Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

VS-Produktkatalog des BSI

Bezeichnung:	Katalog von Produktklassen und –Typen gemäß VSA
Datum:	28.04.2020
Version:	1.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0) 228 99-9582-0
E-Mail: zulassung@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2020

Versionshistorie

Version	Datum	Wesentliche Änderungen
1.0	28.04.2020	Erste öffentliche Fassung

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt den vorliegenden Katalog zur Umsetzung der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) heraus und konkretisiert damit die in § 52 Abs. 2 VSA getroffenen Regelung.

Das vorliegende Dokument ist somit an Parteien adressiert, die im Kontext der VSA mit der Thematik „Zulassungen von IT-Sicherheitsprodukten“ in Berührung kommen können und ist für diese als Erweiterung der VSA verbindlich.

Die gültige Version des Kataloges wird durch die Zulassungsstelle des BSI bereitgestellt und ist von dieser zu beziehen.

Inhalt

Versionshistorie ... 3
Inhalt ... 4
Tabellenverzeichnis ... 6
Abbildungsverzeichnis ... 6
1 Einleitung ... 7
1.1 Anwendungsbereich ... 7
1.2 Adressatenkreis ... 7
1.3 Zweck ... 7
2 Begriffsbestimmung ... 9
2.1 Glossar ... 9
2.2 Abkürzungen ... 12
3 Auswahl geeigneter VS-Produkte ... 13
3.1 Einbettung in den Gesamtkontext der VSA ... 13
3.2 Schematischer Ablauf ... 14
4 Genereller Aufbau des Kataloges ... 16
5 Produktklassen und -typen ... 19
5.1 Produktklasse NETZWERKKOPPELUNG ... 19
5.1.1 Produkttyp „Firewall“ ... 19
5.1.2 Produkttyp „Datendiode“ ... 19
5.1.3 Produkttyp „VS-Guard“ ... 20
5.2 Produktklasse VS VERARBEITENDE SYSTEME ... 21
5.2.1 Produkttyp „VS-Arbeitsplatz“ ... 21
5.2.2 Produkttyp „VS-Registratursysteme“ ... 21
5.2.3 Produkttyp „Langzeitarchivierung“ ... 22
5.2.4 Produkttyp „Digitales Labelling“ ... 22
5.3 Produktklasse IDENTITÄTSMANAGEMENT UND ZUGRIFFSKONTROLLE ... 23
5.3.1 Produkttyp „Verzeichnisdienst“ ... 23
5.4 Produktklasse ÜBERWACHUNG UND PROTOKOLLIERUNG ... 24
5.4.1 Produkttyp „Schadsoftwareerkennung“ ... 24
5.4.2 Produkttyp „Sicherheitsprotokollierung“ ... 24
5.5 Produktklasse VERTRAUENSWÜRDIGE SEPARIERUNG ... 25
5.5.1 Produkttyp „Hypervisor“ ... 25
5.5.2 Produkttyp „Separation Kernel“ ... 25
5.6 Produktklasse VERTRAUENSWÜRDIGES IT-ZUBEHÖR ... 26
5.6.1 Produkttyp „Sichere Netzwerkkarte“ ... 26
5.6.2 Produkttyp „KVM Switch“ ... 26
5.7 Produktklasse SICHERHEITSMANAGEMENT ... 27

5.7.1 Produkttyp „Mobile Device Management“ ... 27
5.7.2 Produkttyp „Netzwerkmanagement“ ... 27
5.8 Produktklasse SCHLÜSSELMANAGEMENT ... 28
5.8.1 Produkttyp „Schlüsselspeicher- und Verteilkomponente“ ... 28
5.8.2 Produkttyp „Key-Management-Software“ ... 28
5.9 Produktklasse KRYPTOMODULE ... 29
5.9.1 Produkttyp „HSM / Kryptobeschleuniger“ ... 29
5.9.2 Produkttyp „Sicherheitsanker“ ... 29
5.9.3 Produkttyp „Verschlüsselungsgerät für Funksysteme“ ... 30
5.9.4 Produkttyp „Verschlüsselungsgerät für Satellitensysteme“ ... 30
5.9.5 Produkttyp „Verschlüsselungsgerät für analoge Leitungen“ ... 30
5.10 Produktklasse SPEICHERVERSCHLÜSSELUNG ... 31
5.10.1 Produkttyp „Dateiverschlüsselung (stand-alone)“ ... 31
5.10.2 Produkttyp „Festplattenverschlüsselung“ ... 31
5.10.3 Produkttyp „Sicherer mobiler Datenträger“ ... 32
5.11 Produktklasse DATENLÖSCHUNG ... 32
5.11.1 Produkttyp „Degausser“ ... 32
5.11.2 Produkttyp „Datenlöschsoftware“ ... 32
5.12 Produktklasse ÜBERTRAGUNGSVERSCHLÜSSELUNG ENDGERÄTE ... 33
5.12.1 Produkttyp „Faxverschlüsselung“ ... 33
5.12.2 Produkttyp „Telefonverschlüsselung“ ... 33
5.12.3 Produkttyp „Funkgeräte (konventionell und SDR)“ ... 33
5.12.4 Produkttyp „E-Mail- und Dateiverschlüsselung“ ... 34
5.12.5 Produkttyp „VPN-Client“ ... 34
5.12.6 Produkttyp „Sichere mobile Lösung“ ... 34
5.13 Produktklasse ÜBERTRAGUNGSVERSCHLÜSSELUNG INFRASTRUKTUR ... 35
5.13.1 Produkttyp „Verschlüsselung Layer 1“ ... 35
5.13.2 Produkttyp „Verschlüsselung Layer 2“ ... 35
5.13.3 Produkttyp „VPN-Gateway“ ... 36
5.13.4 Produkttyp „E-Mailverschlüsselung“ ... 36
6 Anhänge ... 37
6.1 Normative Verweisungen ... 37
6.1.1 DIN Normen und andere Anforderungen ... 37
6.1.2 Richtlinien und Anforderungen anderer Behörden ... 37
7 Literaturverzeichnis ... 38

Tabellenverzeichnis

Tabelle 1: Glossar 12
Tabelle 2: Abkürzungsverzeichnis 12
Tabelle 3: Abkürzungen der IT-Sicherheitsfunktionen gem. § 52 VSA 18

Abbildungsverzeichnis

Abbildung 1: Beziehungen zwischen Produktkatalog und Liste der VS-Produkte gem. § 52 Abs. 2 VSA 8
Abbildung 2: Beziehungen zwischen Informationssicherheitskonzept und dem Zulassungsschema 13
Abbildung 3: Schematische Darstellung der Nutzung der BSI Schrift 7164 und dem Produktkatalog 15
Abbildung 4: Beschreibende Merkmale einer Produktklasse 17
Abbildung 5: Beschreibende Merkmale eines Produkttypen 17

1 Einleitung

1.1 Anwendungsbereich

Das vorliegende Dokument „VS-Produktkatalog des BSI“ stellt eine Konkretisierung der Zulassungsparagraphen §§51 und 52 der VSA [3] dar. Insbesondere werden die im Rahmen von Zulassungsaussagen des BSI erforderlichen Regelungen gem. § 52, Abs. 2 VSA getroffen und sind damit in Kontext der Erteilung von Zulassungsaussagen für IT-Sicherheitsprodukte innerhalb eines VS-IT-Systems verbindlich.

1.2 Adressatenkreis

Der vorliegende Produktkatalog richtet sich an Personen und Organisationen, die mittelbar oder unmittelbar vom Zulassungsprozess und dessen Ergebnissen betroffen sind.

Im Zulassungskontext lassen sich daher im Wesentlichen folgende beteiligten Gruppen identifizieren:

1. Das BSI in der Rolle der *Zulassungsstelle (BSI-Zulassungsstelle)*
2. Die Bedarfsträger und Betreiber als unmittelbare oder mittelbare *Anwender von VS-Produkten*
3. Hersteller von IT-Sicherheitsprodukten zur *Realisierung von VS-Produkten*
4. Das BSI und die externen Prüfstellen in der Rolle der *Evaluierungsstelle (BSI-Evaluierungsstelle bzw. CC-Prüflabore)*
5. Das BSI in seiner Rolle als *BSI-Geheimschutzberatung*

1.3 Zweck

Der gemäß § 52 (2) VSA vom BSI zu erstellende und kontinuierlich zu pflegende Katalog von Produktklassen und –typen beinhaltet eine aktuelle und strukturierte Auflistung aller Produkttypen, die nach Maßgabe des BSI einer Zulassung oder Freigabeempfehlung bedürfen. Er dient so als Orientierungshilfe insbesondere für Bedarfsträger, die sich im Rahmen der Erstellung oder Aktualisierung ihres Informationssicherheitskonzeptes einen Überblick verschaffen wollen, in welchen Bereichen VS-Produkte verwendet werden müssen. Weiterhin ergänzt der Produktkatalog die TL Zulassung [2] in der dafür vorgesehenen Weise.

Dabei repräsentiert ein Produkttyp eine Menge von VS-Produkten, die mittels einer Menge von IT-Sicherheitsfunktionen (siehe § 52 VSA) charakterisiert sind und ähnliche Sicherheitsprobleme adressieren. Beispielhaft sei an dieser Stelle der Produkttyp „Festplattenverschlüsselung“ genannt, der primär die IT-Sicherheitsfunktionen „kryptographische Unterstützung“ und „Zugangs- und Zugriffskontrolle“ umsetzt.

Produkttypen werden aus Strukturierungsgründen in sogenannte Produktklassen unterteilt, um ein Auffinden zu erleichtern. So gehört z.B. der oben genannte Produkttyp „Festplattenverschlüsselung“ der Produktklasse „Speicherverschlüsslung“ an, zu der weitere Produkttypen wie zum Beispiel der Typ „Sicherer mobiler Datenträger“ gehört.

Der grundsätzliche Aufbau dieses Katalogs wird in der Abbildung 1 dargestellt. Der senkrechte Strich in der Abbildung stellt die Grenze dar zwischen der Beschreibung der Produkttypen und der BSI-Schrift 7164, in der die einzelnen, zugelassenen Produkte aufgeführt sind. Die BSI-Schrift 7164 ist über die Internetseiten des BSI erreichbar.

