



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

Einsatz- und Betriebsbedingungen GnuPG VS-Desktop 3.x

BSI-VSA-10867

Stand: 27.10.2023

Geeignet zum Schutz von: VS - NUR FÜR DEN DIENSTGEBRAUCH
RESTREINT UE/EU RESTRICTED
NATO RESTRICTED

Nationale Version

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: zulassung@bsi.bund.de
Internet: <https://www.bsi.bund.de>
© Bundesamt für Sicherheit in der Informationstechnik 2024

Inhaltsverzeichnis

Inhaltsverzeichnis.....	3
Annexe.....	5
VORWORT	7
1 EINLEITUNG	8
1.1 Inhalt.....	8
1.2 Verwendung.....	8
1.3 Weitergabe	8
1.4 Referenzen	8
1.5 Begriffsbestimmungen	10
1.6 Parteien und Instanzen	12
2 SYSTEMBESCHREIBUNG.....	14
2.1 Einsatzzweck.....	14
2.2 Systemkomponenten und Funktion.....	14
2.3 Zulassung und zugelassener Konstruktionsstand	15
2.4 Kompatibilität, Interoperabilität, Konformität.....	16
2.5 Betriebsarten.....	16
2.6 Installation, Systemintegration und Konfiguration.....	16
2.7 Betrieb	16
2.8 Abstrahlsicherheit.....	20
3 SICHERHEITSMANAGEMENT	21
3.1 Zuständigkeiten für Sicherheits-/Schlüsselmanagement	21
3.2 Beschreibung des Sicherheits-/Schlüsselmanagements	21
3.3 Quantencomputer-Resistenz	21
4 VS-EINSTUFUNGEN.....	22
4.1 VS-Behandlungshinweise	22
5 NACHWEISFÜHRUNG UND KONTROLLE.....	23
5.1 Verkauf, Ausleihe und Export.....	23
5.2 Konformitätserklärung (DoC).....	23
5.3 VS-Nachweisführung und Kontrolle.....	23
6 MATERIELLE SICHERHEIT	24
6.1 Zuständigkeiten.....	24
6.2 Anforderungen an die Materielle Sicherheit.....	24
6.2.1 Allgemein.....	24
6.2.2 Betriebsbereites Gerät	24
6.2.3 Lagerung und Transport.....	24
6.2.4 Behandlung von Schlüsselmaterial.....	25

6.3	Geräteschutzmechanismen.....	25
6.3.1	Meldung und Maßnahmen	25
6.4	Routinemäßige Vernichtung.....	25
6.4.1	Vernichten/Löschen von Schlüsseln/Zertifikaten.....	25
6.4.2	Produktentsorgung und -vernichtung.....	25
7	PERSONELLE SICHERHEIT	26
7.1	Zuständigkeiten.....	26
7.2	Ermächtigung und Autorisierung.....	26
7.3	Kenntnis nur, wenn nötig (Need-To-Know).....	26
8	WARTUNG UND REPARATUR	27
8.1	Zuständigkeiten.....	27
8.2	Vorgaben und Maßnahmen.....	27
9	NOTFALLPROZEDUREN.....	28
9.1	Zuständigkeiten.....	28
9.2	Notfallplan	28
10	SICHERHEITSVORFÄLLE.....	29
10.1	Ansprechpartner des Betreibers.....	29
10.2	Meldepflicht und Zuständigkeiten.....	29
10.3	Meldepflichtige Vorfälle	29
10.4	Maßnahmen bei BSI-Warnung	29
11	KONTAKTE.....	30
11.1	Hersteller	30
11.2	BSI Krypto-Support.....	30
11.3	BSI Zulassung	30

Annexe

- ANNEX A – ZULASSUNG UND KONSTRUKTIONSSTAND
- ANNEX B – EINSTUFUNGSLISTE
- ANNEX C – entfällt
- ANNEX D – entfällt
- ANNEX E – entfällt
- ANNEX F – entfällt
- ANNEX G – entfällt

Abbildungsverzeichnis

Abbildung 1: Zertifikatsdetails - Kleopatra.....18

Tabellenverzeichnis

Tabelle 1: Referenzen.....10

Tabelle 2: Begriffsbestimmungen.....12

Leere Seite

VORWORT

Die vorliegenden Einsatz- und Betriebsbedingungen, international auch als Security Operating Procedures (SecOPs) bezeichnet, für GnuPG VS-Desktop werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben und sind integraler Bestandteil der Zulassungsdokumentation von GnuPG VS-Desktop.

Diese Einsatz- und Betriebsbedingungen ergänzen das Nutzerhandbuch von GnuPG VS-Desktop in einigen sicherheitsrelevanten Bereichen und sind gemeinsam mit diesem zu lesen und anzuwenden.

Die Beachtung und Umsetzung dieses Dokumentes ist verbindlich für den Betrieb von GnuPG VS-Desktop. Abweichende Regelungen bedürfen der ausdrücklichen schriftlichen Genehmigung durch das BSI.

Dieses Dokument sollte allen Stellen, die IT-Systeme mit GnuPG VS-Desktop planen, GnuPG VS-Desktop implementieren und betreiben, sowie den verantwortlichen IT-Sicherheitsbeauftragten, Geheimschutzbeauftragten, Sicherheitsverantwortlichen und Endnutzern zur Verfügung gestellt werden.

Falls erforderlich, wird das BSI Ergänzungen zu diesem Dokument herausgeben.

Eventuelle Fragen zu diesem Dokument sind an folgende Adresse zu richten:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
D-53133 Bonn
Germany

E-Mail: zulassung@bsi.bund.de

DE-Mail: zulassung@bsi-bund.de-mail.de

1 EINLEITUNG

1.1 Inhalt

Das vorliegende Papier beinhaltet die Einsatz- und Betriebsbedingungen für GnuPG VS-Desktop, international auch als Security Operating Procedures (SecOPs) bezeichnet, für den Schutz von Verschlusssachen (VS) mit den maximalen Geheimhaltungsgraden VS - NUR FÜR DEN DIENSTGEBRAUCH, RESTREINT UE/EU RESTRICTED und NATO RESTRICTED.

GnuPG VS-Desktop erfüllt die Anforderungen für Strength of Mechanism (SoM) STANDARD gemäß den Referenzen [IASP 2] (EU) und [AC/322-D/0047] (NATO). In Ausnahmefällen, in denen ein Produkt, das für SoM STANDARD zugelassen ist, zum Schutz von Informationen mit Geheimhaltungsgraden höher als RESTREINT UE/EU RESTRICTED und NATO RESTRICTED eingesetzt werden soll, ist eine vorherige Risikobewertung (Abwägung von Threat und Impact) gemäß vorgenannten Referenzen für die geplante Anwendung und das zugehörige Nutzungsszenario erforderlich. Die erforderliche Bewertung ist durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen mit der Security Accreditation Authority (SAA), falls nicht vorhanden, zusammen mit dem Betreiber vorzunehmen. Das BSI kann zusammen mit der SAA den Einsatz für spezielle Anwendungen in speziellen Einsatzszenarien zulassen, wenn die Anforderungen der zuvor genannten Referenzen erfüllt sind, die Bewertung positiv verlaufen ist und die EU- und NATO- Anforderungen bzgl. der Abstrahlsicherheit eingehalten werden.

Das Dokument beschreibt die Mindestanforderungen für die sichere Installation, Integration und Konfiguration sowie für die Kontrolle, den Schutz und den Betrieb von GnuPG VS-Desktop, zugehörigem Sicherheitsmanagement, Zubehör und produktspezifischer Dokumentation.

1.2 Verwendung

Diese Einsatz- und Betriebsbedingungen gelten national für alle Anwendungen, in denen GnuPG VS-Desktop zum Schutz von nationaler, EU- oder NATO-VS zum Einsatz kommt. Sie sollten allen, die für die Installation und Kontrolle sowie für die Weitergabe und Betrieb von GnuPG VS-Desktop verantwortlich sind, zur Verfügung gestellt werden.

1.3 Weitergabe

Im Falle einer Weitergabe von GnuPG VS-Desktop an ausländische Nationen oder nicht-deutsche Institutionen gelten besondere Bedingungen, auf die im Weiteren (Kapitel 5) noch eingegangen wird.

1.4 Referenzen

In Abhängigkeit von den Einstufungen (national, EU, NATO) der zu schützenden Informationen sind nachfolgend aufgeführte Referenzdokumente zu beachten.

