Bundesamt
für Sicherheit in der
Informationstechnik

Nachweis der Zulassung von Produkten mit Sicherheitsfunktionen nach VSA

BSI-VSA-10187

Zulassung für den Geheimhaltungsgrad:

VS - NUR FÜR DEN DIENSTGEBRAUCH

E-Mail- und Datei-Verschlüsselungs-Software (Ende-zu-Ende)

Gpg4 VS-NfD (Gpg4win und Gpg4KDE)
Version 3.X

Hersteller: Intevation GmbH

Für das Produkt Gpg4 VS-NfD (Gpg4win und Gpg4KDE), Version 3.X des Herstellers Intevation GmbH wurde mit Datum vom 31.01.2019 die Zulassung BSI-VSA-10187 erteilt. Die Zulassung ermöglicht die Verarbeitung und Übertragung von VS - NUR FÜR DEN DIENSTGEBRAUCH eingestuften Informationen. Zur Definition von VS - NUR FÜR DEN DIENSTGEBRAUCH siehe §4 Nr. 4 SÜG (§2 Nr. 4 VSA).

Das Produkt Gpg4 VS-NfD, Version 3.X ist für den Schutz von EU-Informationen bis zum Geheimhaltungsgrad RESTREINT UE/EU RESTRICTED für den nationalen Einsatz zugelassen.

Das Produkt Gpg4 VS-NfD, Version 3.X ist für den Schutz von NATO-Informationen bis zum Geheimhaltungsgrad NATO RESTRICTED zugelassen.

Diese Zulassung ist befristet bis zum 31.01.2022.

Diese Zulassung gilt nur in Verbindung mit dem vollständigen Report, für die in ANNEX A (Konstruktionsstände) aufgeführten oder referenzierten Konstruktionsstände und die nach den SecOps Gpg4 VS-NfD installierten und betriebenen Produkte.

Das BSI übernimmt keine Gewährleistung für das Produkt.

Bonn, 31.01.2019

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

[redacted]

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, D-53175 Bonn • Postfach 20 03 63, D-53133 Bonn
Tel.: +49 (0)228 9582-0 • Fax: +49 (0)228 9582-5400 • Internet: www.bsi.bund.de

Stand: 31.01.2019

Bundesamt
für Sicherheit in der
Informationstechnik

Report BSI-VSA-10187

Gpg4 VS-NfD

(Gpg4win und Gpg4KDE)

Version 3.X

der

Intevation GmbH

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSI-Gesetz[1] und VS-Anweisung[2] die Aufgabe, für IT-Sicherheitsprodukte (Systeme oder Komponenten) Zulassungen zu erteilen.

Diese Zulassung eines Produktes wird auf Veranlassung eines behördlichen Antragstellers, nach einer begründeten Bedarfsmeldung und im Einvernehmen mit dem Hersteller durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produktes gemäß den Richtlinien des BSI.

Die Prüfung wird in der Regel vom BSI durchgeführt.

Das Ergebnis des Verfahrens ist im hier vorliegenden Report zusammengefasst. Hierin als Anhang enthalten sind die für diese Zulassung gültigen SecOps einschließlich mindestens ANNEX A (Konstruktionsstände) und ANNEX B (Einstufungsliste) sowie evtl. weiterer ANNEXE.

1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821

2 Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) vom 31. März 2006

Inhaltsverzeichnis

1. Grundlagen des Zulassungsverfahrens

Die Zulassungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821
- Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) vom 10. August 2018

2. Prüfgegenstand

Gegenstand der Zulassung ist das Produkt

Gpg4 VS-NfD, Version 3.X

des Herstellers

Intevation GmbH
Neuer Graben 17
49074 Osnabrück
Deutschland

3. Prüfstelle

Folgende vom BSI akkreditierte Prüfstelle hat die Prüfung durchgeführt:

Bundesamt für Sicherheit
in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

Die Evaluierung wurde vom Bundesamt für Sicherheit in der Informationstechnik, Abteilung KT, durchgeführt.

4. Durchführung der Evaluierung und Zulassung

Die Evaluierung des Prüfgegenstandes wurde von der oben angegebenen Prüfstelle durchgeführt. Sie wurde am 09.07.2018 beendet.

Das Verfahren wurde damit beendet, dass das BSI die Übereinstimmung mit den Richtlinien überprüft und den vorliegenden Report erstellt hat.

5. Ergebnis der Zulassung

Die Zulassung wurde mit Datum vom 31.01.2019 erteilt.

Gpg4 VS-NfD Version 3.X ist hiermit für die Übertragung und Verarbeitung von nationalen Verschlusssachen bis einschließlich zum Geheimhaltungsgrad VS - NUR FÜR DEN DIENSTGEBRAUCH zugelassen.

6. Gültigkeit der Zulassung

Dieser Report bezieht sich nur auf die angegebene Version des Prüfgegenstandes.

Die Zulassung gilt nur

- für die in ANNEX A (Konstruktionsstände) der SecOps Gpg4 VS-NfD aufgeführten oder referenzierten Konstruktionsstände,
- für Produkte, die gemäß der SecOps Gpg4 VS-NfD installiert und betrieben werden. Hierzu sind die Secops mit jedem ausgelieferten Produkt dem Nutzer zur Verfügung zu stellen und ggf. beim Nutzer in vorhandene Dienstanweisungen zu integrieren. Die Überwachung der wirksamen Umsetzung der Einsatz- und Betriebsbedingungen liegt in der Verantwortung des zuständigen Geheimschutz- bzw. IT-Sicherheitsbeauftragten, des Betreibers und des Anwenders.