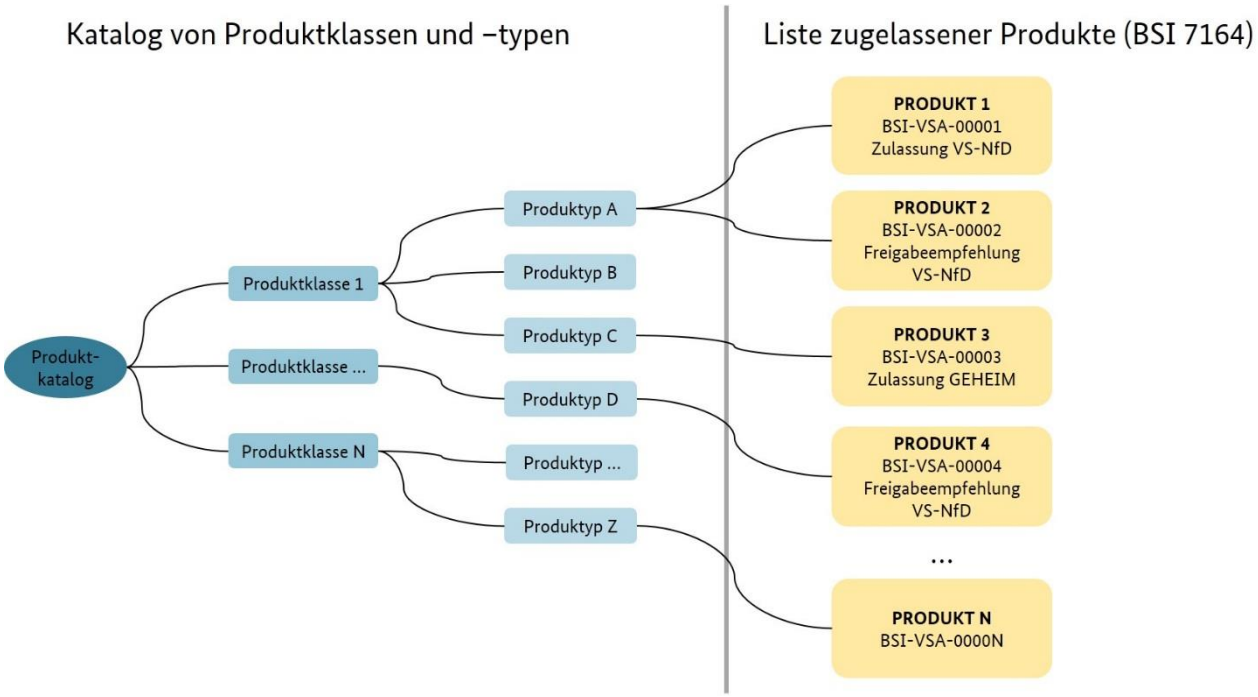

Abbildung 1: Beziehungen zwischen Produktkatalog und Liste der VS-Produkte gem. § 52 Abs. 2 VSA

Das BSI legt für die einzelnen Produkttypen fest, welche Art von Zulassungsaussage ein IT-Sicherheitsprodukt eines Produkttypen benötigt. Grundsätzlich sollen IT-Sicherheitsprodukte eine Zulassung nach § 51, Abs. 1 erhalten. Bestimmte Produkttypen kommen jedoch für eine Zulassung a priori nicht in Betracht, da die Zulassungsvoraussetzungen nicht oder nur mit unverhältnismäßigem Aufwand erfüllbar sind. Für diese Produkttypen ist ausschließlich die Freigabeempfehlung nach § 51, Abs. 5 vorgesehen.

In Ergänzung dazu finden sich alle in der BSI Schrift 7164 vom BSI mit einer Zulassungsaussage versehenen IT-Sicherheitsprodukte. Die Verknüpfung zum Produktkatalog wird dadurch hergestellt, dass einem IT-Sicherheitsprodukt mindestens ein zugehöriger Produkttyp aus dem Produktkatalog zugeordnet wird. Auf diese Weise ist gewährleistet, dass ein Bedarfsträger erkennen kann, welches Sicherheitsproblem mit einem IT-Sicherheitsprodukt adressiert werden kann.

Der Katalog der Produktklassen und –typen gliedert sich wie folgt:

- Kapitel 2 definiert die im Zulassungskontext und diesem Dokument verwendeten Begriffe und erläutert wichtige Abkürzungen
- Kapitel 3 enthält Erläuterungen, wie der Produktkatalog und die BSI Schrift 7164 im Rahmen der Erstellung des Informationssicherheitskonzeptes gem. § 13 VSA genutzt werden kann.
- Kapitel 4 definiert den Aufbau des Kataloges und gibt Hinweise, wie die Definition der Produktklassen und –typen zu lesen sind.
- Kapitel 5 enthält den eigentlichen Katalog, in dem es alle Produktklassen und –typen mit Zulassungsbezug auflistet und definiert.
- Kapitel 6 und 7 schließen das Dokument mit Normativen Verweisen und einem Literaturverzeichnis

2 Begriffsbestimmung

Im Kontext der Zulassung und damit auch im Rahmen dieses Produktkataloges sind die folgenden Begriffe und Abkürzungen relevant. Sie werden im restlichen Dokument in dem hier definierten Sinne verwendet und stimmen mit den Definitionen überein, welche in der TL Zulassung verwendet werden.

2.1 Glossar

Begriff	**Erklärung**
Antragsteller	Bedarfsträger, der der Zulassungsstelle des BSI mittels Antrag einen Bedarf an einem zuzulassenden IT-Sicherheitsprodukt anzeigt bzw. das BSI selber auf Basis eines festgestellten Bedarfs (z.B. in der Bundesverwaltung).
Bedarfsträger	Dienststellen (gem. § 1 VSA), die mit Verschlusssachen mit VS-IT verarbeiten und hierzu IT-Sicherheitsprodukte zum Schutz der VS einsetzen müssen.
BSI-Geheimschutzberatung	Organisatorischer Bereich des BSI, der für die Geheimschutzberatung zuständig ist.
BSI-Evaluierungsstelle	Organisatorischer Bereich des BSI, der für die Prüfung und Bewertung von IT-Sicherheitsprodukten im Rahmen von Zulassungsverfahren verantwortlich ist. Für einzelne Zulassungsverfahren werden Projektteams / Evaluierungsteams in der Regel aus mehreren fachlichen Bereichen zusammengesetzt.
BSI-Schrift 7164	Aktuelle von der BSI-Zulassungsstelle gepflegte Liste von VS-Produkten, VS-Anforderungsprofilen und dem Produktkatalog.
BSI-Zulassungsstelle	Organisatorischer Bereich des BSI, der den Gesamtprozess der Zulassung betreut und koordiniert.
CC-Prüflabor	Vom BSI anerkanntes externes und kommerzielles Prüflabor, das Evaluierungen auf der Basis der Common Criteria [5] durchführt.
Einstufung	Siehe Geheimhaltungsgrade.
Freigabe	Bestätigung der Verwendbarkeit eines Informationssicherheitskonzeptes (§ 13 Abs. 6 VSA) bzw. des Betriebs von VS-IT (§ 50 VSA). Die Freigabe erfolgt durch die Dienstellenleitung des Bedarfsträgers. Gem. § 13 VSA kann das BSI an dieser Freigabe durch die Abgabe eines Votums zur Freigabe des Informationssicherheitskonzeptes bzw. durch Abgabe eines Votums zur Freigabe der VS-IT (VS-Freigabe-Votum) gem. § 50 Abs. 2 beteiligt sein.
Freigabeempfehlung	Eine Zulassungsaussage der BSI-Zulassungsstelle (gem. § 51 Abs. 5 VSA) für ein IT-Sicherheitsprodukt, das in der Regel nicht alle für eine Zulassung erforderlichen IT-Sicherheitsfunktionen bietet oder keine vollständige vom BSI durchgeführte Evaluierung durchlaufen hat, das jedoch unter Einhaltung bestimmter Rahmenbedingungen für den Schutz von VS verwendet werden kann.
VS-Freigabe-Votum	Eine Empfehlung der BSI-Geheimschutzberatung bzgl. der Freigabe von VS-IT gem. § 50 VSA.

Begriff	Erklärung
Geheimhaltungsgrad(e)	VS sind je nach dem Schutz, dessen sie bedürfen, gemäß § 4 (2) des Sicherheitsüberprüfungsgesetzes (SÜG) [4] 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.
Hersteller	Eine Organisation, die ein IT-Sicherheitsprodukt herstellt und im Rahmen eines Zulassungsverfahrens seine Sicherheitsleistungen nachweist.
Informations-sicherheitskonzept	Nach den Standards des IT-Grundschutzes des BSI erstelltes Sicherheitskonzept, ergänzt um die Anforderungen des Geheimschutzes, die über den IT-Grundschutz hinausgehen. Es legt die erforderlichen Anforderungen und Maßnahmen für den Schutz von VS fest und bildet damit insbesondere auch eine Voraussetzung für den Betrieb von VS-IT (siehe § 13 VSA). In Bezug auf diese TL ist in diesem Konzept insbesondere die Verwendung zugelassener / freigabeempfohlener IT-Sicherheitsprodukte gemäß §§ 51 und 52 VSA festzuschreiben.
IT-Sicherheitsfunktion	Eine Funktion oder Leistung eines IT-Sicherheitsproduktes zur Abwehr von Bedrohungen und damit Umsetzung von Sicherheitszielen und zum Schutz von Werten (Assets). § 52 VSA listet in allgemeiner Art IT-Sicherheitsfunktionen für IT-Sicherheitsprodukte auf. Welche IT-Sicherheitsfunktionen oder Kombinationen von IT-Sicherheitsfunktionen von einem IT-Sicherheitsprodukt eines bestimmten Typs umgesetzt werden müssen, ist in einem vom BSI herausgegebenen Produktkatalog (siehe § 52 Abs. 2 VSA) geregelt.
IT-Sicherheitsprodukt	Ein IT-Produkt, das mit einer oder mehreren IT-Sicherheitsfunktionen dafür vorgesehen ist, elektronische Verschlusssachen vor potentiellen Bedrohungen zu schützen. Ein IT-Sicherheitsprodukt, das über eine Zulassungsaussage verfügt, wird als „VS-Produkt“ bezeichnet.
Produktklasse	Eine Produktklasse ist eine Menge von Produkttypen, die mindestens eine IT-Sicherheitsfunktion gemeinsam haben. Eine Produktklasse dient ausschließlich der Gliederung und Sortierung von Produkttypen und hat darüber hinaus keine weitere Bewandtnis.
Produktkatalog	Ein vom BSI gem. § 52 Abs. 2 VSA herausgegebenes Dokument, das im Sinne der §§ 51, 52 VSA relevanten Produkttypen definiert, diese Produktklassen