Die nachfolgenden Referenzen beziehen sich im nationalen Kontext grundsätzlich auf die einschlägigen VS-Bestimmungen insbesondere die VSA. Entsprechende Richtlinien der einzelnen Ressorts¹ sind sinngemäß umzusetzen.

1 So sind z.B. im Bereich der Bundeswehr insbesondere die dort geltenden Vorschriften (z.B. ZDv A-1130/1, ZDv A-1130/2, ZDv A-1130/3, ZDv A-960/1, ZDv A-962/1) bzw. im Bereich der geheimschutzbetreuten Wirtschaft das Geheimschutzhandbuch (GHB) des BMWi zu beachten.

Nationale Sicherheitsvorschriften		
	[SÜG]	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG)
	[VSA]	Verschlusssachenanweisung - Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz, vom 10.08.2018
	[BSI TL - IT 01]	Technische Leitlinie des BSI „Mitwirkungspflichten in Zulassungsverfahren“, Stand: 27.10.2020
	[BSI TL - M50]	Technische Leitlinie des BSI „Löschen und Vernichten von Verschlusssachen auf Datenträgern“, Stand: Dezember 2020
	[BSI TR-02102-1]	Technische Richtlinie des BSI „Kryptografische Verfahren: Empfehlungen und Schlüssellängen“, Stand: März 2020
	[GHB]	Handbuch für den Geheimschutz in der Wirtschaft (Geheimschutzhandbuch), 2004, Stand: 23.08.2017
Internationale Sicherheitsvorschriften		
	<u>EU Security Policy</u>	
	[2013/488/EU]	Council Decision of 23 September 2013 on the Council Security Rules
	[2015/844/EC]	Beschluss (EU, Euratom) vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen
	[2013/C 190/01]	EEAS Decision of the HR on the Security Rules for the European External Action Service
	[IASG 2-03]	IA Security Guidelines on Crypto and COMSEC Management
	[IASP 2]	EU Council 10745/11 – IASP 2 – Information Assurance Security Policy on Cryptography, 30 May 2011, RESTREINT UE/EU RESTRICTED
	<u>NATO Security Policy</u>	
	[C-M(2002)49]	NATO Security Policy (NU)
	[SDIP-293]	Instructions for the Control and Safeguarding of NATO Crypto material (NR)
	[AC/322-D/0047]	AC/322-D/0047-REV2 – INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, NATO RESTRICTED
	[AC/322-D/0048-REV3 (INV)]	AC/322-D/0048-REV3 - Technical and Implementation Directive on CIS Security (18.11.2019)
TEMPEST/EMSEC		
	<u>EU</u>	
	[IASP 7]	IA Security Policy on TEMPEST (R-UE/EU-R)
	[IASG 7-01]	IA Security Guidelines on Selection and Installation of TEMPEST Equipment

	[IASG 7-02]	IA Security Guidelines on TEMPEST Zoning Procedures (R-UE/EU-R)
	[IASG 7-03]	IA Security Guidelines on EU TEMPEST Requirements and Evaluation Procedures (C-UEU/EU-C)
	<u>NATO</u>	
	[AC/322-D(2019)0021]	INFOSEC Technical and Implementation Directive on Emission Security (NR)
	[SDIP-27]	NATO TEMPEST Requirements and Evaluation Procedures (NC)
	[SDIP-28]	NATO Zoning Procedures (NR)
	[SDIP-29]	Selection and Installation of Equipment for the Processing of Classified Information (NR)
Sonstige Referenzen		
	<u>Zulassungen/Freigabeempfehlungen</u>	
	[Zulassung-National]	Nationale Zulassung für den Schutz von VS - NUR FÜR DEN DIENSTGEBRAUCH: BSI-VSA-10867 vom 01.06.2021 inkl. Anlagen
	[EU-Zulassung]	(EU)-Zulassung für den Schutz von RESTREINT UE/EU RESTRICTED: 11753/22, vom 05.08.2022 inkl. Anlagen
	<u>Konformitätserklärung</u>	
	[Konformität]	Konformitätserklärung/Declaration of Compliance (siehe Kapitel 5 – Nachweisführung und Kontrolle)

Tabelle 1: Referenzen

1.5 Begriffsbestimmungen

Nachfolgend die Erläuterung einiger Begriffe, die in diesem Dokument benutzt werden:

Allgemeine Begriffe und Abkürzungen	
ATO	Approval To Operate
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAA	Crypto Approval Authority (EU-Begriff; in Deutschland das BSI)
CCI	Controlled Cryptographic Item bzw. Controlled COMSEC Item Die Festlegung für das vorliegende IT-Sicherheitsprodukt GnuPG VS-Desktop erfolgt in Annex B dieser Dokumentation.
CIS	Communications and Information Systems
COMSEC	Communications Security
DEUmilSAA	Beim ZCSBw angesiedelte Stelle, die für den Bereich der Bundeswehr die Aufgaben einer SAA übernimmt.
EVG	Evaluierungsgegenstand
IT	Informationstechnik
IT-SiBe	IT-Sicherheitsbeauftragter

Kryptomittel	Nationale Kryptomittel im Sinne § 59 [VSA] sind Produkte, Geräte und die dazugehörigen Dokumente sowie zugehörige Schlüsselmittel zur Entschlüsselung, Verschlüsselung und Übertragung von Informationen, die vom Bundesamt für Sicherheit in der Informationstechnik oder für den Geschäftsbereich des Bundesministeriums der Verteidigung vom Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr als solche festgelegt werden. Internationale Kryptomittel werden nach den einschlägigen über- oder zwischenstaatlichen Vorschriften sowie den jeweiligen nationalen Vorschriften anderer Staaten festgelegt. Die Festlegung für das vorliegende IT-Sicherheitsprodukt GnuPG VS-Desktop erfolgt in Annex B dieser Dokumentation.
MEP	Manipulationserkennungsplakette (Klebeetikett, mit dem Gerätegehäuse gegen Manipulation gesichert werden kann.)
NCSA	National CIS Security Authority (in Deutschland das BSI)
SAA	Security Accreditation Authority, zu den Aufgaben siehe Kapitel 1.6 „Parteien und Instanzen“
SecOPs	Security Operating Procedures (Einsatz und Betriebsbedingungen)
SLA	Service Level Agreement
SoM	Strength of Mechanism
TEMPEST	Bezeichnet sowohl die Nutzung kompromittierender Abstrahlung für Lauschangriffe sowie Maßnahmen zum Schutz gegen kompromittierende Abstrahlung
TOE	Target of Evaluation, engl. Bezeichnung für EVG
VS	Verschlusssache(n)
VS-NfD	VS-NUR FÜR DEN DIENSTGEBRAUCH
VS-V	VS-VERTRAULICH
VSA	Verschlusssachenanweisung des Bundes (siehe Referenzen)
ZCSBw	Zentrum für Cyber-Sicherheit der Bundeswehr
Gerätespezifische Begriffe und Abkürzungen	
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
OCB	Der Offset-Codebuch-Modus (OCB-Modus) ist eine authentifizierte Verschlüsselungsbetriebsart für kryptografische Blockchiffren.
OCSP	Online Certificate Status Protocol
PKCS#1	Public-Key Cryptography Standard, definiert das Format der RSA-Verschlüsselung
PKI	Public Key Infrastructure
S/MIME	Secure Multipurpose Internet Mail Extensions

X.509	Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate
-------	--

Tabelle 2: Begriffsbestimmungen

1.6 Parteien und Instanzen

Nachfolgend aufgeführte Parteien und Instanzen² sind mit beschriebenen Aufgaben und Verantwortlichkeiten (Rollen) bei der Umsetzung der Einsatz- und Betriebsbedingungen involviert.

Sofern eine der unten beschriebenen Rollen Aufgaben aus dem Verantwortungsbereich des Geheimschutzbeauftragten übernimmt, legt dieser fest, ob hierfür ein "besonders beauftragter Mitarbeiter" nach § 8 [VSA] zu bestellen ist. Dies kann z.B. die Rolle "Administrator/Systemadministrator" betreffen.

