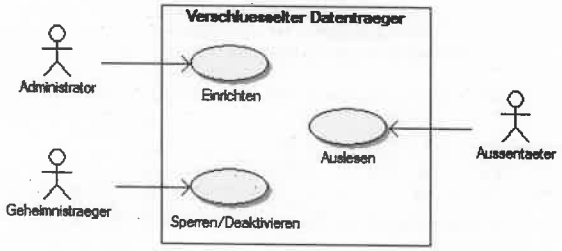
Schutz Inaktiver VS-Datenträgern bei Verbringung	
Beschreibung:	Inaktive Datenträger mit VS (z.B.: USB-Sticks) oder Systeme (z.B.: Notebooks) sollen außerhalb der Diensträumen verbracht werden. Die Datenträger bzw. Systeme sind nicht in Betrieb.
Akteure:	1. Mit der Verbringung beauftragte, nicht vertrauenswürdige Person(en). 2. Ein oder mehrere Geheimnisträger, die mit der Bearbeitung von VS betraut sind. 3. Administrator 4. Angreifer
Vorbedingungen:	1. Die Datenträger bzw. das komplette System wurden mit einer zugelassenen Festplattenverschlüsselung verschlüsselt. 2. Sender und Empfänger besitzen beide den Schlüssel. Falls diese Rollen von verschiedenen Personen ausgeübt wird, muss vorher ein Schlüsselaustausch auf sicherem Wege stattgefunden haben.
Schutzziele:	1. Vertraulichkeit der VS 2. Schutz vor gezielter Manipulation
Einsatz der Festplatten-verschlüsselung:	Während der Verbringung wird die Software zur Festplattenverschlüsselung nicht benötigt.
Sicherheitsleistungen der Festplattenver-schlüsselung:	1. Vertraulichkeit der VS in der Zeit, in der sie verbracht wird
Einschränkungen:	1. Die **Integrität der Daten** sowie die **Integrität des Systems** wird durch eine Festplattenverschlüsselung nicht gewährleistet (siehe Anwendungsfall 1).
Nachbedingungen:	1. Das Löschen der VS beinhaltenden Datenträgern kann über eine Software erfolgen, welche den Datenträger mindestens zweimal mit zufälligen Werten überschreibt, oder durch die entsprechende Löschfunktion der zugelassenen Festplattenverschlüsselungssoftware, wobei zu beachten ist, dass sämtliche Backups (auch der Header) gelöscht werden müssen. (siehe 2.6)
andere Anwendungsfälle:	2. Sicheres Löschen von Datenträgern mit VS 3. Schutz der VS bei Verlust durch Abhandenkommen / Diebstahl

VS – NUR FÜR DEN DIENSTGEBRAUCH



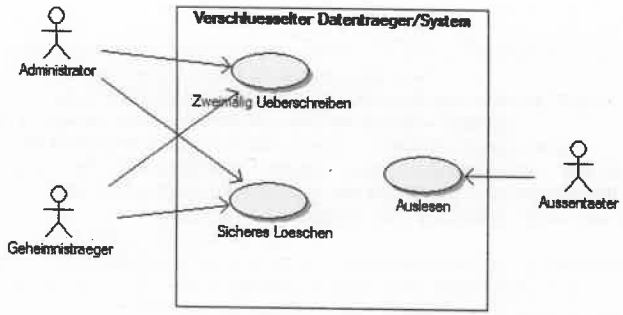
2.5 Schutz der VS bei Verlust durch Abhandenkommen / Diebstahl

Schutz der VS bei Verlust durch Abhandenkommen / Diebstahl	
Beschreibung:	Der Schutz von VS, die auf inaktiven Datenträgern bzw. Systemen gespeichert sind, soll nach Verlust gewährleistet werden.
Akteure:	1. Geheimnisträger, der mit der Bearbeitung von VS betraut ist. 2. Administrator 3. Angreifer (erlangt den Datenträger/das System als Fund oder per Diebstahl)
Vorbedingungen:	1. Die Datenträger bzw. das komplette System wurden vor dem Verlust mit einer zugelassenen Festplattenverschlüsselung verschlüsselt.
Schutzziele:	1. Vertraulichkeit der VS
Einsatz der Festplatten-verschlüsselung:	Die Festplattenverschlüsselung wird vor dem Verlust eingesetzt.
Sicherheitsleistungen der Festplattenver-schlüsselung:	1. Vertraulichkeit der VS, nach dem Verlust.
Einschränkungen:	1. Keine
Nachbedingungen:	1. Taucht der verloren gegangene Datenträger bzw. das System wieder auf, so ist dessen Integrität nicht sichergestellt.
Andere Anwendungsfälle:	Keine