Begriff	Erklärung
	zuweist und für jeden Produkttyp die Zulassungsrelevanz auf Basis der IT-Sicherheitsfunktionen aus § 52 Abs. 1 VSA festlegt (dieses Dokument).
Produkttyp	Ein Produkttyp umfasst eine Menge von IT-Sicherheitsprodukten, die die gleichen IT-Sicherheitsfunktionen umsetzen, zusätzlich für gleiche Einsatzzwecke vorgesehen sind und dafür gegebenenfalls dieselbe Technologie verwenden.
Protection Profile	Ein in der Common Criteria definiertes Dokument (im Deutschen auch als „Schutzprofil“ bezeichnet), das IT-Sicherheitsanforderungen an IT-Produkte gleicher Art festlegt.
Security Operating Procedures (SecOPs)	Ein Dokument (im Deutschen auch als Einsatz- und Betriebsbedingungen bezeichnet), das bei erfolgreichem Abschluss eines Zulassungsverfahrens von der BSI-Zulassungsstelle erstellt wird und die Nutzung/Verwendung des VS-Produktes im Rahmen der getroffenen Zulassungsaussage regelt. Eine Gültigkeit der Zulassungsaussage bei der Verwendung eines VS-Produktes ist nur dann gegeben, wenn der Bedarfsträger die Regelungen der SecOPs einhält.
Verschlusssache (VS)	Nach § 4 Abs. 1 des Sicherheitsüberprüfungsgesetzes (SÜG) in der jeweils geltenden Fassung sind Verschlusssachen (VS) im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines seiner Länder, 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.
VS-Anforderungsprofil (VS-AP)	VS-Anforderungsprofile (VS-APs) beschreiben (funktionale) IT-Sicherheitsanforderungen für bestimmte Produktklassen und –typen. Sofern sich einem IT-Sicherheitsprodukt ein oder mehrere VS-APs zuordnen lassen, sind diese IT-Sicherheitsanforderungen im Rahmen eines Zulassungsverfahrens anzuwenden.
VS-Produkt	Ein mit einer Zulassungsaussage versehenes IT-Sicherheitsprodukt. Eine aktuelle Liste der VS-Produkte findet sich in der BSI Schrift 7164.
Zulassung	Zulassungsaussage der BSI-Zulassungsstelle, die auf der Grundlage der Nachweise im Zulassungsverfahren (siehe [1]) bestätigt, dass ein IT-Sicherheitsprodukt alle erforderlichen IT-Sicherheitsfunktionen umsetzt. Damit kann das IT-Sicherheitsprodukt zum Schutz von VS im Rahmen §§ 51 und 52 VSA verwendet werden.
Zulassungsprozess	Bezeichnet die Vorgehensweise im BSI, die dazu dient, die Eignung eines IT-Sicherheitsproduktes zum Schutz von elektronischer VS festzustellen und zu bestätigen.
Zulassungsantrag	Vom Bedarfsträger auszufüllendes Formular zur Initiierung eines Zulassungsverfahrens, das vom BSI bereitgestellt wird.
Zulassungsaussage	Aussage des BSI als Ergebnis des Zulassungsprozesses. In der Regel eine Bestätigung der Verwendbarkeit eines IT-Sicherheitsproduktes zum Schutz von VS, siehe auch „Zulassung“ und „Freigabeempfehlung“.

Begriff	Erklärung
Zulassungskonzept	Ein gem. § 51 Abs. 2 VSA zwischen dem BMI und BSI abgestimmtes Konzept bzgl. der BSI internen Abläufe und der Beschreibung der dabei relevanten Subjekte, Objekte, Rollen und Regelungen im Zulassungsschema. Es dient ausschließlich der Festlegung der Arbeitsweise des BSI und wird über den Rahmen der Festlegung mit dem BMI nicht weiter verteilt.
Zulassungsverfahren	Das Durchlaufen des Zulassungsprozesses für ein konkretes IT-Sicherheitsprodukt.

Tabelle 1: Glossar

2.2 Abkürzungen

Abkürzung	Bedeutung
AP	Anforderungsprofil
BSI-7164	BSI Schrift 7164; Liste der VS-Produkte
BT	Bedarfsträger
CC	Common Criteria
IT	Informationstechnik
SecOPs	Security Operating Procedures
SF01 – SF11	Abkürzungen für die in § 52 Absatz 1 VSA definierten IT-Sicherheitsfunktionen. Für eine genaue Zuordnung siehe Kapitel 4
ST	Security Target (im Deutschen auch Sicherheitsvorgaben)
TL	Technische Leitlinie
VS	Verschlusssache
VS-IT	Informationstechnik zur Handhabung von Verschlusssachen
VSA	Verschlusssachenanweisung
VS-AP	Anforderungsprofil an die Sicherheit von IT-Sicherheitsprodukten des gleichen Produkttyps
VS-NfD	VS – NUR FÜR DEN DIENSTGEBRAUCH
VS-V	VS – VERTRAULICH

Tabelle 2: Abkürzungsverzeichnis

3 Auswahl geeigneter VS-Produkte

Das folgende Kapitel beschreibt, wie eine Organisation, die die Notwendigkeit hat, VS mittels IT-Sicherheitsprodukten zu schützen, gem. VSA an die erforderlichen Informationen bezüglich zugelassener IT-Sicherheitsprodukte gelangt (BSI Schrift 7164), und wie im Rahmen der Erstellung des nach § 13 VSA vorgeschriebenen Informationssicherheitskonzeptes der BSI Produktkatalog (§ 52 Abs. 2 VSA) verwendet werden soll.

3.1 Einbettung in den Gesamtkontext der VSA

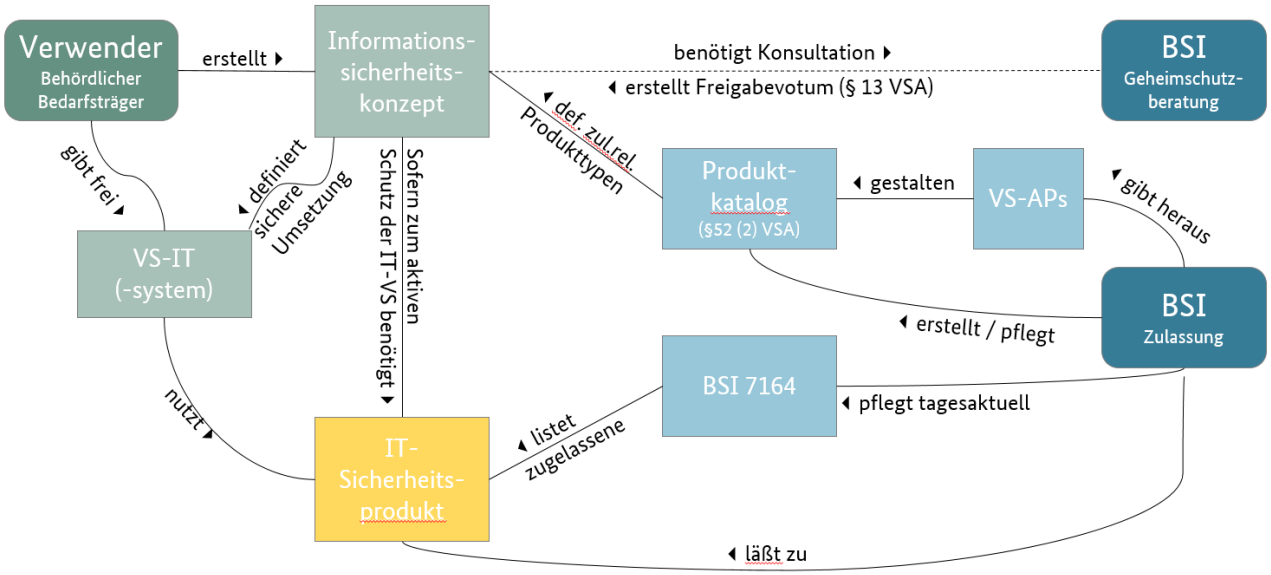

Abbildung 2: Beziehungen zwischen Informationssicherheitskonzept und dem Zulassungsschema

Abbildung 2 beschreibt die im Rahmen dieses Kapitels relevanten Subjekte (Bedarfsträger, BSI-Beratungsstelle (BSI-Geheimschutzberatung, BSI-Zulassungsstelle) sowie die Objekte, mit denen diese Subjekte im Kontext des vorliegenden Themas in Beziehung treten.

Gemäß § 1 Abs. 1 VSA richtet sich die VSA an Dienststellen, die mit Verschlusssachen arbeiten bzw. an dort tätige Personen, die in Kontakt mit Verschlusssachen kommen können. Sofern diese Verschlusssachen in elektronischer Form vorliegen und mittels VS-IT verarbeitet werden sollen, ist gem. § 13 VSA durch die verarbeitende Instanz (Verwender, behördlicher Bedarfsträger) ein Informationssicherheitskonzept zu erstellen und vor Nutzung der VS-IT freizugeben.

Das Informationssicherheitskonzept muss nach den Standards des BSI Grundschutzes erstellt werden und die darüberhinausgehenden Anforderungen des Geheimschutzes berücksichtigen.

Sofern von der VS-IT lediglich VS-NUR FÜR DEN DIENSTGEBRAUCH verarbeitet werden soll, ist das BSI beratend einzubeziehen, wenn:

- eine besondere Bedeutung der VS-IT festgestellt wurde oder
- die VS-IT durch eine Dienststelle gem. § 42 VSA betrieben wird.