- **Administrator/Systemadministrator**
Die Person(en), die das VS-IT-Produkt oder -System administrieren. Diese ist (sind) verantwortlich für sichere Einrichtung des VS-IT-Produktes, -Systems. In der Regel hat der Administrator volle Zugriffsrechte für die Konfiguration und Bedienung des Produktes/Systems.
- **Betreiber bzw. Nutzer (des IT-Systems/IT-Sicherheitsproduktes)**
Die Stelle, die für den Betrieb des IT-Systems verantwortlich ist. Der Betreiber ist u.a. zuständig für
 - o die geschäftlichen und betrieblichen Anforderungen an das IT-System, Vorgaben für dessen Betrieb und Anforderungen bzgl. des Informationsaustausches;
 - o Zuarbeit für die SAA bei der Erstellung einer Risikobewertung für das IT-System (wenn erforderlich);
 - o die Erstellung eines Planes, um das bei einer Risikobewertung ermittelte Restrisiko zu handhaben;
 - o die Sicherstellung, dass Servicevereinbarungen (SLA) oder ähnliche Mechanismen, die für die Erbringung von IT-Services vereinbart werden, Vorgaben für die Implementierung, den Betrieb, die Überwachung und das Änderungsmanagement von Sicherheitsmaßnahmen enthalten;
 - o die Durchführung der betrieblichen Evaluierung (operational evaluation) des IT-Systems und die Validierung/Autorisierung/Freigabe des IT-Systems für den Betrieb nach erfolgter Sicherheitsakkreditierung des IT-Systems durch die SAA (wenn erforderlich);
 - o Ermittlungen im Falle eines Sicherheitsvorfalls, Feststellung des Schadens und Berichterstattung (an die SAA, falls vorhanden, und an den Krypto-Support des BSI),
 - o die Verteilung der Einsatz- und Betriebsbedingungen an die Endnutzer.
- **BSI**
Das BSI ist als nationale IT-Sicherheitsbehörde u.a. zuständig für IT-sicherheitstechnische Bewertungen (Evaluierungen) von Sicherheitsprodukten/-systemen und deren Zulassung oder Zertifizierung. Außerdem ist es am Freigabeverfahren nach § 50 [VSA] ggf. zu beteiligen. Das BSI nimmt gegenüber der NATO die Funktion der „German National CIS Security Authority (NCSA)“ wahr. Bei der EU wird diese Funktion auch als „Crypto Approval Authority (CAA) bezeichnet.

² Aus Gründen der besseren Lesbarkeit wird für die einzelnen Parteien und Instanzen auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Personen- bzw. Rollenbezeichnungen gelten gleichermaßen für beide Geschlechter.

- **Endnutzer (End User)**
Die Person(en), die das VS-IT-Produkt oder -System als Anwender nutzen und bedienen. Diese ist (sind) zuständig für die Umsetzung der in den vorliegenden Einsatz- und Betriebsbedingungen aufgestellten Anforderungen an den Endnutzer, um einen ordnungsgemäßen, sicheren Betrieb des VS-IT-Produktes, -Systems zu gewährleisten. In der Regel hat der Endnutzer nur eingeschränkte Berechtigungen zur Bedienung des Produktes/Systems.
- **Hersteller**
Der Hersteller g10 code GmbH des VS-IT-Produktes GnuPG VS-Desktop unterliegt in Abhängigkeit vom jeweiligen VS-Geheimhaltungsgrad der zu schützenden Informationen bestimmten Vorgaben für die Entwicklung, Produktion, Evaluierung, Zulassung und den Vertrieb seines Produktes. Darüber hinaus ist er zur Einhaltung gesetzlicher Vorgaben für den Export verpflichtet.
- **Geheimenschutzbeauftragter**
Nach § 8 [VSA] sorgt der Geheimenschutzbeauftragte für die Umsetzung der Verschlusssachanweisung und berät die Dienststellenleitungen in allen Fragen des Geheimenschutzes. Geheimenschutzbeauftragte haben ein unmittelbares Vortragsrecht bei den Dienststellenleitungen. Geheimenschutzbeauftragte sind bei allen geheimenschutzrelevanten Maßnahmen zu beteiligen.
- **IT-Sicherheitsbeauftragter**
IT-Sicherheitsbeauftragte unterstützen und beraten nach § 9 [VSA] die Geheimenschutzbeauftragten in allen Fragen des Einsatzes von Informationstechnik zur Handhabung von Verschlusssachen (VS-IT).
- **Sicherheitsbevollmächtigter**
Der Sicherheitsbevollmächtigte ist im Bereich der geheimenschutzbetreuten Wirtschaft gemäß Kap. 3.1 des [GHB] das zentrale Sicherheitsorgan im Unternehmen. Die Geschäftsleitung überträgt ihm die Zuständigkeit für die Durchführung aller Geheimenschutzmaßnahmen und bevollmächtigt ihn entsprechend.
- **Security Accreditation Authority (SAA)**
Das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimenschutz ist im Sinne der nationalen Zuständigkeit SAA für IT-Systeme zur Handhabung von Verschlusssachen über- oder zwischenstaatlicher Organisationen. Gemäß § 36 [VSA] müssen IT-Systeme zur Handhabung von Verschlusssachen über- oder zwischenstaatlicher Organisationen (beispielsweise der EU oder der NATO) einem Sicherheitsakkreditierungsverfahren unterzogen werden.
Für den Bereich der Bundeswehr übernimmt die DEUmilSAA diese Aufgaben. Ferner ist die DEUmilSAA in ihrem Verantwortungsbereich für die Freigabegenehmigungen sowie für die Analogieprüfung zu bereits geprüften Produkten und Szenarien zuständig.

2 SYSTEMBESCHREIBUNG

2.1 Einsatzzweck

GnuPG VS-Desktop soll den VS-NfD-konformen verschlüsselten Austausch von E-Mails sowie die VS-NfD-konforme Verschlüsselung von Dateien ermöglichen. GnuPG VS-Desktop kann auf den Plattformen Windows (MSI-Installationsdatei) und GNU/Linux (AppImage) eingesetzt werden.

Bei dem Produkt handelt es sich um eine Kryptobibliothek mit verschiedenen darauf aufbauenden Komponenten. Die zulassungsrelevanten Komponenten sind ein Plugin (also ein Zusatzprogramm) für das E-Mailsystem Microsoft Outlook unter Windows oder für Kontact unter Linux mit einer Zertifikatsverwaltung. Es unterstützt sowohl den S/MIME-Standard mit X.509-Zertifikaten als auch den OpenPGP-Standard zum Austausch und zur Speicherung öffentlicher Schlüssel.

Die wesentlichen Sicherheitsleistungen des Produkts bestehen darin, mittels S/MIME bzw. OpenPGP verschlüsselte und/oder signierte Dateien oder E-Mails zu empfangen und dabei entschlüsseln und/oder verifizieren zu können, oder aber selbst mittels S/MIME bzw. OpenPGP verschlüsselte und/oder signierte Dateien oder E-Mails versenden zu können.

Mit dem Produkt GnuPG VS-Desktop lassen sich S/MIME und OpenPGP-basiert Dateien und E-Mails ver- und entschlüsseln, sowie ihre Integrität (Unversehrtheit) und Authentizität (Herkunft) mittels digitaler Signaturen absichern und überprüfen. Ferner können Dateien symmetrisch mit Hilfe eines Passwortes ver- und entschlüsselt werden.

Das Produkt GnuPG VS-Desktop setzt sich wie folgt zusammen:

Ein MSI Installationspaket für Windows, welches aus verschiedenen Freien-Software-Komponenten besteht, die wahlweise installiert werden können.

Eine AppImage Datei für die GNU/Linux Plattform, welche distributionsübergreifend eingesetzt werden kann, ohne den jeweiligen Paketmanager benutzen zu müssen.

Beide Installationsdateien (MSI und AppImage) enthalten folgende Komponenten:

GnuPG:

Das Kernstück; das eigentliche Verschlüsselungsprogramm.

Kleopatra:

Ein Zertifikatsmanager für X.509 (S/MIME); stellt einheitliche Benutzerführung für alle Krypto-Dialoge bereit.

Die beiden folgenden Komponenten GpgOL und GpgEX sind nicht Bestandteil des AppImages, da deren Funktionalitäten unter Linux durch Bordkomponenten zur Verfügung gestellt werden.

GpgOL:

Eine Programmerweiterung für Microsoft Outlook 2010/2013/2016/2019 (E-Mail-Verschlüsselung). Exchange Server werden ab Exchange Version 2010 unterstützt.