2.6 Sicheres Löschen von Datenträgern mit VS

Sicheres Löschen von Datenträgern mit VS	
Beschreibung:	Sicheres Löschen der Datenträger auf denen VS gespeichert sind.
Akteure:	1. Geheimnisträger, die mit der Bearbeitung von VS betraut sind. 2. Administrator 3. Angreifer
Vorbedingungen:	1. Die Datenträger bzw. das komplette System wurden vor dem ersten Aufbringen von VS mit einer zugelassenen Festplattenverschlüsselung verschlüsselt.
Schutzziele:	1. Vertraulichkeit der VS
Einsatz der Festplatten-verschlüsselung:	Anstelle des zeitintensiven Löschens des VS beinhaltenden Datenträgers, bei dem der Datenträger mindestens zweimal mit zufälligen Werten überschrieben wird, kann die Funktion „Sicheres Löschen" der vom BSI zugelassenen Festplattenverschlüsselungssoftware eingesetzt werden. Dabei wird der Header zerstört, sodass auch mit den richtigen Authentisierungsdaten kein Zugriff mehr möglich ist.
Sicherheitsleistungen der Festplattenver-schlüsselung:	1. Vertraulichkeit der VS nach dem Löschen.
Einschränkungen:	1. Existiert eine Sicherheitskopie der sogenannten Headerdaten der Festplattenverschlüsselung, ist die Löschung wirkungslos, d.h. es kann nach einer Wiederherstellung des Headers wie zuvor mit den richtigen Authentisierungsdaten zugegriffen werden.
Nachbedingungen:	1. Wenn während des Vorgangs „Sicheres Löschen" Fehler auftreten, ist der Datenträger sicher zu vernichten.
Andere Anwendungsfälle:	Keine



3 ASE_SPD.NfD

Die folgenden Annahmen zum Operational Environment und Organisatorische Sicherheitsrichtlinien wurden nach der in AP3 durchgeführten Sicherheitsanalyse ermittelt. Die Nummerierung der einzelnen Punkte ist von dort übernommen. Aus den Angriffsbäumen dort können so auch umfangreichere Informationen über die Erforderlichkeit und die genaue Umsetzung eingesehen werden.

Mit (*) markierte Punkte können entweder nicht mit der momentanen Version von TrueCrypt erfüllt werden und benötigen eine Erweiterung bzw. Zusatzsoftware oder sind anderweitig problematisch, siehe dazu AP3, Kapitel 6.1.
Mit (**) markierte Punkte werden im nachfolgenden Kapitel 3.3 (entspricht AP3, Kapitel 4.1) kurz näher erläutert.

3.1 Annahmen Operational Environment

A1 Der System-Administrator ist vertrauenswürdig.
A4 ATA-TRIM ist deaktiviert.
A5 Die Kryptoalgorithmen sind sicher.
- A5.1 Die Kryptoalgorithmen sind korrekt implementiert.
- A5.2 Es wird ein sicherer Kryptoalgorithmus verwendet.
- A5.3 Es wird ein sicherer Betriebsmodus verwendet.
- A5.4 Die Kryptoalgorithmen werden innerhalb ihrer Parameter eingesetzt.

A8 Es wird eine Integritätssicherung durchgeführt.(*)(**)
- A8.1 Es wird eine blockweise Integritätssicherung durchgeführt.(*)
- A8.2 Es wird eine vollständige Integritätssicherung durchgeführt.(*)

A11 Unnötige Anzeigen werden unterbunden.(*)(*)
- A11.1 Die Anzeige von Schlüsselmaterial wird unterbunden.
- A11.2 Die Anzeige von Zufallsmaterial wird unterbunden.

A12 Es wird ein sicherer Zufallsgenerator verwendet. (**)
A15 Es wird ein zertifizierter Smartcard-Leser eingesetzt. (**)
- A15.1 Die Verbindung zwischen Rechner und Smartcard ist sicher. (**)

- A15.2 Die Benutzer sind geschult im Umgang mit dem Smartcard-Leser.
- A15.3 Die Smartcard wird nur für Festplattenverschlüsselung benutzt.

A16 Das Betriebssystem ist sicher.(*)
- A16.1 Das Betriebssystem setzt eine Benutzertrennung zuverlässig durch.
- A16.2 Es ist keine relevante Sicherheitslücke in Betriebssystem oder Drittsoftware vorhanden.
- A16.3 Das Betriebssystem oder Drittsoftware schützt vor Angriffen über das Netz.