Für VS-IT, die VS-VERTRAULICH oder höher verarbeiten soll, ist das BSI grundsätzlich beratend hinzuzuziehen. Anlaufstelle für diese Beratungen im Rahmen des Informationssicherheitskonzeptes bildet das Fachreferat, das für die BSI-Beratungsstelle zuständig ist.

Details dazu finden sich im auch im Grundschutzbaustein „CON.B1: VS-IT Sicherheit“.

Ein wesentlicher Bestandteil des Informationssicherheitskonzeptes ist die Definition der VS-IT (bzw. des VS-IT-Systems) und wie diese VS-IT gemeinsam mit weiteren Maßnahmen organisatorischer, personeller oder physikalischer Art in Summe eine gesicherte Verarbeitung von elektronischer VS ermöglicht.

Zentraler Baustein bei der Handhabung und Verarbeitung von elektronischer VS durch VS-IT ist, dass diese (bzw. bestimmte darin verwendete VS-Produkte), sofern andere Schutzmechanismen der Umgebung nicht greifen oder ausreichend sind, IT-Sicherheitsfunktionen enthält, die für den Schutz von VS vorgesehen sind. Daher ist es ein wesentliches Ziel und Gegenstand der Erstellung des Konzeptes festzustellen, ob und wenn ja wann und welche IT-Sicherheitsfunktionen für den Schutz der VS erforderlich sind.

Zum einen kann es in bestimmten technischen Bereichen des Informationssicherheitskonzeptes (z.B. Übertragung von VS über öffentliche Leitungen, Kopplungen von Netzen mit unterschiedlichen Einstufungsgraden oder VS Sprachkommunikation) klar auf der Hand liegen, dass IT-Sicherheitsprodukte eines bestimmten Produkttyps zum Schutz von VS erforderlich sind und welche IT-Sicherheitsfunktionen diese Produkte erbringen müssen. In diesem Fall ist es möglich, sich aus der Liste der bereits zugelassenen / freigabeempfohlenen Produkte (BSI-Schrift 7164) zu bedienen.

In anderen Teilbereichen, z.B. bei neuartigen oder sehr spezifischen Verwendungskontexten, kann dies jedoch nicht so offensichtlich sein, so dass eine vollständige und detaillierte Ermittlung der benötigten IT-Sicherheitsfunktionen im Rahmen der Konzepterstellung erforderlich ist.

Eine Hilfestellung bei der Identifikation der benötigten IT-Sicherheitsfunktionen soll dieses Dokument bieten. Den in Kapitel 5 aufgelisteten Produkttypen sind die von ihnen umzusetzenden IT-Sicherheitsfunktionen aus § 52 VSA zugeordnet. Sofern vorhanden, werden die detaillierten Anforderungen / Sicherheitsleistungen eines Produkttyps mittels VS-Anforderungsprofilen (VS-AP) ergänzend beschrieben. Diese Informationen können dann gemäß den im nächsten Kapitel dargestellten Ablauf genutzt werden, um relevante Produkttypen und passende zugelassene Produkte zu identifizieren.

3.2 Schematischer Ablauf

In Abbildung 3 ist dargestellt, wie bei der Erstellung des Informationssicherheitskonzeptes die BSI Schrift 7164 und der BSI Produktkatalog genutzt werden sollen.

Im Schritt 1 der Abbildung identifiziert der Ersteller des Informationssicherheitskonzeptes alle erforderlichen IT-Sicherheitsfunktionen die benötigt werden, damit eine ausreichende Schutzwirkung durch IT-Sicherheitsprodukte erzielt werden kann.

Auf dieser Basis kann der der Ersteller des Konzeptes in Schritt 3 unter zur Hilfenahme der BSI Schrift 7164 prüfen, ob bereits zugelassene oder freigabeempfohlene IT-Sicherheitsprodukte (VS-Produkte) verfügbar sind, die dann zu nutzen sind.

Ist dies nicht der Fall, kann in einem nächsten Schritt 4 geprüft werden, ob der BSI Produktkatalog Produkttypen bereithält, die den identifizierten Bedarf an IT-Sicherheitsfunktionen abdecken. Ist dies der Fall, so kann davon ausgegangen werden, dass die Notwendigkeit einer Zulassung oder Freigabeempfehlung für einen Produkttypen im Produktkatalog erkannt wurde, jedoch noch kein zugelassenes / freigabeempfohlenes IT-Sicherheitsprodukt verfügbar ist. Daher ist an die BSI-Zulassungsstelle heranzutreten und ein Zulassungsantrag zu stellen bzw. im Falle eines Entwicklungsvorhabens eine Zulassungsmöglichkeit zu sondieren.

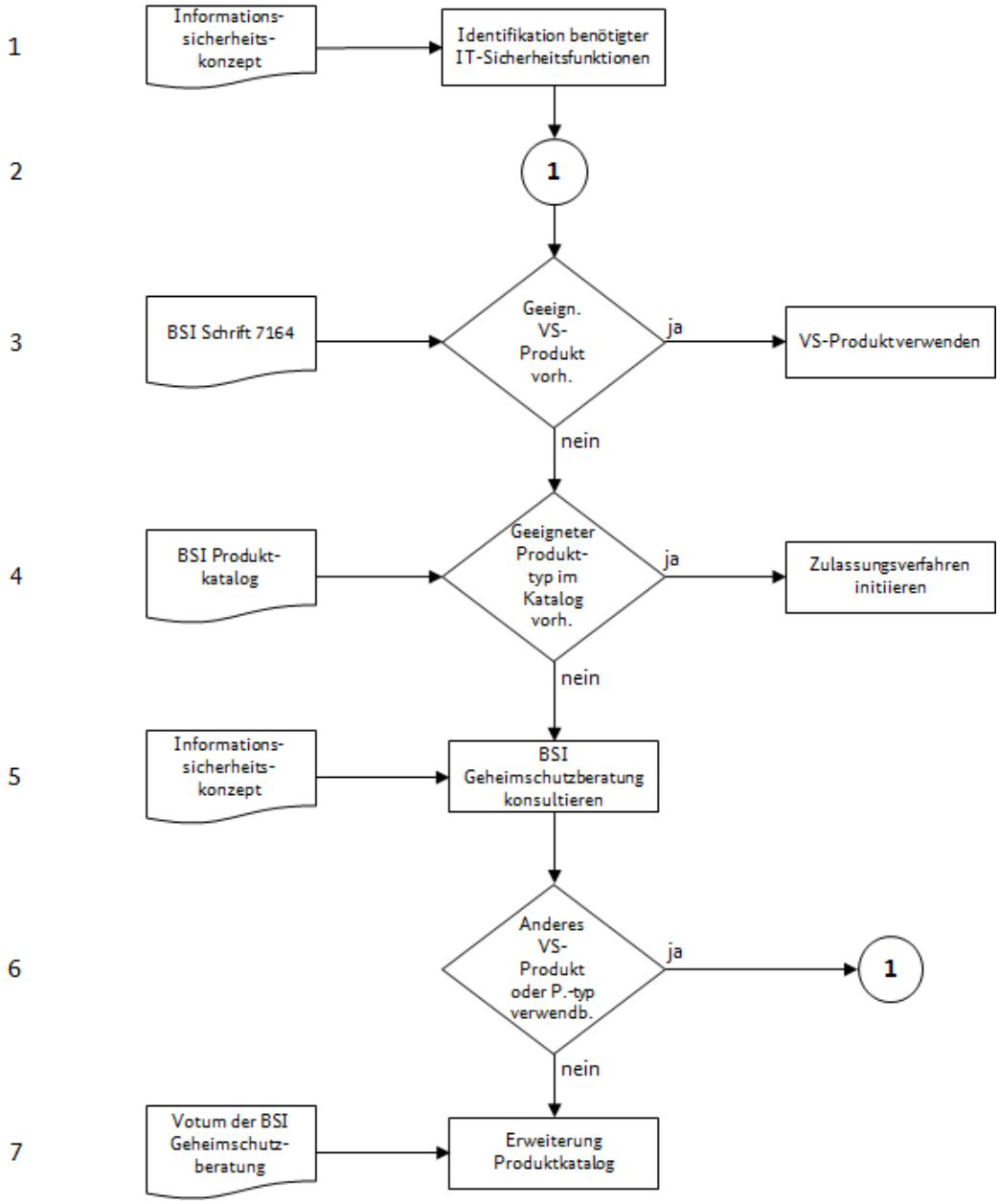

Abbildung 3: Schematische Darstellung der Nutzung der BSI Schrift 7164 und dem Produktkatalog

Schritt 5 von Abbildung 3 wird erst dann relevant, wenn für die im Informationssicherheitskonzept definierten IT-Sicherheitsfunktionen weder ein passender Produkttyp im BSI Produktkatalog noch ein VS-Produkt in der BSI Schrift 7164 identifiziert werden konnte. In diesem Fall tritt der Ersteller des Konzeptes an die BSI-Geheimschutzberatungsstelle heran um prüfen zu lassen, ob die im Konzept getroffene Einschätzung (weder Produkttyp noch VS-Produkt sind passend) zutrifft.

Sofern die BSI-Geheimschutzberatung in Schritt 6 zu dem Schluss kommt, dass der bestehende Produktkatalog ausreichend ist beziehungsweise bereits VS-Produkte doch verwendet werden können, ist das Informationssicherheitskonzept entsprechend anzupassen und mit Schritt 2 von Abbildung 3 fortzufahren.

An die BSI-Zulassungsstelle ist erst in Schritt 7 heranzutreten, wenn für eine Anpassung des bestehenden Produktkataloges auch von der BSI-Geheimschutzberatung votiert wird.

4 Genereller Aufbau des Kataloges

Gegenstand des vorliegenden Kapitels ist die Erläuterung des Aufbaus des eigentlichen Kataloges der Produktklassen und Produkttypen, der sich in Kapitel 5 befindet.