GpgEX:

Eine Programmerweiterung für den Microsoft Explorer (Dateiverschlüsselung).

2.2 Systemkomponenten und Funktion

Bei dem Produkt GnuPG VS-Desktop handelt es sich um mehrere Komponenten, die als Paket installiert werden können. Dies beinhaltet ein Plugin (also ein Zusatzprogramm) für das E-Mailprogramm Microsoft Outlook bzw. für Kontact unter Linux, das Programm Kleopatra zur

Dateiverschlüsselung und für das Schlüsselmanagement und die Erweiterung GpgEX zur Dateiverschlüsselung im Windows Explorer bzw. in Dolphin unter Linux.

Das Produkt unterstützt zum Austausch und zur Speicherung öffentlicher Schlüssel sowohl den S/MIME-Standard und verwendet X.509-Zertifikate als auch den OpenPGP-Standard mit OpenPGP-Zertifikaten. Der geheime private Schlüssel ist entweder direkt durch Verwendung einer in Annex A gelisteten Smartcard oder mittelbar durch einen Hardware-Sicherheitsanker in der Einsatzumgebung geschützt (vgl. BSI-VS-AP-0014-2022) in der eine zugelassene Festplattenverschlüsselung oder ein zugelassener sicherer VS-Arbeitsplatz verwendet wird.

Die wesentlichen Sicherheitsleistungen des Produkts bestehen aus:

- Bearbeitung empfangener S/MIME-verschlüsselter oder signierter Dateien und E-Mails sowie deren Entschlüsselung und Signaturverifikation
- Bearbeitung empfangener OpenPGP-verschlüsselter oder signierter Dateien und E-Mails sowie deren Entschlüsselung und Signaturverifikation
- Erstellung von S/MIME -verschlüsselten oder signierten Dateien und E-Mails
- Erstellung von OpenPGP -verschlüsselten oder signierten Dateien und E-Mails
- Symmetrische Ver- und Entschlüsselung von Dateien mittels eines Passworts
- Erzeugung von OpenPGP-Schlüsseln.
- Verwendung von RSA mit PKCS#1-Padding in der Version 1.5 und AES im CBC-Modus bei S/MIME
- Verwendung von RSA und ECC mit Brainpoolkurven und AES in einem modifizierten CFB-Modus oder OCB-3 Modus bei OpenPGP
- Verwendung als Backend in automatisierten Lösungen (Kommandozeile)
- Verwalten von Schlüsseln bzw. Schlüsselzertifikaten

Dazu gehört beim Empfang einer S/MIME-signierten Datei oder E-Mail sowie beim Versenden einer S/MIME-verschlüsselten Datei oder E-Mail jeweils die Prüfung der zugehörigen Zertifikatskette auf Basis von Sperrlisten, OCSP-Abfragen und vertrauenswürdigen Root-Zertifikaten.

Am betrachteten Arbeitsplatz erfolgt die Verarbeitung von offenen und maximal VS-NfD eingestuften Informationen. Dafür muss der Arbeitsplatz freigegeben sein. Insbesondere dürfen nur berechtigte Personen Zutritt zum Arbeitsplatz haben.

2.3 Zulassung und zugelassener Konstruktionsstand

Die Art der Zulassung und der aktuell zugelassene Konstruktionsstand von GnuPG VS-Desktop sind Annex A zu entnehmen.

Vor einer Installation und Inbetriebnahme des Produktes hat sich der Geheimschutzbeauftragte mit Hilfe des Betreibers des IT-Systems davon zu überzeugen, dass für das IT-System eine Zulassung für den Betrieb (Approval to Operate (ATO)) von der zuständigen SAA (falls vorhanden) für den zu schützenden Geheimhaltungsgrad vorliegt. Für deutsche VS ist die Dienststellenleitung mit

Unterstützung des Geheimschutzbeauftragten für die Freigabe für den Einsatz zuständig (für die entsprechenden Geheimhaltungsgrade (national, EU, NATO) oder SoM Level).

2.4 Kompatibilität, Interoperabilität, Konformität

GnuPG VS-Desktop ist kompatibel zu anderen zugelassenen Produkte, die den S/MIME-Standard mit X.509-Zertifikaten oder den OpenPGP-Standard zum Austausch und zur Speicherung öffentlicher Schlüssel unterstützen.

Eine VS-NfD- oder EU/NATO RESTRICTED-konforme Kommunikation ist nur mit den dafür zugelassenen Produkten möglich, auch wenn andere technisch kompatibel sind. Die Kommunikationspartner sollten sich gegenseitig zusichern, dass sie entsprechende Produkte einsetzen. Eine technische Prüfung (z. B. auf Algorithmen, Modi und Schlüssellänge) wird von den Produkten durchgeführt und das Ergebnis angezeigt.

2.5 Betriebsarten

Die Software GnuPG VS-Desktop muss in der Betriebsart: „Konformität VS-NfD“ betrieben werden.

2.6 Installation, Systemintegration und Konfiguration

Anforderungen für die Installation und Integration von GnuPG VS-Desktop in einem IT-System, sowie eine systemspezifische Konfiguration sind der Herstellerdokumentation zu entnehmen. Die Umsetzung dieser Anforderungen sind vom Betreiber und der SAA (falls vorhanden) im Rahmen der Installation, Konfiguration und Akkreditierung sicherzustellen.

Zusätzlich zu der Herstellerdokumentation sind nachfolgende Vorgaben zu beachten und einzuhalten:

- Administration, Installation und Konfiguration der Software müssen bei der ersten Initialisierung in einem gesicherten Bereich von dazu berechtigtem Personal durchgeführt werden
- Vor der Installation bzw. einer Aktualisierung ist die Integrität des Installationspakets zu prüfen. Dazu ist die Signatur der Installationsdatei auf Gültigkeit zu überprüfen. Die Quellen der dafür nötigen aktuellen Schlüssel des Herstellers werden im Annex A angegeben.
- Bei der Installation und Administration der Rechner, auf denen GnuPG VS-Desktop eingesetzt wird, muss eine Trennung zwischen Anwender und Administrator auf Ebene des Betriebssystems erfolgen. Der Administrator ist dabei für die Installation des Produkts sowie die Durchsetzung der entsprechenden Optionen für die zugelassene Version über Gruppenrichtlinien verantwortlich.

2.7 Betrieb

Die Anforderungen, die beim zugelassenen Betrieb von GnuPG VS-Desktop zu beachten sind, können der Herstellerdokumentation oder dem Handbuch zur Zulassung entnommen werden.

Darüberhinausgehende Anforderungen sind nachfolgend aufgeführt:

1. Keine Schadprogramme auf den verwendeten Rechnern:

Die Systeme, auf denen GnuPG VS-Desktop zum Einsatz kommt, müssen frei von Schadsoftware sein.

2. Nutzung der Zertifikate aus der Verwaltungs-PKI oder einer vergleichbaren PKI für den S/MIME-Standard:

Eine PKI stellt durch die Umsetzung der für sie gültigen Policy von der Zertifizierungsstelle bis zum Teilnehmer sicher, dass Signaturen, Verschlüsselung und Authentisierung vertrauenswürdig eingesetzt werden können. Bei der Nutzung des Produktes GnuPG VS-Desktop nach S/MIME-Standard zum Schutz von Daten mit der Einstufung VS-NfD muss eine PKI verwendet werden, welche den Anforderungen der TR-03145-VS-NfD Secure CA operation gerecht wird.

3. Prüfung auf Widerruf von Zertifikaten für den S/MIME-Standard:

Eine wichtige Sicherheitsmaßnahme ist die Prüfung eines Zertifikats vor dessen Gebrauch auf Widerruf durch Abruf von Sperrlisten (Certificate Revocation List - CRL) oder OCSP-Abfragen bei der ausstellenden CA. Ungültig erklärte Zertifikate werden von der ausstellenden Zertifizierungsstelle entsprechend gekennzeichnet. Die Prüfung auf Widerruf sollte vor jedem Gebrauch eines Zertifikats durchgeführt und möglichst in den Gruppenrichtlinien für alle Nutzer vorgeschrieben werden.

4. Zertifikate für den S/MIME-Standard und Sperrlisten können u. a. über LDAP abrufbar sein:

Zertifikate und Sperrlisten werden von CAs in Verzeichnissen veröffentlicht. Dort können sie u. a. mittels des Protokolls "LDAP" (Lightweight Directory Access Protocol) gesucht und abgerufen werden. Der Verzeichniszugriff ist durch die IT-Administration zu konfigurieren.