A17 Innerhalb des Volumes sind die Zugriffsrechte geeignet beschränkt.
A18 Es werden nur die Funktionen benutzt, die keine Administratorrechte seitens des Benutzers erfordern.
A19 Ein benutzter Passwort-Cache ist nach Benutzern getrennt.
A14 Es wird eine passend zertifizierte Smartcard verwendet.
A20 Angriffe über externe Schnittstellen werden verhindert.
- A20.1 Erweiterungssteckplätze sind gegen Zugang von außen logisch oder physikalisch abgesichert. Dies kann z.B. durch Deaktivieren der Treiber oder physikalisches Unbrauchbarmachen sichergestellt werden.
- A20.2 Firewire-Anschlüsse sind gegen Zugang von außen logisch oder physikalisch abgesichert. (Treibereinstellungen/IOMMU)

A21 Das Booten von anderen Quellen als der eingebauten Festplatte ist im BIOS deaktiviert.
- A21.1 Das BIOS ist mit einem Passwort vor Veränderung geschützt.
- A21.2 Der Veränderungsschutz des BIOS lässt sich nicht durch ein Masterpasswort umgehen.
- A21.3 Es wird ein Rechner verwendet, bei dem das Rücksetzen der BIOS-Einstellungen nicht trivial möglich ist.
- A21.4 Das Laden eines Erweiterungs-BIOS ist im BIOS abgeschaltet.

A25 Die Speichermodule werden mittels Kleber fixiert und isoliert. (*)
A26 Zur Abwehr von Cache-Timing-Angriffen auf AES wird eine Hardwarebeschleunigung eingesetzt.
A27 Geheim zu haltende Algorithmen müssen entweder vom System getrennt sein oder durch einen öffentlichen Kryptoalgorithmus geschützt werden. (*) (*)
A28 Das System ist verschlüsselt.
- A28.1 Der Auslagerungsspeicher wird verschlüsselt.
- A28.2 Alle möglichen Orte für temporäre Dateien sind verschlüsselt.

A31 Der Quelltext wurde vollständig auf Fehler und Hintertüren untersucht.
A32 Es wird ein von einer vertrauenswürdigen Instanz kompilierter oder verifizierter Binärcode verwendet.

3.2 Organisatorische Sicherheitsrichtlinien

A2 Das Volume muss vor oder bei dem Formatieren sicher gelöscht werden.
- A2.1 Es darf insbesondere kein Quickformat verwendet werden.

A3 Auf dem Datenträger wurden vor dem Einsatz der Festplattenverschlüsselung und auch während des Einsatzes nie sensible

Daten im Klartext gespeichert.

A6 Umschlüsseln (*)

A6.1 Durch Mitzählen der verschlüsselten Datenmenge wird rechtzeitig ein Umschlüsseln erzwungen. Der Zähler wird sicher gespeichert.(*)

A6.2 Wird eine Verschleierung von Änderungen gewünscht, muss das Volume vollständig umgeschlüsselt werden.

A6.3 Beim Entzug von Zugriffsrechten auf ein Volume wird dieses Volume vollständig umgeschlüsselt.

A7 Der Datenträger wird durch Siegel vor unbemerkter Benutzung geschützt. (**)

A9 Es wird verhindert, dass mehrere Versionen eines Datenträgers mit dem gleichen Schlüssel vorhanden sind.

A9.1 Es werden nur physikalische Datenträger, also keine Container, benutzt.

A9.2 Physikalische Datenträger werden nicht bitweise geklont.

A10 Es sind sicher verwahrte Backups der Header vorhanden. (**)

A13 Sicherer Umgang mit Authentisierungsmerkmalen.

A13.1 Es werden sichere Passwörter verwendet.

A13.2 Passwörter werden sicher behandelt.

A20.3 Der Docking-Port wird behandelt wie alle darüber verfügbaren Anschlüsse

A20.4 Docking-Stationen werden genauso behandelt wie der zugehörige PC.

A22 Vor jedem Start wird die physikalische Integrität des Rechners und aller mit ihm verbundener weiterer Komponenten durch den Benutzer überprüft, z.B. durch Siegel.

A22.1 Der Benutzer stellt sicher, dass er ein ihm bekanntes System vor sich hat.

A22.2 Der Benutzer versichert sich, dass alle Komponenten des Systems unverändert sind.

A22.3 Der Benutzer überprüft vor jedem Systemstart die Integrität der Schnittstellen.

A23 Der Benutzer ist geschult im sicheren Umgang mit dem System.

A24 Bei Abwesenheit des Benutzers muss dafür gesorgt werden, dass keine sensiblen Daten und Schlüssel im RAM mehr gespeichert sind.