Dort werden alle Produkttypen, die eine Zulassungsrelevanz besitzen, aufgelistet. Zur Gewährleistung einer einfacheren Auffindbarkeit wird jeder Produkttyp eindeutig einer Produktklasse zugeordnet. Die folgende Darstellung gibt einen Überblick über alle Klassen und Typen des Kataloges:

NETZWERKKOPPLUNG	• Firewall • Datendiode • VS-Guard
VS VERARBEITENDE SYSTEME	• VS-Arbeitsplatz • VS-Registratursysteme • Langzeitarchivierung • Digitales Labelling
IDENTITÄTSMANAGEMENT UND ZUGRIFFSKONTROLLE	• Verzeichnisdienst
ÜBERWACHUNG UND PROTOKOLLIERUNG	• Schadsoftwareerkennung • Sicherheitsprotokollierung
VERTRAUENSWÜRDIGE SEPARIERUNG	• Hypervisor • Separation Kernel
VERTRAUENSWÜRDIGES IT-ZUBEHÖR	• Sichere Netzwerkkarte • KVM-Switch
SICHERHEITSMANAGEMENT	• Mobile Device Management • Netzwerkmagement
SCHLÜSSELMANAGEMENT	• Schlüsselspeicher- und Verteilkomponente • Key-Management-Software
KRYPTOMODULE	• HSM / Kryptobeschleuniger • Sicherheitsanker • Verschlüsselungsgeräte für Funksysteme • Verschlüsselungsgeräte für Satellitensysteme • Verschlüsselungsgeräte für analoge Leitungen
SPEICHERVERSCHLÜSSELUNG	• Dateiverschlüsselung • Festplattenverschlüsselung • Sicherer mobiler Datenträger
DATENLÖSCHUNG	• Degausser

	• Datenlöschsoftware
ÜBERTRAGUNGSVERSCHLÜSSELUNG ENDGERÄTE	• Faxverschlüsselung • Telefonverschlüsselung • Funkgeräte • E-Mail- und Dateiverschlüsselung • VPN-Client • Sichere Mobile Lösung
ÜBERTRAGUNGSVERSCHLÜSSELUNG INFRASTRUKTUR	• Verschlüsselung Layer 1 • Verschlüsselung Layer 2 • VPN-Gateway • E-Mailverschlüsselung

Jede Produktklasse wird in Kapitel 5 durch die in Abbildung 4 dargestellten Merkmale beschrieben:

Produktklasse:	**NAME**
Charakterisierung:	Kurze Beschreibung der Klasse
IT-Sicherheitsfunktionen:	Auflistung der IT-Sicherheitsfunktionen gem. § 52 VSA
Produkttypen:	Auflistung der zugeordneten Produkttypen

Abbildung 4: Beschreibende Merkmale einer Produktklasse

Neben dem Namen und einer Kurzbeschreibung der Klasse finden sich eine Auflistung der IT-Sicherheitsfunktionen gem. § 52, Abs. 2 VSA, die die Produktklasse ausmachen und eine Auflistung der Produkttypen, die der Produktklasse zugeordnet sind.

Für jeden Produkttypen finden sich dann in den Unterkapiteln von Kapitel 5 eine beschreibende Tabelle für jeden Produkttypen (siehe Abbildung 5).

Produkttyp:	**Firewall**
Charakterisierung:	Kurze Beschreibung des Produkttypen.
IT-Sicherheitsfunktionen:	Auflistung der IT-Sicherheitsfunktionen gem. § 52 VSA.
VS-AP:	Referenz auf das VS-Anforderungsprofil, das den Produkttypen umfassend beschreibt.
Zulassungsart:	Erforderliche Zulassungsaussage (Zulassung oder Freigabeempfehlung gem. § 51 VSA) und Zuordnung des Geheimhaltungsgrades für den die Zulassungsaussage erforderlich ist.

Abbildung 5: Beschreibende Merkmale eines Produkttypen

Charakterisiert wird der Produkttyp durch einen Namen, die gem. § 52, Abs. 2 VSA typischen IT-Sicherheitsfunktionen ergänzt um eine Referenz auf ein VS-Anforderungsprofil, das die sicherheitsfunktionalen Anforderungen an den Produkttyp umfassend beschreibt.

Darüber hinaus wird für jeden Produkttyp festgelegt, welche Art von Zulassungsaussage (Zulassung oder Freigabeempfehlung gem. § 51 VSA) ab welchem Geheimhaltungsgrad erforderlich ist. Sofern ein Produkttyp die Zulassungsaussage „Zulassung“ erfordert, ist diese für ein IT-Sicherheitsprodukt des Typs immer anzustreben. Eine Versorgung mittels Freigabeempfehlung ist gem. § 51 VSA jedoch übergangsweise möglich. Ist für einen Produkttypen eine Freigabeempfehlung als Zulassungsaussage festgelegt, ist es nicht Absicht des BSIs Zulassungen auszusprechen.

Für die in den o.g. Tabellen aus § 52 verwendeten IT-Sicherheitsfunktionen werden die folgenden Abkürzungen verwendet. Zusätzlich zu den Abkürzungen wird ergänzend eine Referenz zu den sicherheitsfunktionalen Common Critieria Spezifikationen aus Teil 2 [5] hergestellt:

Bezeichnung:	IT-Sicherheitsfunktionen gem. § 52 Absatz (1) VSA:
SF01	zur Zugangs- und Zugriffskontrolle
SF02	zur Identifikation und Authentisierung
SF03	zur kryptographischen Unterstützung
SF04	für das Sicherheitsmanagement
SF05	zur Informationsflusskontrolle
SF06	zum internen Schutz der Benutzerdaten
SF07	zum Selbstschutz der Sicherheitsfunktionen und ihrer Daten
SF08	zur Netzwerktrennung
SF09	zum Schutz der Unversehrtheit
SF10	zur Verfügbarkeitsüberwachung
SF11	zur Sicherheitsprotokollierung und Nachweisführung

Tabelle 3: Abkürzungen der IT-Sicherheitsfunktionen gem. § 52 VSA

5 Produktklassen und -typen

5.1 Produktklasse NETZWERKKOPPELUNG

Produktklasse:	NETZERKKOPPELUNG
Charakterisierung:	Die Klasse Netzwerkkopplung beinhaltet Produkttypen zur zielgerichteten Kopplung bzw. Trennung von Netzen unterschiedlicher Sicherheitsdomänen oder Einstufungsgrade.
IT-Sicherheitsfunktionen:	SF05 (FDP_ICC/IFC) SF08 (FDP_ICC/IFC)
Produkttypen:	• Firewall (siehe Kapitel 5.1.1) • Datendiode (siehe Kapitel 5.1.2) • VS-Guard (siehe Kapitel 5.1.3)

5.1.1 Produkttyp „Firewall“

Produkttyp:	Firewall
Charakterisierung:	Netzwerkgerät, das Netze unterschiedlicher Sicherheitsdomänen mittels einer vom Gerät umgesetzten Informationskontrollflusspolitik miteinander verbindet, bzw. voneinander trennt. Die Identifikation der Kommunikationspartner kann erforderlich sein. Der Informationsfluss wird protokolliert.
IT-Sicherheitsfunktionen:	SF05 (FDP_ICC/IFC) SF08 (FDP_ICC/IFC) SF02 (FIA_UID) SF11 (FAU)
VS-AP:	BSI-VS-AP-0018 Firewall (VS-NUR FÜR DEN DIENSTGEBRAUCH)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.1.2 Produkttyp „Datendiode“

Produkttyp:	Datendiode
Charakterisierung:	Netzwerkgerät das ausschließlich einen unidirektionalen Nutzdatenfluss zwischen zwei Netzen / unterschiedlicher Sicherheitsdomänen zulässt. Ein minimaler Rückfluss von Steuerinformationen kann dabei möglich sein. Der Informationsfluss wird protokolliert.
IT-Sicherheitsfunktionen:	SF05 (FDP_ICC/IFC) SF08 (FDP_ICC/IFC) SF11 (FAU)
VS-AP:	Derzeit kein VS-AP.
Zulassungsart:	Zulassung (VS-VERTRAULICH und höher)

5.1.3 Produkttyp „VS-Guard“

Produkttyp:	VS-Guard
Charakterisierung:	Netzwerkgerät, das Netze unterschiedlicher Sicherheitsdomänen mittels einer vom Gerät umgesetzten Informationskontrollflusspolitik miteinander verbindet. In den Netzen werden üblicherweise Informationen unterschiedlicher Geheimhaltungsgrade verarbeitet. Eine inhaltliche Kontrolle der fließenden Daten (ggfs. auf der Basis digitaler Label) gewährleistet, dass kein unberechtigter Informationsabfluss stattfindet. Die Identifikation der Kommunikationspartner kann erforderlich sein. Der Informationsfluss wird protokolliert.
IT-Sicherheitsfunktionen:	SF05 (FDP_ICC/IFC) SF08 (FDP_ICC/IFC) SF11 (FAU) SF02 (FIA_UID)
VS-AP:	BSI-VS-AP-0017 „VS-Guard“ (GEHEIM)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.2 Produktklasse VS VERARBEITENDE SYSTEME

Produktklasse:	VS VERARBEITENDE SYSTEME
Charakterisierung:	Die Klasse VS verarbeitende Systeme beinhaltet Produkttypen, die primär den Schutz von Benutzerdaten zum Gegenstand haben. Dabei finden sich in dieser Produktklasse Produkttypen, die lediglich die Integrität von Benutzerdaten schützen als auch Produkttypen, die sowohl die Integrität als auch die Vertraulichkeit von sowohl ruhenden als auch transportierten Benutzerdaten schützen.
IT-Sicherheitsfunktionen:	Übergeordnete Sicherheitsgrundfunktion ist die Verwendung kryptographischer Funktionen (SF03), mit denen die angestrebten Sicherheitsziele erreicht werden sollen.
Produkttypen:	• VS-Arbeitsplatz (siehe Kapitel 5.2.1) • VS-Registratursysteme (siehe Kapitel 5.2.2) • Langzeitarchivierung (siehe Kapitel 5.2.3) • Digitales Labelling (siehe Kapitel 5.2.4)