5. Auswahl der kryptographischen Algorithmen für den OpenPGP-Standard:

Bei der Erstellung eines OpenPGP-Schlüsselpaars kann der Anwender wählen zwischen RSA (3072 Bit) und ECDSA/ECDH mit Brainpool-Kurven (256, 384 oder 512 Bit).

Die Gültigkeitsdauer ist mit 2 Jahren voreingestellt und kann vom Nutzer verlängert werden; das BSI empfiehlt hier eine maximale Gültigkeitsdauer von 3 Jahren.

6. Empfangen von OpenPGP-Zertifikaten/Schlüsseln

Bei der Verwendung von Schlüsseln im OpenPGP-Format ist der Nutzer eigenständig für die Authentizität der Schlüssel verantwortlich. Vor der erstmaligen Nutzung eines OpenPGP-Schlüsselzertifikats hat sich der Nutzer von der Echtheit des Zertifikats zu vergewissern, insbesondere, wenn er das Zertifikat nicht persönlich vom Inhaber erhalten hat, sondern wenn er es beispielsweise über einen Schlüsselservers, in einem E-Mail-Anhang oder durch einen Dritten erhalten hat. Um die Echtheit des Zertifikats zu überprüfen, kann der Empfänger eines Zertifikats den Inhaber telefonisch kontaktieren, um den Fingerabdruck des im Zertifikat enthaltenen Schlüssels zu vergleichen. Der Fingerabdruck kann im Zertifikatsmanager Kleopatra angezeigt werden (siehe Abbildung). Die Überprüfung muss mit einer „Beglaubigung“ im System hinterlegt werden.

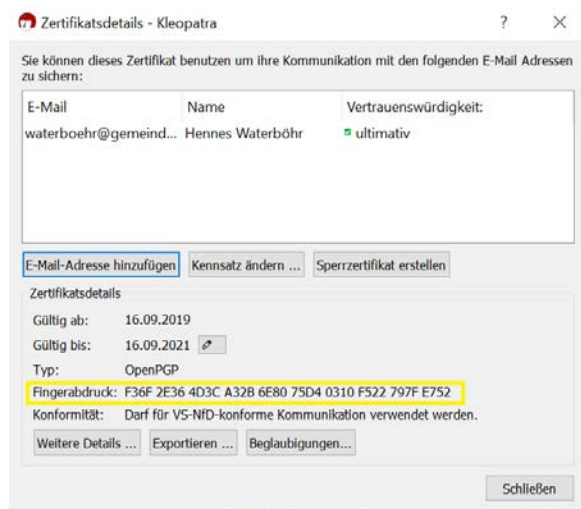


Abbildung 1: Zertifikatsdetails - Kleopatra

7. PIN-Cache:

Die Funktionalität PIN-Cache der Smartcard sollte deaktiviert werden.

8. Eingesetzte Smartcard:

Für den zugelassenen Betrieb dürfen grundsätzlich nur solche Smartcards eingesetzt werden, welche in Annex A gelistet sind. Zur Nutzung alternativer Smartcards müssen sich Anwender an den Hersteller wenden, der diese Nutzung mit dem BSI abstimmt.

9. Nutzung der Smartcard:

Die Smartcard darf nicht an Dritte weitergegeben werden. Die in Verbindung mit GnuPG VS-Desktop genutzten Hardware-Schlüsselspeicher sollten grundsätzlich nicht in anderen Anwendungen zum Einsatz kommen.

10. Smartcard-PINs:

Die PINs der Smartcard zum Schutz der geheimen Signatur- und Entschlüsselungsschlüssel dürfen nur dem Eigentümer zugänglich sein.

11. PUK von Smartcards:

Beim Einsatz von Smartcards oder einem anderen Hardware-Speicher kann es notwendig sein, diese von einer autorisierten Stelle entsperren lassen zu können. Deshalb soll bei der Beschaffung darauf geachtet werden, dass bei der Smartcard oder einem anderen Hardware-Speicher die Implementierung einer PUK (Personal Unblocking Key) vorhanden ist.

12. Verwendung von Softtoken

Bei der Verwendung von Softtoken sind diese bei der Erstellung durch Passwörter zu sichern, welche die Anforderungen des BSI-Grundschutzes erfüllen und der Rechner ist durch eine zugelassene Festplattenverschlüsselung oder einen zugelassenen sicheren VS-IT Arbeitsplatz zu schützen

13. Auswahl der kryptografischen Algorithmen für den S/MIME-Standard:

Durch die genutzte PKI (etwa Bundeswehr-PKI oder Verwaltungs-PKI) werden kryptografische Algorithmen aus dem S/MIME-Standard vorgegeben. Diese sind bei GnuPG VS-Desktop durch den Hersteller voreingestellt, können aber vom Betreiber auf andere zugelassene Algorithmen geändert werden.

Nicht konforme Wahlmöglichkeiten dürfen den Anwendern nicht zur Verfügung stehen und sind durch die IT-Administration mittels entsprechender Konfiguration der Produkte auszuschließen.

14. Symmetrische Ver- und Entschlüsselung mittels Passwörtern

Bei der symmetrischen Ver- und Entschlüsselung mittels Passwörtern sind starke Passwörter zu verwenden. Ein Passwort sollte dabei aus mindestens 20 zufällig gewählten Zeichen bestehen. Die Bestandteile des Passworts dürfen keinem Wörterbuch zu entnehmen sein. Zur Erzeugung von Passwörtern, sollte der Passwortgenerator von GnuPG VS-Desktop verwendet werden um eine hinreichende Entropie bei maximaler Kompatibilität zu erreichen. (Hinweis: Es ist legitim das Passwort aufzuschreiben und vergleichbar sicher zu verwahren wie VS-NfD. Wenn möglich, sollte eine asymmetrische Ver- und Entschlüsselung mittels SmartCard bevorzugt werden.)

Passwörter, mit denen VS-NfD-Daten verschlüsselt werden, sind selbst mindestens VS-NfD einzustufen. Sollen mit einem Schlüssel eine große Anzahl von VS-NfD-Daten geschützt werden, ist der Schlüssel gemäß Anlage 1 zu § 8 der VSA [1] ggf. höher einzustufen.

Der Austausch von Passwörtern muss auf einem vertraulichen Wege erfolgen. Passwörter mit der Einstufung VS-NfD sind auszutauschen

- bei einem persönlichen Kontakt,
- über eine mindestens für VS-NfD zugelassene verschlüsselte Verbindung (Telefon, Fax oder DFÜ),
- per Post; vornehmlich in einem versiegelten Umschlag oder als Wertbrief.

VS-NfD-eingestufte Passwörter sollen nicht über eine offene Telefonverbindung ausgetauscht werden. Keinesfalls darf ein Passwort unverschlüsselt über das Internet (z. B. als E-Mail) versandt werden. Wenn ein Passwort nicht persönlich übergeben wird, muss sich der Sender telefonisch beim Empfänger über den ordnungsgemäßen Eingang des Passworts erkundigen, bevor er es das erste Mal zum Verschlüsseln einsetzt.

15. Durch den Nutzer nicht veränderbare Wurzelzertifikate:

Zertifikate von Wurzelzertifizierungsstellen (Root-CA) haben eine besondere Funktion bei der Prüfung von Zertifikaten. Spricht man dem Wurzelzertifikat sein Vertrauen aus, so vertraut man indirekt auch allen Zertifikaten, die in der Hierarchie darunter angeordnet sind. Das Aussprechen des Vertrauens gegenüber Wurzelzertifikaten stellt daher einen sicherheitskritischen Schritt bei der Nutzung von Produkten für elektronische Signatur und Verschlüsselung dar.

Wurzelzertifikate sollen nur durch die IT-Administration im E-Mail-Client bzw. in Kleopatra verankert bzw. verändert werden können und somit integritätsgeschützt gespeichert sein. Die IT-Administration muss entscheiden, ob der Import von weiteren Wurzelzertifikaten dem Nutzer eigenverantwortlich gestattet ist.

16. Unverschlüsselte Speicherung der E-Mails auf dem Server:

Unverschlüsselte VS-NfD-eingestufte E-Mails dürfen nur in für VS-NfD geeigneten Umgebungen abgespeichert werden.