A24.1 Beim regulären Herunterfahren müssen Daten und Schlüssel aus dem RAM gelöscht werden. (*)

A24.2 Nach ungesichertem Ausschalten und Abstürzen muss der Benutzer den ausgeschalteten Rechner mehrere Minuten beaufsichtigen.

A29 Bei der Deinstallation dürfen keine Informationen bezüglich der verarbeiteten sensiblen Daten mehr im System enthalten sein.

A29.1 Bei der Deinstallation wird der Swap sicher gelöscht.

A29.2 Es müssen alle freien Bereiche innerhalb des verschlüsselten Volumes vor der Deinstallation sicher gelöscht sein.

A30 Alle zu installierenden Dateien werden zuvor per Signatur auf ihre Integrität geprüft.

3.3 Erläuterungen

Zu A2.1 (Quickformat)

Es wird von TrueCrypt die Option „Quickformat" angeboten. Wenn sie aktiviert ist, werden nur die Verwaltungsinformationen für das Dateisystem verschlüsselt geschrieben. Der weitere (freie) Platz wird nicht berührt. Die dort enthaltenen Rückstände bzw. die Tatsache, dass dieser Platz vom Angreifer als unverschlüsselt erkennbar sein kann, führt zu unten beschriebenen Angriffen.

Wenn die Option deaktiviert ist, überschreibt TrueCrypt vor dem eigentlichen Formatieren das Volume mit Zufallsdaten. Tatsächlich fordert TrueCrypt die darauf folgende eigentliche Formatierung unabhängig davon vom System immer als Quickformat an.

Das System schreibt dann nur die für das Dateisystem nötigen Verwaltungsinformationen auf das Volume, ohne sich um den freien Speicherplatz zu kümmern.

Der Hintergrund ist, dass so der freie Speicher sowohl bei Betrachtung von außerhalb als auch von innerhalb des Volumes mit (Pseudo-)Zufall belegt ist und so eine Nutzung dieses freien Speichers durch ein verstecktes Volume erst möglich wird. Bei der direkten Voll-Formatierung durch das System würde der freie Platz innerhalb des Volumes mit Nullen belegt sein.

Zu A7 (Schutz vor unbemerkter Benutzung durch Siegel)

Der Datenträger muss so versiegelt werden, dass jegliche Manipulation an der Hardware und jeder Zugriff auf die Daten erkannt wird. Dies kann z.B. durch ein Siegel an den Schnittstellen geschehen oder in einem entsprechenden Umschlag. Je nach Einsatzszenario muss dann das Siegel nach jeder rechtmäßigen Benutzung neu angebracht werden.

Zu A8 (Integritätssicherung)

Dies kann z.B. blockweise passieren, wie die Verwendung eines integritätssichernden Betriebsmodus oder eines RAIDs innerhalb des verschlüsselten Volumes, schützt dann aber nicht gegen alle aufgeführten Angriffe. Umfassendere Integritätssicherung kann durch zusätzliche Software stattfinden. Darüber hinaus kann ein Dateisystem mit aktivierter Integritätssicherung wie ZFS verwendet werden. Siehe dazu auch AP4.

Zu A10 (Headerbackup)

Es muss ein Headerbackup verfügbar sein, das so verwahrt sein muss, dass nur (wenige) Berechtigte darauf Zugriff haben.

Zu A12 (Zufallszahlengenerator)

Der Zufallszahlengenerator muss für kryptografische Anwendungen geeignet sein. Die genaue Konstruktion des TrueCrypt-Zufallszahlengenerators und dessen Eignung wird näher in AP4 und AP5 betrachtet.

Zu A15 (Smartcard-Leser)

Der Smartcard-Leser muss dem für die Festplattenverschlüsselung erforderlich Schutzgrad entsprechen. Insbesondere muss er gegen Abhören und Manipulation gesichert sein. Dies kann im einfachsten Falle durch eine geeignete anderweitige Zertifizierung sichergestellt werden.

Zu A15.1 (sichere Verbindung)

Die Verbindung sowohl zwischen System und Smartcard-Leser sowie zwischen Smartcard-Leser und Smartcard müssen geeignet manipulations- und abhörsicher sein, z.B. durch markiertes Kabel bzw. geeignete mechanische Bauweise u.ä.

3.4 Bedrohungen

- Der berechtigte Zugriff auf die Daten könnte verhindert werden.
- Unberechtigter Zugriff auf die Daten selbst oder auf Informationen zu den Daten könnte ermöglicht werden.
- Daten könnten unberechtigt manipuliert werden.