5.2.1 Produkttyp „VS-Arbeitsplatz“

Produkttyp:	VS-Arbeitsplatz
Charakterisierung:	Arbeitsplatz (auch mobil), der Verschlusssachen und Verschlusssachen, die über potentiell unsichere Netze übertragen werden müssen, mittels kryptographischer Mittel schützt. Der Zugriff eines Nutzers auf die Verschlusssachen erfolgt nach vorheriger Identifikation und Authentisierung. Die Separierung unterschiedlich eingestufter Bereiche oder auch offener von eingestuften Bereichen ist möglich. Die Sicherheitsfunktionen werden in gekapselter Weise erbracht.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF02 (FDP_ACC/ACF) SF03 (FCS und FTP_ITC)
VS-AP:	Derzeit kein VS-AP.
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.2.2 Produkttyp „VS-Registratursysteme“

Produkttyp:	VS-Registratursysteme
Charakterisierung:	IT-Sicherheitsprodukte, die die verwalteten Verschlusssachen selbst handhaben/bereitstellen. Separierung von identifizierten/authentisierten Mandanten und Durchsetzen des Need-To-Know Prinzipes unter Nutzung kryptographischer Mechanismen. Abbildung der Rolle des VS-Verwalters und Nachweisführung der verwalteten VS.
IT-Sicherheitsfunktionen:	SF01 (FDP_ACC/ACF)

Produkttyp:	VS-Registratursysteme
	SF02 (FIA) SF03 (FCS) SF04 (FMT)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-VERTRAULICH und höher)

5.2.3 Produkttyp „Langzeitarchivierung“

Produkttyp:	Langzeitarchivierung
Charakterisierung:	Sicherstellung der Integrität von Verschlusssachen über einen langen Zeitraum unter Nutzung kryptographischer Mittel. Zugriff auf die archivierten Daten darf nur nach vorheriger Nutzeridentifikation und Authentisierung erfolgen.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF01 (FDP_ACC/ACF) SF09 (FDP_SDI) SF03 (FCS)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-VERTRAULICH und höher)

5.2.4 Produkttyp „Digitales Labelling“

Produkttyp:	Digitales Labelling
Charakterisierung:	Anbringung von kryptographischen Labeln an Verschlusssachen nach Sicherstellung einer vorherigen Identifizierung & Authentisierung. Export/Bereitstellung dieser Verschlusssachen inkl. des Labels.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF03 (FCS und FDP_ETC)
VS-AP:	BSI-VS-AP-0016 „Digitales Labelling“ (GEHEIM)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.3 Produktklasse IDENTITÄTSMANAGEMENT UND ZUGRIFFS-KONTROLLE

Produktklasse:	IDENTITÄTSMANAGEMENT UND ZUGRIFFSKONTROLLE
Charakterisierung:	Die Klasse „Identitätsmanagement und Zugriffskontrolle“ beinhaltet Produkttypen, die Nutzer (Personen oder Geräte) identifizieren und authentisieren und auf dieser Basis Zugriffsberechtigungen auf Objekte zuordnet.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF01 (FCS_ACC/ACF)
Produkttypen:	• Verzeichnisdienst (siehe Kapitel 5.3.1)

5.3.1 Produkttyp „Verzeichnisdienst“

Produkttyp:	Verzeichnisdienst
Charakterisierung:	Verantwortlich für die Identifikation und Authentisierung von Entitäten und Verwaltung von Rechten und Rollen dieser Entitäten. Vermittlung/Bereitstellung von Zugriffsrechten von Entitäten auf Objekte. Protokollierung der Vorgänge.
IT-Sicherheitsfunktionen:	SF01 (FDP_ACC/ACF) SF02 (FIA) SF04 (FMT) SF11 (FAU)
VS-AP:	Derzeit kein VS-AP.
Zulassungsart:	Freigabeempfehlung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.4 Produktklasse ÜBERWACHUNG UND PROTOKOLLIERUNG

Produktklasse:	ÜBERWACHUNG UND PROTOKOLLIERUNG
Charakterisierung:	Teil der Klasse „Überwachung und Protokollierung“ sind Produkttypen, die zum Einen ein kontinuierliches Monitoring VS-relevanter Vorgänge und/oder zum Anderen eine Protokollierung dieser VS-relevanter Vorgänge zum Gegenstand haben.
IT-Sicherheitsfunktionen:	SF10 (FRU) und/oder SF11 (FAU)
Produkttypen:	• Schadsoftwareerkennung (siehe Kapitel 5.4.1) • Sicherheitsprotokollierung (siehe Kapitel 5.4.2)

5.4.1 Produkttyp „Schadsoftwareerkennung“

Produkttyp:	Schadsoftwareerkennung
Charakterisierung:	Überprüfung der Unversehrtheit/Integrität von Objekten und Meldung von Verstößen und damit mittelbarer Schutz von Verschlusssachen. Überwachung der Verfügbarkeit von überwachten Systemdiensten.
IT-Sicherheitsfunktionen:	SF11 (FAU gemeinsam mit FDP_ITT) SF10 (FRU)
VS-AP:	Derzeit kein VS-AP.
Zulassungsart:	Freigabeempfehlung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.4.2 Produkttyp „Sicherheitsprotokollierung“

Produkttyp:	Sicherheitsprotokollierung
Charakterisierung:	Protokollierung sicherheitsrelevanter Ereignisse insbesondere bei der Verarbeitung von Verschlusssachen. Einsicht und Auswertung der Protokolldaten nur für Subjekte mit entsprechender Zugriffsberechtigung nach vorheriger Identifikation und Authentisierung. Sicherstellung der Integrität der Protokolldaten. Überwachung der Verfügbarkeit von Systemen, die Loginformationen bereitstellen.
IT-Sicherheitsfunktionen:	SF11 (FAU) SF02 (FIA) SF01 (FDP_ACC/ACF) SF09 (FDP_SDI) SF10 (FRU)
VS-AP:	Derzeit kein VS-AP.
Zulassungsart:	Freigabeempfehlung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.5 Produktklasse VERTRAUENSWÜRDIGE SEPARIERUNG

Produktklasse:	VERTRAUENSWÜRDIGE SEPARIERUNG
Charakterisierung:	Die Klasse „Vertrauenswürdige Separierung“ beinhaltet Produkttypen, die eine Separierung von unterschiedlichen Sicherheitsdomänen zum Ziel haben. Dabei stehen der (interne) Schutz von Benutzerdaten aber auch der Selbstschutz der Separierungsfunktion im Vordergrund. Produkte dieser Klasse werden in der Regel in umfassendere Produkte oder Systeme integriert und liefern dort einen Teilbeitrag zur Gesamtsicherheit.
IT-Sicherheitsfunktionen:	SF01 (FDP_ACC/ACF) SF07 (FPT)
Produkttypen:	• Hypervisor (siehe Kapitel 5.5.1) • Separation Kernel (siehe Kapitel 5.5.2)

5.5.1 Produkttyp „Hypervisor“

Produkttyp:	Hypervisor
Charakterisierung:	Geregelte Trennung des Zugriffs auf Ressourcen sowie Steuerung von Informationsflüssen in Form einer Hardware-Abstraktionsschicht. Selbstschutz (Trennung unterschiedlicher Sicherheitsdomänen (DomainSeparation), Unumgehbarkeit).
IT-Sicherheitsfunktionen:	SF01 (FDP_ACC/ACF) SF05 (FDP_ICC/IFC) SF07 (FPT)
VS-AP:	Derzeit kein VS-AP.
Zulassungsart:	Freigabeempfehlung (VS-NUR FÜR DEN DIENSTGEBRAUCH) Zulassung (VS-VERTRAULICH und höher)

5.5.2 Produkttyp „Separation Kernel“

Produkttyp:	Separation Kernel
Charakterisierung:	Trennung des Zugriffs auf Ressourcen, Steuerung von Informationsflüssen Selbstschutz (DomainSeparation, Unumgehbarkeit) Minimalisierte Umsetzung (Virtualisierung nicht zwingend)
IT-Sicherheitsfunktionen:	SF01 (FDP_ACC/ACF) SF05 (FDP_ICC/IFC) SF07 (FPT)
VS-AP:	BSI-VS-AP-0015 „Separation Kernel“ (GEHEIM)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.6 Produktklasse VERTRAUENSWÜRDIGES IT-ZUBEHÖR

Produktklasse:	IT SICHERHEITPRODUKTE DER PLATTFORM
Charakterisierung:	Die Klasse „Vertrauenswürdiges IT-Zubehör“ beinhaltet Produkttypen, die sich durch eine eng begrenzte, nicht veränderliche Funktionalität auszeichnen. Dabei steht ihre Unversehrtheit und damit der Selbstschutz (z.B. passiver Tamperschutz) dieser Komponenten gegen Manipulation im Vordergrund. Die Komponenten unterstützen in diesem Rahmen den vertrauenswürdigen Betrieb von IT-Systemen, in denen sie zum Einsatz kommen.
IT-Sicherheitsfunktionen:	SF07 (FPT)
Produkttypen:	• Sichere Netzwerkkarte (siehe Kapitel 5.6.1) • KVM Switch (siehe Kapitel 5.6.2)

5.6.1 Produkttyp „Sichere Netzwerkkarte“

Produkttyp:	Sichere Netzwerkkarte
Charakterisierung:	Minimalisierte Implementierung einer Netzwerkkarte und damit Sicherstellung der Integrität des stattfindenden Netzwerkverkehrs.
IT-Sicherheitsfunktionen:	SF07 (FPT) SF09 (FDP_SDI)
VS-AP:	BSI-VS-AP-0004 „Sichere Netzwerkkarte“ (GEHEIM)
Zulassungsart:	Zulassung (VS-VERTRAULICH und höher)

5.6.2 Produkttyp „KVM Switch“

Produkttyp:	KVM Switch
Charakterisierung:	Steuerung der Informationsflüsse von I/O-Geräten zwischen mehreren VS-verarbeitenden Geräten.
IT-Sicherheitsfunktionen:	SF05 (FDP_ICC/IFC)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Freigabeempfehlung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.7 Produktklasse SICHERHEITSMANAGEMENT

Produktklasse:	SICHERHEITSMANAGEMENT
Charakterisierung:	Sammlung von Produkttypen, die für das Management zugelassener Geräte zuständig sind und in diesem Zusammenhang sicherheitsbezogene Aspekte verwalten und steuern.
IT-Sicherheitsfunktionen:	SF04 (FMT)
Produkttypen:	• Mobile Device Management (siehe Kapitel 5.7.1) • Netzwerk-Management (siehe Kapitel 5.7.2)