17. Beachtung der ausgewählten E-Mail-Adressen:

Im Adressbuch des E-Mail-Clients speichert der Anwender im Allgemeinen neben den internen Adressen der jeweiligen Organisation auch Adressen externer Kommunikationspartner. Bei Übereinstimmungen zwischen den Synonymen, unter denen die interne und externe Adresse im Adressbuch abgelegt ist (z. B. gibt es eine Frau Mueller intern und als externe Adressatin – beide sind als „mueller“ im Adressbuch vorhanden), besteht die Gefahr der Verwechslung bei der Auswahl eines Adressaten.

Der Nutzer muss daher die Empfängeradresse und die zugeordneten Schlüssel sorgfältig prüfen und sich vergewissern, dass keine Verwechslungen vorliegen.

18. Automatisch signieren:

Im E-Mail-Client sollte die Einstellung „Nachrichten automatisch signieren“ immer aktiv sein.

19. Vermeiden von HTML-Inhalten:

Die E-Mail-Clients Outlook bzw. Contact sollten grundsätzlich keine HTML Inhalte anzeigen. Das Nachladen externer Inhalte muss ausgeschaltet sein.

20. Verwendung als Backend in automatisierten Lösungen (Kommandozeile)

Bei der Verwendung als Backend in automatisierten Lösungen muss sichergestellt sein, dass die notwendige Passphrase zur Entschlüsselung, Signatur oder symmetrischen Verschlüsselung sicher übergeben wird. Hierzu wird die Verwendung der Option "--passphrase" explizit ausgeschlossen.

Nur die Optionen "--passphrase-fd" und "--passphrase-file" dürfen Verwendung finden. Alternativ kann ein dediziertes Pinentry Modul benutzt werden.

21. Bei der Entschlüsselung von Daten über das Kommandozeileninterface muss sichergestellt sein, dass die option --require-compliance übergeben wird, um bei nicht konformen Operationen einen Fehler zu erzwingen. Sollte dies nicht möglich sein müssen die Statusmeldungen von GnuPG ausgewertet werden
22. Beachtung der Hinweise in der Benutzerdokumentation und den Release-Notes:
Wichtige Hinweise, wie mit dem Produkt umzugehen ist und wie Warn- und Fehlermeldungen zu interpretieren sind können auf der Seite des Herstellers erhalten werden (<https://gnupg.com/vsd>). Insbesondere sind die Hinweise zur Konfiguration und sicheren Nutzung des Produkts GnuPG VS-Desktop zu beachten.

2.8 Abstrahlsicherheit

Bei GnuPG VS-Desktop handelt es sich um ein reines Softwareprodukt, das nicht abstrahlgeprüft wird.

3 SICHERHEITSMANAGEMENT

Nachfolgend werden besondere Anforderungen an das Sicherheitsmanagement bzw. Schlüsselmanagement von GnuPG VS-Desktop beschrieben.

3.1 Zuständigkeiten für Sicherheits-/Schlüsselmanagement

Der IT-Sicherheitsbeauftragte, der IT-System-Administrator und, sofern in Annex B Bestandteile des TOE mit dem Warnvermerk CRYPTO oder CCI versehen worden sind, der Kryptoverwalter sind in ihrem Zuständigkeitsbereich verantwortlich für die Umsetzung der Anforderungen.

Sofern eine SAA existiert, sind diese von der SAA in geeigneter Weise in die Akkreditierungsdokumentation einzubinden und im Rahmen der Systemakkreditierung zu überprüfen.

3.2 Beschreibung des Sicherheits-/Schlüsselmanagements

Das Sicherheitsmanagement für GnuPG VS-Desktop ist im Handbuch zur Zulassung von GnuPG VS-Desktop beschrieben.

3.3 Quantencomputer-Resistenz

Es wird darauf hingewiesen, dass das Produkt in der zugelassenen Konfiguration kryptografische Mechanismen verwendet, die nicht Quantencomputer-resistent sind.

4 VS-EINSTUFUNGEN

4.1 VS-Behandlungshinweise

Die für Kontroll- und Schutzmaßnahmen für GnuPG VS-Desktop zugrunde zu legenden VS-Einstufungen sind der als Annex B beigefügten Einstufungsliste zu entnehmen.

Sollten neben deutschen Verschlusssachen auch EU/NATO Classified Information verarbeitet werden, sind die entsprechenden EU/NATO Einstufungen ebenfalls zu berücksichtigen.³

³ EU/NATO Geheimhaltungsgrade und ihre jeweilige deutsche Entsprechung sind z.B. in Anlage VII [VSA] aufgeführt.

5 NACHWEISFÜHRUNG UND KONTROLLE

5.1 Verkauf, Ausleihe und Export

Für GnuPG VS-Desktop gibt es keine Einschränkungen hinsichtlich des Verkaufes, der Ausleihe und des Exports.

5.2 Konformitätserklärung (DoC)

In GnuPG VS-Desktop werden ausschließlich Typ B-Algorithmen eingesetzt. Die Unterzeichnung einer Konformitätserklärung ist daher nicht erforderlich.

5.3 VS-Nachweisführung und Kontrolle

Eine VS-Nachweisführung wird für GnuPG VS-Desktop nicht gefordert.

6 MATERIELLE SICHERHEIT

6.1 Zuständigkeiten

Dieses Kapitel beschreibt sicherheitsrelevante Aspekte hinsichtlich des Einsatzes von GnuPG VS-Desktop. Die strikte Einhaltung der nachfolgend aufgeführten Anweisungen ist erforderlich, um dauerhaft die Sicherheit der mit GnuPG VS-Desktop zu schützenden eingestufteten Informationen zu gewährleisten. Für die Umsetzung und Einhaltung dieser Vorgaben sind der Geheimschutzbeauftragte, der IT-Sicherheitsbeauftragte und, sofern in Annex B Bestandteile des TOE mit dem Warnvermerk CRYPTO oder CCI versehen worden sind, der Kryptoverwalter verantwortlich.

Sofern eine SAA existiert, sind diese von der SAA in geeigneter Weise in die Akkreditierungsdokumentation einzubinden und im Rahmen der Systemakkreditierung zu überprüfen.

6.2 Anforderungen an die Materielle Sicherheit

Die für den jeweiligen Anwender geltenden Geheimschutzbestimmungen zur materiellen Sicherheit sind zu beachten.

Werden EU- und NATO-eingestufte Verschlusssachen mit GnuPG VS-Desktop geschützt, kommen die Schutzmaßnahmen, die in den jeweiligen Vorschriften unter den Referenzen [2013/488/EU], [2015/844/EC], [2013/C 190/01], [IASG 2-03] und [C-M(2002)49], [SDIP-293] gemacht werden, ebenfalls zur Anwendung.

Darüber hinaus gelten nachstehende Sicherheitsvorgaben.

6.2.1 Allgemein

Für GnuPG VS-Desktop sind Sicherheitsvorkehrung in Übereinstimmung mit der Einstufungsliste in ANNEX B zu treffen.

- GnuPG VS-Desktop darf nur von autorisiertem Personal benutzt und betrieben werden, das eine Nutzer-Chipkarte und das erforderliche Nutzer-Passwort (User Access Code (UAC)) besitzt.
- Im Betrieb ist GnuPG VS-Desktop gegen unautorisierten Zugriff zu schützen, um einen Missbrauch und eine dadurch verursachte Kompromittierung der Vertraulichkeit oder eine Verletzung der Integrität oder der Authentizität geschützter Informationen und die Verletzung der Integrität von GnuPG VS-Desktop zu verhindern.
- GnuPG VS-Desktop ist in regelmäßigen Intervallen, die ein Jahr nicht überschreiten sollten, durch den IT-Sicherheitsbeauftragten (oder einer von diesem beauftragten Stelle) auf Manipulationen zu überprüfen.
- Jede vermutete Manipulation oder externe Beschädigung des zugelassenen Produktes ist unverzüglich dem zuständigen Geheimschutzbeauftragten oder IT-Sicherheitsbeauftragten zu melden (siehe Kapitel 10 „SICHERHEITSVORFÄLLE“).

6.2.2 Betriebsbereites Gerät

Die in Annex B aufgeführten VS-Einstufungen und Behandlungshinweise sind zu beachten.

6.2.3 Lagerung und Transport

Für Lagerung und Transport gelten keine besonderen Vorgaben.