5.7.1 Produkttyp „Mobile Device Management“

Produkttyp:	Mobile Device Management
Charakterisierung:	Identifikation und Authentisierung (hoch)mobiler Endgeräte. Verwaltet die Sicherheitspolicies zugelassener Endgeräte, stellt diese bereit und setzt sie durch. Insbesondere bzgl. der Installierbaren Software und einer Notfall-Deaktivierung. Protokollierung sicherheitsrelevanter Managementereignisse.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF04 (FMT insb. inkl. SW-Kontrolle und Deaktivierung im Notfall) SF11 (FAU)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Freigabeempfehlung (VS-NUR FÜR DEN DIENSTGEBRAUCH) Zulassung (VS-VERTRAULICH und höher)

5.7.2 Produkttyp „Netzwerkmanagement“

Produkttyp:	Netzwerkmanagement
Charakterisierung:	Identifikation und Authentisierung von Netzwerkgeräten (Infrastruktur und Endpunkt). Verwaltet die Sicherheitspolicies zugelassener Geräte, verteilt diese und setzt sie ggf. durch. Protokollierung sicherheitsrelevanter Managementereignisse.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF04 (FMT) SF11 (FAU)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Freigabeempfehlung (VS-NUR FÜR DEN DIENSTGEBRAUCH) Zulassung (VS-VERTRAULICH und höher)

5.8 Produktklasse SCHLÜSSELMANAGEMENT

Produktklasse:	SCHLÜSSELMANAGEMENT
Charakterisierung:	Management kryptographischer Schlüssel oder Parameter. Dabei stehen zentrale Aspekte wie Generierung, Verwaltung und Transport im Fokus. Sicherstellung von Integrität/Authentizität und Vertraulichkeit der verwalteten kryptographischen Objekte durch die Verwendung von kryptographischen Mechanismen und Verfahren.
IT-Sicherheitsfunktionen:	SF04 (FMT) SF03 (FCS)
Produkttypen:	• Schlüsselspeicher- und Verteilkomponente (siehe Kapitel 5.8.1) • Key-Management Software (siehe Kapitel 5.8.2)

5.8.1 Produkttyp „Schlüsselspeicher- und Verteilkomponente“

Produkttyp:	Schlüsselspeicher- und Verteilkomponente
Charakterisierung:	Speichert Schlüssel, verteilt diese und ist in der Lage diese zuverlässig zu löschen. Verfügt über Autorisierung vor Nutzung (ggfs. auch organisatorisch) Unterstützt ggfs. Rollentrennung und eine Administration des Gerätes Der Schutz der Schlüssel im Gerät erfolgt ggfs. mittels kryptographischer Mittel.
IT-Sicherheitsfunktionen:	SF01 (FDP) und SF06 (insb. FDP_RIP) SF02 (FIA) SF04 (FMT insb. FMT_SMR) SF03 (FCS)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-VERTRAULICH und höher)

5.8.2 Produkttyp „Key-Management-Software“

Produkttyp:	Key-Management-Software
Charakterisierung:	Bereitstellung von Schlüsseln und kryptographischen Parametern. Dabei insbesondere Generierung, Verwaltung und Löschung. Muss ggfs. Rollen nach vorheriger Identifizierung/Authentisierung unterscheiden können und basierend auf diesen Rollen, Zugriffsrechte durchsetzen.
IT-Sicherheitsfunktionen:	SF03 (FCS) SF02 (FIA) SF01 (FDP_ACC/ACF) SF04 (FMT insb. FMT_SMR)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.9 Produktklasse KRYPTOMODULE

Produktklasse:	KRYPTOMODULE
Charakterisierung:	Sammlung von Produkttypen, deren primäre Aufgabe die gekapselte Bereitstellung kryptografischer Funktionen ist.
IT-Sicherheitsfunktionen:	SF03 (FCS)
Produkttypen:	• HSM / Kryptobeschleuniger (siehe Kapitel 5.9.1) • Secure Element / Smart Card (siehe Kapitel 5.9.2) • Verschlüsselungsgerät für Funksysteme (siehe Kapitel 5.9.3) • Verschlüsselungsgerät für Satellitensysteme (siehe Kapitel 5.9.4) • Verschlüsselungsgerät für analoge Leitungen (siehe Kapitel 5.9.5)

5.9.1 Produkttyp „HSM / Kryptobeschleuniger“

Produkttyp:	HSM / Kryptobeschleuniger
Charakterisierung:	Bereitstellung kryptographischer Funktionen für berechtigte Nutzer nach vorheriger Authentisierung durch dedizierte/gekapselte Hardware. Selbstschutz (physikalisch und/oder logisch). Einsatzszenario stationär und hoch performant.
IT-Sicherheitsfunktionen:	SF03 (FCS) SF02 (FIA) SF01 (FDP_ACC/ACF) SF07 (FPT)
VS-AP:	BSI-VS-AP-0002 Hardware Sicherheitsmodul (für VS-NfD) BSI-VS-AP-0013 Hardware Sicherheitsmodule (für GEHEIM)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.9.2 Produkttyp „Sicherheitsanker“

Produkttyp:	Sicherheitsanker
Charakterisierung:	Bereitstellung kryptographischer Funktionen für berechtigte Nutzer nach vorheriger Authentisierung durch dedizierte/gekapselte Hardware. Selbstschutz (physikalisch und/oder logisch). Einsatzszenario mobil (kleiner Formfaktor) und/oder weniger performant.
IT-Sicherheitsfunktionen:	SF03 (FCS) SF02 (FIA) SF01 (FDP_ACC/ACF) SF07 (FPT)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Freigabeempfehlung (VS-NUR FÜR DEN DIENSTGRBAUCH und höher)

5.9.3 Produkttyp „Verschlüsselungsgerät für Funksysteme“

Produkttyp:	Verschlüsselungsgerät für Funksysteme
Charakterisierung:	Dediziertes Gerät zur Kryptierung von Funkstrecken.
IT-Sicherheitsfunktionen:	SF03 (FCS)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGRBAUCH und höher)

5.9.4 Produkttyp „Verschlüsselungsgerät für Satellitensysteme“

Produkttyp:	Verschlüsselungsgerät für Satellitensysteme
Charakterisierung:	Dediziertes Gerät zur Kryptierung von Funkstrecken von Satellitensystemen.
IT-Sicherheitsfunktionen:	SF03 (FCS)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS- NUR FÜR DEN DIENSTGRBAUCH und höher)

5.9.5 Produkttyp „Verschlüsselungsgerät für analoge Leitungen“

Produkttyp:	Verschlüsselungsgerät für analoge Leitungen
Charakterisierung:	Dediziertes Gerät zur Kryptierung von analogen Telekommunikations-Leitungen.
IT-Sicherheitsfunktionen:	SF03 (FCS)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS- NUR FÜR DEN DIENSTGRBAUCH und höher)

5.10 Produktklasse SPEICHERVERSCHLÜSSELUNG

Produktklasse:	SPEICHERVERSCHLÜSSELUNG
Charakterisierung:	Kryptographische Absicherung ruhender/nicht-volatiler Informationen. Zugang/Zugriff zu den entschlüsselten Informationen erst nach vorheriger Identifizierung/Authentisierung.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF03 (FCS) und SF01 (FDP_ACC/ACF)
Produkttypen:	• Dateiverschlüsselung (siehe Kapitel 5.10.1) • Festplattenverschlüsselung (siehe Kapitel 5.10.2) • Sicherer mobiler Datenträger (siehe Kapitel 5.10.3)

5.10.1 Produkttyp „Dateiverschlüsselung (stand-alone)“

Produkttyp:	Dateiverschlüsselung (stand-alone)
Charakterisierung:	Ver- und Entschlüsselung einzelner Dateien oder Ordner nach Authentisierung zur Nutzung von Schlüsseln.
IT-Sicherheitsfunktionen:	SF03 (FCS insbesondere FCS_COP (Ver- und Entschlüsselung)) SF02 (FIA) SF01 (FDP_ACC/ACF)
VS-AP:	Derzeit kein VS-AP.
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.10.2 Produkttyp „Festplattenverschlüsselung“

Produkttyp:	Festplattenverschlüsselung
Charakterisierung:	Ver- und Entschlüsselung von gesamten Datenspeichern / Festplatten. Dabei sowohl kryptographische Absicherung von Nutzdaten und Systeminhalten gleichermaßen. Identifizierung und Authentisierung vor Zugriff auf Daten (bzw. PreBoot-Authentisierung vor Zugriff auf Systeminhalten) Löschen ganzer verschlüsselter Bereich durch Löschen entsprechender Schlüssel.
IT-Sicherheitsfunktionen:	SF03 (FCS insbesondere FCS_COP (Ver- und Entschlüsselung)) SF01 (FDP_ACC/ACF für den Zugriff auf Systeminhalte) SF06 (FDP_RIP (bzw. FCS_CKM.4) Löschen von Nutzdaten durch Löschung von Schlüsseln) SF02 (FIA)
VS-AP:	BSI-VS-AP-0008 „Festplattenverschlüsselung“ (VS-NUR FÜR DEN DIENSTGEBRAUCH)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGRBAUCH und höher)

5.10.3 Produkttyp „Sicherer mobiler Datenträger“

Produkttyp:	Sicherer mobiler Datenträger
Charakterisierung:	Ver- und Entschlüsselung von gesamten Datenträgern (mobil). Identifizierung und Authentisierung vor Zugriff auf Daten. Löschen der Nutzinformationen auf den Datenträgern durch Löschen entsprechender Schlüssel.
IT-Sicherheitsfunktionen:	SF03 (FCS insbesondere FCS_COP (Ver- und Entschlüsselung)) SF01 (FDP_ACC/ACF für den Zugriff auf Nutzdaten) SF06 (FDP_RIP (bzw. FCS_CKM.4) Löschen von Nutzdaten durch Löschung von Schlüsseln) SF02 (FIA)
VS-AP:	BSI-VSA-0006 „Sicherer Mobiler Datenträger“ (VS-NUR FÜR DEN DIENSTGEBRAUCH)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.11 Produktklasse DATENLÖSCHUNG