6.2.4 Behandlung von Schlüsselmaterial

Der Endnutzer und, sofern in Annex B Bestandteile des TOE mit dem Warnvermerk CRYPTO oder CCI versehen worden sind, der Kryptoverwalter sind für eine sichere Handhabung des Schlüsselmaterials verantwortlich.

Die Anforderungen für die Handhabung von Schlüsselmaterial zum Schutz von eingestuften EU- und NATO-Informationen sind den Referenzen [IASG 2-03] und [SDIP-293] zu entnehmen.

6.3 Geräteschutzmechanismen

GnuPG VS-Desktop besitzt keine besonderen Geräteschutzmechanismen.

6.3.1 Meldung und Maßnahmen

Anforderung für das Melden eines Sicherheitsvorfalls oder vermuteten Sicherheitsvorfalls und zu ergreifende Maßnahmen sind in Kapitel 10 aufgeführt.

6.4 Routinemäßige Vernichtung

6.4.1 Vernichten/Löschen von Schlüsseln/Zertifikaten

Nicht mehr genutzte Smartcards können in ähnlichen Einsatzszenarien beim gleichen Anwender weiterhin verwendet werden. Dazu muss altes Schlüsselmaterial durch Neuinitialisierung aktiv überschrieben werden.

6.4.2 Produktentsorgung und -vernichtung

Bzgl. der Entsorgung und Vernichtung von GnuPG VS-Desktop bestehen keine besonderen Anforderungen.

Endgültig nicht mehr genutzte oder defekte Smartcards sind durch Zerstörung sicher zu vernichten (z.B. durch kreuzweises Zerschneiden des Smartcard-Chips).

Nach der Entscheidung eine Smartcard nicht mehr nutzen zu wollen, ist die Nichtverwendbarkeit dieser Karte bis zur endgültigen Vernichtung sicherzustellen. Dies kann durch technische und/oder organisatorische Maßnahmen erfolgen.

7 PERSONELLE SICHERHEIT

Zusätzlich zu den Maßnahmen und Kriterien, die in den Referenzen [SÜG], [VSA], [2013/488/EU], [2015/844/EC], [2013/C 190/01], [IASG 2-03] und [C-M(2002)49], [SDIP-293] beschrieben sind, gelten die nachfolgend aufgeführten Sicherheitsanforderungen für GnuPG VS-Desktop:

7.1 Zuständigkeiten

Die aufgeführten Maßnahmen bzgl. der personellen Sicherheit und Autorisierung des Personals sind vom Geheimschutzbeauftragten, Sicherheitsbevollmächtigten und dem IT-Sicherheitsbeauftragten zu beachten und umzusetzen.

7.2 Ermächtigung und Autorisierung

Zugang zu Verschlusssachen (VS), die im Sinne von § 4 Abs. 1, 2 [SÜG] mit dem Geheimhaltungsgrad VS-VERTRAULICH oder höher eingestuft sind, darf nur Personen gewährt werden, die zuvor nach dem SÜG und den allgemeinen Verwaltungsvorschriften zur Durchführung von Sicherheitsüberprüfungen überprüft und zum Zugang ermächtigt wurden.

VS des Geheimhaltungsgrades VS- NUR FÜR DEN DIENSTGEBRAUCH dürfen nur den Personen zugänglich gemacht werden, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis haben müssen. Bevor eine Person Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH erhält, ist sie auf Anlage V zur Verschlusssachenanweisung [VSA] zu verpflichten. Dabei ist ihr gegen Empfangsbestätigung ein Exemplar der Anlage V zugänglich zu machen.

7.3 Kenntnis nur, wenn nötig (Need-To-Know)

Der Zugang zu GnuPG VS-Desktop ist gemäß dem Prinzip „Kenntnis nur, wenn nötig (Need-To-Know)“ zu begrenzen.

8 WARTUNG UND REPARATUR

8.1 Zuständigkeiten

Folgende Vorgaben sind bei Wartung und Reparatur von GnuPG VS-Desktop zu beachten. In der Regel sind der Betreiber (ggf. unterstützt durch den Geheimschutzbeauftragten, den IT-Sicherheitsbeauftragte, den Systemadministrator und, sofern in Annex B Bestandteile des TOE mit dem Warnvermerk CRYPTO oder CCI versehen worden sind, den Kryptoverwalter) sowie der Hersteller für die Einhaltung der Maßnahmen in ihrem jeweiligen Zuständigkeitsbereich verantwortlich.

8.2 Vorgaben und Maßnahmen

Der Administrator sollte sich in regelmäßigen Abständen über aktualisierte Versionen des Produktes informieren und diese gegebenenfalls installieren.

Vor einer Aktualisierung der Software soll geprüft werden, ob für diese eine Sicherheitsaussage des BSI vorliegt.

Eine Wartung der Rechner und eine Aktualisierung der Software darf nur von dazu berechtigtem und geschultem Personal durchgeführt werden.

9 NOTFALLPROZEDUREN

Für den Schutz nationaler VS sind für GnuPG VS-Desktop keine speziellen Notfallprozeduren vorgesehen.

9.1 Zuständigkeiten

In der Regel sind der Betreiber, der Geheimschutzbeauftragte, der IT-Sicherheitsbeauftragte, der Systemadministrator, der Nutzer und, sofern in Annex B Bestandteile des TOE mit dem Warnvermerk CRYPTO oder CCI versehen worden sind, der Kryptoverwalter in ihrem jeweiligen Verantwortungsbereich zuständig für die Umsetzung und Einhaltung der nachfolgend aufgeführten Maßnahmen.

9.2 Notfallplan

Der Schutz von GnuPG VS-Desktop und zugehörigem Schlüsselmaterial unter Notfallbedingungen sollte in einem vom Nutzer bzw. Betreiber zu erstellenden Notfallplan adressiert sein, der die unter Notfallbedingungen zu ergreifenden Maßnahmen beschreibt.

Die Anforderungen der EU- und NATO für einen Notfallplan können den Referenzen [IASG 2-03] und [SDIP-293] entnommen werden.

10 SICHERHEITSVORFÄLLE

10.1 Ansprechpartner des Betreibers

Der Betreiber bzw. Endnutzer des Produktes ist verpflichtet, dem Hersteller einen Ansprechpartner für Sicherheitsthemen z.B. den Geheimschutz- oder IT-Sicherheitsbeauftragten inkl. Kontaktdaten zu benennen und diese Informationen auf dem aktuellen Stand zu halten. Der Hersteller wird diesen Ansprechpartner nur für Informationen zu Sicherheitsvorfällen, erforderlichen Sicherheitsmaßnahmen, sicherheitsrelevanten Produktupdates sowie Aktualisierungen dieser Zulassung kontaktieren.

10.2 Meldepflicht und Zuständigkeiten

Für die Untersuchung und den Bericht meldepflichtiger Sicherheitsvorfälle sind die SAA (falls vorhanden) und der Betreiber (unterstützt durch den Geheimschutzbeauftragten und den IT-Sicherheitsbeauftragten) zuständig.

Die in der Referenz [BSI TL - IT 01] aufgeführten Mitwirkungspflichten von Hersteller und Bedarfsträger bei der Behandlung von Sicherheitsvorfälle (Incidents) sind zu beachten.

10.3 Meldepflichtige Vorfälle

Eine Auflistung meldepflichtiger Vorfälle und Vorgaben für einen Bericht sind in den Referenzen [IASG 2-03] und [SDIP-293] enthalten. Diese Vorgaben werden auch national für meldepflichtige Vorfälle zugrunde gelegt. Das BSI nimmt gegenüber der NATO die Funktion der „German National CIS Security Authority (NCSA)“ wahr. Bei der EU wird diese Funktion auch als „Crypto Approval Authority (CAA) bezeichnet.

10.4 Maßnahmen bei BSI-Warnung

Bei entdeckten Schwachstellen des Produkts oder entdeckten Sicherheitsproblemen in seiner Einsatzumgebung kommuniziert das BSI oder der Hersteller nach Absprache mit dem BSI Warnungen und Hinweise, i.d.R. verbunden mit umzusetzenden Maßnahmen (bspw. unverzügliche Update Pflicht, Austausch von Zertifikaten, Änderung in der Konfiguration des Produkts, Änderung der Einsatz- und Betriebsbedingungen, etc.).

Diese Warnungen und Hinweise werden durch den Hersteller an den in 10.1 genannten Ansprechpartner des Betreibers gesendet.

Diesen Anweisungen ist verpflichtend Folge zu leisten.

11 KONTAKTE

11.1 Hersteller

g10 code GmbH
Bergstr. 3a
40699 Erkrath
Deutschland
<https://g10code.com>

Anfragen und Support: vsbfd@gnupg.com

11.2 BSI Krypto-Support

Bei entdeckter oder vermuteter Manipulation nennen Sie bitte nur die Gerätebezeichnung und Ihre Kontaktinformation.

Weitere Informationen müssen vertraulich ausgetauscht werden.

Bundesamt für Sicherheit in der Informationstechnik
Krypto-Support
Postfach 20 03 63
53133 Bonn

E-Mail: krypto-support@bsi.bund.de

11.3 BSI Zulassung

Bei Fragen zum Verfahren verweisen wir auf unsere FAQ-Übersicht im Internet unter <https://www.bsi.bund.de/Zulassung>

Sollten darüber hinaus noch Fragen offen sein, so können Sie sich – sofern es sich um nicht sensible Inhalte handelt – per E-Mail an folgende Adresse wenden:

E-Mail: zulassung@bsi.bund.de

DE-Mail: zulassung@bsi-bund.de-mail.de

ANNEX A

Zulassung und Konstruktionsstand

GnuPG VS-Desktop

Zulassungs-ID BSI-VSA-10867

1 Zulassung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für GnuPG VS-Desktop mit der Zulassungs-ID BSI-VSA-10867 mit Stand 31.05.2024 eine Zulassung für den Schutz von Informationen ausgestellt, die national als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft sind.

Mit dieser Zulassung können auch Informationen mit dem Geheimhaltungsgrad NATO RESTRICTED und NATO-VS, die einen Strength of Mechanism (SoM) STANDARD (NATO) erfordern, sowie Informationen mit dem Geheimhaltungsgrad RESTREINT UE/EU RESTRICTED und EU-VS, die einen Strength of Mechanism (SoM) STANDARD (EU) erfordern, geschützt werden.

Die in den Einsatz- und Betriebsbedingungen getroffenen Regelungen sind einzuhalten.

Nachfolgend ist der aktuell zugelassene Konstruktionsstand von GnuPG VS-Desktop aufgeführt. Der Konstruktionsstand wird für jede zugelassene Produktversion festgehalten und ist integraler Bestandteil der Zulassungsdokumentation.

2 Überprüfung des Konstruktionsstandes

Der Hersteller ist für die Auslieferung von GnuPG VS-Desktop mit dem korrekten, zugelassenen Konstruktionsstand und der korrekten Version verantwortlich. Vor einer Installation und Inbetriebnahme ist vom Betreiber des IT-Systems und der SAA (falls vorhanden), ggf. unterstützt durch den IT-Sicherheitsbeauftragten zu prüfen, ob das zu installierende Produkt zugelassen ist und der Konstruktionsstand des ausgelieferten Produktes mit dem nachfolgend aufgeführten, zugelassenen Konstruktionsstand übereinstimmt. Vor der ersten Nutzung ist der Betrieb des Produktes durch den jeweiligen Dienststellenleiter für den Einsatz für den entsprechenden nationalen Geheimhaltungsgrad freizugeben und für EU/NATO classified information gemäß EU/NATO Vorschriften zu akkreditieren.

3 Abweichungen vom Konstruktionsstand

Werden Abweichungen zwischen dem hier aufgeführten und dem ausgelieferten Konstruktionsstand festgestellt, sind die in Kapitel 11 des Hauptteils dieses Dokumentes aufgeführten Kontakte zu konsultieren, um eine Klärung herbeizuführen.

4 Konstruktionsstand

Nachfolgend ist der aktuell zugelassene Konstruktionsstand von GnuPG VS-Desktop aufgeführt. Der Konstruktionsstand wird für jede zugelassene Produktversion festgehalten und ist integraler Bestandteil der Zulassungsdokumentation.

Zulassungsgegenstand

Nr	Software
1	GnuPG VS-Desktop, Version 3.x, ab Unterversion 3.1.26 und folgende

In der Regel wird GnuPG VS-Desktop vom Hersteller an den Endnutzer mit folgenden System- und Zubehörkomponenten ausgeliefert:

1. Windows Installationspaket (GnuPG-VS-Desktop-3.1.x.msi) sowie zugehörige OpenPGP-Signatur:
GnuPG-VS-Desktop-3.1.x.msi.sig
2. Linux AppImage (gnupg-vs-desktop-3.1.x-x86_64.AppImage) sowie zugehörige OpenPGP-Signatur:
gnupg-vs-desktop-3.1.x-x86_64.AppImage.sig
3. Vollständiger Quelltext (GnuPG-VS-Desktop-3.1.x.tar.bz2) sowie zugehöriger OpenPGP-Signatur:
GnuPG-VS-Desktop-3.1.x.tar.bz2.sig
4. Die OpenPGP-Signaturen der zulässigen Komponenten werden vom Hersteller g10 Code GmbH (GnuPG) erstellt. Üblicherweise wird dafür folgender Schlüssel verwendet:

```
pub brainpoolP256r1 2021-10-15 [SC] [expires: 2029-12-31]
02F3 8DFF 731F F97C B039 A1DA 549E 695E 905B A208
uid GnuPG.com (Release Signing Key 2021)
```

Die jeweils aktuellen Schlüssel des Herstellers finden sich unter:

<https://gnupg.org/signature-key.pdf>

5. Smartcards:
 - TeleSec NetKey 3.0
 - SLE78CFX*P mit CardOS 5.0, CardOS 5.3
 - SLE78CLUFH*H mit Yubikey Firmware Version 5.x

ANNEX B

Einstufungsliste

GnuPG VS-Desktop

Zulassungs-ID BSI-VSA-10867

		Geheimhaltungsgrad ^{a b}				OFFEN ^a	Bemerk.
		STRENG GEHEIM	GEHEIM	VS-V	VS-NfD		
1	GnuPG VS-Desktop SW-Installationsmedium					X	1)
2	Nutzer Smartcard					X	2) 4)
3	GnuPG VS-Desktop, installiert, betriebsbereit				X		
4	GnuPG VS-Desktop, ausgeschalteter Zustand, Schlüssel geladen				X		3) 5)
5	GnuPG VS-Desktop, ausgeschalteter Zustand, Schlüssel gelöscht				X		3) 4)

- 1) Das Installationsmedium ist nicht eingestuft, jedoch bezüglich seiner Integrität zu schützen.
- 2) Die Smartcard ist nicht eingestuft, doch jederzeit gegen unbefugten Zugriff zu schützen
- 3) Eine personenbezogene Nachweisführung ist nicht erforderlich.
- 4) GnuPG VS-Desktop und Chipkarten sind separat zu lagern und zu transportieren.

Abkürzungen Einstufungen/Kennzeichnungen:

VS-NfD (VS-NUR FÜR DEN DIENSTGEBRAUCH)

VS-V (VS-VERTRAULICH)

CCI (Controlled Cryptographic (COMSEC) Item)

- a Nationale Kryptomittel im Sinne § 59 Abs. 1 VSA sind Produkte, Geräte und die dazugehörigen Dokumente sowie zugehörige Schlüsselmittel zur Entschlüsselung, Verschlüsselung und Übertragung von Informationen, die vom BSI als solche festgelegt werden. Kryptomittel sind gem. Abschnitt IX, VSA insbesondere mittels Kryptoverwalter zu handhaben. Kryptomittel verfügen gem. § 59 Abs. 2 VSA bei vorliegender Einstufung über den Warnvermerk „CRYPTO“ bzw. „KRYPTO“ oder bei nicht vorliegender Einstufung den Warnvermerk „CCI“. EU-Vorschriften hierzu sind im IASG2-03 Annex B, respektive für die NATO im SDIP-293-1 Kap. 6 aufgeführt.
VS-IT-Produkte, die keine Kryptomittel im Sinne von § 59 Abs. 1 VSA sind, werden in der obigen Tabelle dagegen lediglich mit „X“ markiert.
- b Bei der Verwendung des Produktes zum Schutz von NATO / EU-Verschlusssachen gelten korrespondierende internationale Geheimhaltungsgrade und Markierungen.