Produktklasse:	DATENLÖSCHUNG
Charakterisierung:	Zentraler Aspekt der Produktklasse ist das Löschen von Nutzdaten.
IT-Sicherheitsfunktionen:	SF06 (FDP_RIP)
Produkttypen:	• Degausser (siehe Kapitel 5.11.1) • Datenlöschsoftware (siehe Kapitel 5.11.2)

5.11.1 Produkttyp „Degausser“

Produkttyp:	Degausser
Charakterisierung:	Physikalisches Löschen von Nutzdaten auf magnetischen Datenträgern.
IT-Sicherheitsfunktionen:	SF06 (FDP_RIP)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-VERTRAULICH und höher)

5.11.2 Produkttyp „Datenlöschsoftware“

Produkttyp:	Datenlöschsoftware
Charakterisierung:	Logisches Löschen (Überschreiben) von Nutzdaten auf Datenträgern und Protokollierung des Löschvorgangs.
IT-Sicherheitsfunktionen:	SF06 (FDP_RIP) SF11 (FAU)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.12 Produktklasse ÜBERTRAGUNGSVERSCHLÜSSELUNG ENDGERÄTE

Produktklasse:	ÜBERTRAGUNGSVERSCHLÜSSELUNG ENDGERÄTE
Charakterisierung:	Sicherung von Daten und/oder Sprache bei der Übertragung über unsichere Kanäle durch den Einsatz kryptographischer Mittel. Die Produkttypen der vorliegenden Klasse fokussieren sich auf mögliche Endgeräte dieser Kommunikation.
IT-Sicherheitsfunktionen:	SF03 (FCS)
Produkttypen:	• Faxverschlüsselung (siehe Kapitel 5.12.1) • Telefonverschlüsselung (siehe Kapitel 5.12.2) • Funkgeräte (siehe Kapitel 5.12.3) • E-Mail und Dateiverschlüsselung (siehe Kapitel 5.12.4) • VPN-Client (siehe Kapitel 5.12.5) • Sichere mobile Lösung (siehe Kapitel 5.12.6)

5.12.1 Produkttyp „Faxverschlüsselung“

Produkttyp:	Faxverschlüsselung
Charakterisierung:	Ende-zu-Ende verschlüsselte Kommunikation zwischen zwei Fax-Geräten
IT-Sicherheitsfunktionen:	SF03 (FCS inkl. FTP_ITC (sichere Ende-zu-Ende Verbindung))
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.12.2 Produkttyp „Telefonverschlüsselung“

Produkttyp:	Telefonverschlüsselung
Charakterisierung:	Ende-zu-Ende verschlüsselte Kommunikation zwischen zwei (stationären) Telefongeräten
IT-Sicherheitsfunktionen:	SF03 (FCS inkl. FTP_ITC (sichere Ende-zu-Ende Verbindung))
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.12.3 Produkttyp „Funkgeräte (konventionell und SDR)“

Produkttyp:	Funkgeräte (konventionell und SDR)
Charakterisierung:	Ende-zu-Ende verschlüsselte Kommunikation von Sprache und/oder Daten zwischen zwei Funkgeräten (konventionell und software-definiert (SDR)).
IT-Sicherheitsfunktionen:	SF03 (FCS inkl. FTP_ITC (sichere Ende-zu-Ende Verbindung))
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.12.4 Produkttyp „E-Mail- und Dateiverschlüsselung“

Produkttyp:	E-Mail- und Dateiverschlüsselung
Charakterisierung:	Ver- und Entschlüsselung einzelner Dateien/Ordner/Nachrichten nach vorheriger Authentisierung zur Nutzung von Schlüsseln. Ziel ist die Anschließende Übermittlung über ungesicherte Transportwege.
IT-Sicherheitsfunktionen:	SF03 (FCS) SF02 (FIA) SF01 (FDP_ACC/ACF Schlüsselzugriff)
VS-AP:	BSI-VS-AP-0014 „Sichere Übertragung von E-Mails und Dateien“ (VS-NUR FÜR DEN DIENSTGEBRAUCH)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.12.5 Produkttyp „VPN-Client“

Produkttyp:	VPN-Client
Charakterisierung:	Geräte-Identifizierung und –Authentisierung. Übertragung von Daten über einen mittels Kryptographie geschützten vertrauenswürdigen Kanal zu einer korrespondierenden Infrastrukturkomponente.
IT-Sicherheitsfunktionen:	SF01 (FIA) SF03 (FCS inkl. FTP_ITC zu einer Infrastrukturkomponente)
VS-AP:	BSI-VS-AP-0005 „VPN-Client“ (VS-NUR FÜR DEN DIENSTGEBRAUCH)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.12.6 Produkttyp „Sichere mobile Lösung“

Produkttyp:	Sichere mobile Lösung
Charakterisierung:	Geräte-Identifizierung und –Authentisierung. Übertragung von Daten und/oder Sprache über einen mittels Kryptographie geschützten vertrauenswürdigen Kanal zu korrespondierenden Infrastrukturkomponenten. Speicherverschlüsselung und Identifizierung und Authentisierung von Nutzern am Gerät.
IT-Sicherheitsfunktionen:	SF01 (FIA sowohl von Nutzern als auch Geräten) SF03 (FCS insbes. für Sprache und/oder Daten zu einer zentralen Infrastrukturkomponenten und Ende-zu-Ende)
VS-AP:	BSI-VS-AP-0003 „Sichere Mobile Lösung“ (VS-NUR FÜR DEN DIENSTGEBRAUCH)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH oder höher)

5.13 Produktklasse ÜBERTRAGUNGSVERSCHLÜSSELUNG INFRASTRUKTUR

Produktklasse:	ÜBERTRAGUNGSVERSCHLÜSSELUNG INFRASTRUKTUR
Charakterisierung:	Infrastrukturkomponenten, die mittels kryptographischer Mechanismen einen Kommunikationsendpunkt für Endgeräte darstellen bzw. selbst eine verschlüsselte Kommunikationsinfrastruktur bereitstellen. In dieser Eigenschaft separieren sie verschlüsselte von unverschlüsselter Kommunikation und führen so eine Netztrennung herbei. Eine Kommunikation findet erst nach erfolgreicher Identifikation / Authentisierung statt.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF03 (FCS) SF08 (FDP_ICC/IFC)
Produkttypen:	• Verschlüsselung Layer 1 (siehe Kapitel 5.13.1) • Verschlüsselung Layer 2 (siehe Kapitel 5.13.2) • VPN-Gateway (siehe Kapitel 5.13.3) • E-Mail Verschlüsselung (siehe Kapitel 5.13.4)

5.13.1 Produkttyp „Verschlüsselung Layer 1“

Produkttyp:	Verschlüsselung Layer 1
Charakterisierung:	Verschlüsselung nach vorheriger Geräteauthentisierung auf ISO/OSI Netzwerk-Schicht 1 (Punkt-zu-Punkt). Netzwerktrennung durch Verschlüsselung.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF03 (FCS inkl. FTP_ITC Punkt-zu-Punkt Verschlüsselung) SF08 (FDP_ICC/IFC)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH oder höher)

5.13.2 Produkttyp „Verschlüsselung Layer 2“

Produkttyp:	Verschlüsselung Layer 2
Charakterisierung:	Verschlüsselung nach vorheriger Geräteauthentisierung auf ISO/OSI Netzwerk-Schicht 2 (Punkt-zu-Punkt oder Punkt-zu-Multi-Punkt). Netzwerktrennung durch Verschlüsselung.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF03 (FCS inkl. FTP_ITC Punkt-zu-Punkt/Punkt-zu-Multi-Punkt Verschlüsselung) SF08 (FDP_ICC/IFC)
VS-AP:	Derzeit kein VS-AP

Produkttyp:	Verschlüsselung Layer 2
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH oder höher)

5.13.3 Produkttyp „VPN-Gateway“

Produkttyp:	VPN-Gateway
Charakterisierung:	Verschlüsselung nach vorheriger Geräteauthentisierung auf ISO/OSI Netzwerk-Schicht 3 (Punkt-zu-Multi-Punkt). Netzwerktrennung durch Verschlüsselung.
IT-Sicherheitsfunktionen:	SF02 (FIA) SF03 (FCS inkl. FTP_ITC Punkt-zu-Multi-Punkt Verschlüsselung) SF08 (FDP_ICC/IFC)
VS-AP:	BSI-VS-AP-0001 „VPN Gateway“ (VS-NUR FÜR DEN DIENSTGEBRAUCH)
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

5.13.4 Produkttyp „E-Mailverschlüsselung“

Produkttyp:	E-Mailverschlüsselung
Charakterisierung:	Serverbasierte / Stellvertretende Verschlüsselungen von E-Mails (benutzer- oder benutzergruppen-spezifisch) Verwaltung von Nutzer-Schlüsseln (rollenbasiert). Informationsflusskontrolle der ein und ausgehenden Mails
IT-Sicherheitsfunktionen:	SF02 (FIA) SF03 (FCS inkl. FTP_ITC Punkt-zu-Multi-Punkt Verschlüsselung) SF08 (FDP_ICC/IFC)
VS-AP:	Derzeit kein VS-AP
Zulassungsart:	Zulassung (VS-NUR FÜR DEN DIENSTGEBRAUCH und höher)

6 Anhänge

6.1 Normative Verweisungen

Keine.

6.1.1 DIN Normen und andere Anforderungen

Keine.

6.1.2 Richtlinien und Anforderungen anderer Behörden

Keine.

7 Literaturverzeichnis

[1] BSI. Nachweise für eine Evaluierung für eine Zulassung
Teil 1: Nachweise für eine Zulassung bis VS-NUR FÜR DEN DIENSTGEBRAUCH.
Teil 2: Nachweise für eine Zulassung bis VS-VERTRAULICH / GEHEIM

[2] BSI. Technische Leitlinie des BSI, Mitwirkungspflichten in Zulassungsverfahren, BSI TL - IT 01

[3] BMI. Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA). In der Fassung vom 10. August 2018

[4] BRD. Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867), zuletzt geändert durch Artikel 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2732).2017

[5] The Australian Signals Directorate et al. Common Criteria for Information Technology Security Evaluation Part 1-3, Version 3.1, Revision 5. 2017.