Die Zulassung ist befristet bis zum 31.01.2022.

Die Zulassung berücksichtigt die technischen Möglichkeiten zum Zeitpunkt der Ausstellung. Angriffe, mit neuen oder weiterentwickelten Methoden, die in Zukunft möglich sind, können im Rahmen dieses Verfahrens nicht berücksichtigt werden. Die Zulassungsstelle befristet daher die Zulassung, um regelmäßig eine Einschätzung der Widerstandsfähigkeit vornehmen zu können.

7. Internationale Zulassungen

Für diesen Prüfgegenstand liegen folgende internationale Zulassungen vor bzw. werden durch das BSI erteilt:

7.1. EU

Gpg4 VS-NfD, Version 3.X ist mit Datum vom 31.01.2019 unter der Kennung BSI-VSA-10187 für die Verarbeitung von EU-Informationen bis zum Geheimhaltungsgrad STANDARD zugelassen.

7.2. EU

Gpg4 VS-NfD, Version 3.X erfüllt die EU-Anforderungen, gemäß dem EU „Requirements Model" für „Strength of Cryptographic Mechanism" STANDARD[1] und ist zugelassen für den Schutz von EU eingestuften Informationen, in Einsatzszenarien, die mit Kryptomechanismen der Stärke STANDARD geschützt werden können.

Sofern die vorgegebenen Einsatz- und Betriebsbedingungen eingehalten werden, kann das Produkt Gpg4 VS-NfD, ohne weitere Einschränkung, in allen Einsatzszenarien für den Schutz von RESTREINT UE / EU RESTRICTED eingestuften Informationen eingesetzt werden.

7.3. NATO

Gpg4 VS-NfD, Version 3.X ist mit Datum vom 31.01.2019 unter der Kennung BSI-VSA-10187 für die Verarbeitung von NATO-Informationen bis zum Geheimhaltungsgrad STANDARD zugelassen.

7.4. NATO

Gpg4 VS-NfD, Version 3.X erfüllt die NATO-Anforderungen, gemäß dem NATO „Requirements Model" für „Strength of Mechanism" STANDARD[2] und ist zugelassen für den Schutz von NATO

[1] Vgl. EU Council 10745/11 – IASP 2 – Information Assurance Security Policy on Cryptography, 30 May 2011, RESTREINT UE/EU RESTRICTED

[2] Vgl. AC/322-D/0047-REV2 – INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, NATO RESTRICTED

eingestuften Informationen, in Einsatzszenarien, die mit Krypto-Mechanismen der Stärke STANDARD geschützt werden können.

Sofern die vorgegebenen Einsatz- und Betriebsbedingungen eingehalten werden, kann das Produkt Gpg4 VS-NfD, ohne weitere Einschränkung, in allen Einsatzszenarien für den Schutz von NATO RESTRICTED [3] eingestuften Informationen eingesetzt werden.

8. Veröffentlichung

Das Produkt Gpg4 VS-NfD, Version 3.X wird in die „Liste der zugelassenen IT-Sicherheitsprodukte und -Systeme“ (BSI 7164) aufgenommen; diese kann auf den Webseiten des BSI eingesehen werden.

9. Hinweise an den Hersteller

9.1. Änderungen am zugelassenen Produkt

Im Falle von Änderungen an der evaluierten Version des Produktes kann die Gültigkeit auf neue Versionen ausgedehnt werden, sofern für das geänderte Produkt ein entsprechender Antrag durch die behördlichen Bedarfsträger gestellt wird und die Evaluierung keine sicherheitstechnischen Mängel ergibt.

9.2. Vertrieb

Zugelassene Kryptosysteme und deren Komponenten unterliegen einem eingeschränkten Vertrieb.

Der Export von zugelassenen Kryptosystemen und deren Komponenten unterliegt der deutschen Exportgesetzgebung und bedarf grundsätzlich der Zustimmung der zuständigen Stellen.

10. Literaturverzeichnis

[BSI-Gesetz, 2009]

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821

[IT-Grundschutz-Kataloge, 2008]

Webseite des BSI (inkl. Ergänzungslieferungen), https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[Verschlusssachenanweisung, 2018]

Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) vom 10. August 2018

[EU-Council Security Rules, CSR]

COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified

3 Für einen Einsatz mit Geheimhaltungsgrad „NATO-SECRET“ oder höher ist eine erfolgreiche Zweitevaluierung durch die zuständige NATO-Behörde und eine Zulassung durch das NATO Military Committee (NAMILCOM) erforderlich.

information (2013/488/EU)

[NATO C-M (2002)49, 2002]

Security within the North Atlantic Treaty Organisation vom 26. März 2002

Bundesamt
für Sicherheit in der
Informationstechnik

Einsatz- und Betriebsbedingungen Gpg4 VS-NfD (Gpg4win und Gpg4KDE) Version 3.X

BSI-VSA-10187

Stand: 31.01.2019

VS-Einstufung: offen

Nationale Version

Inhaltsverzeichnis

Annexe

ANNEX A - ZULASSUNG UND KONSTRUKTIONSSTAND

ANNEX B - EINSTUFUNGSLISTE

Leere Seite

EINSATZ- UND BETRIEBSBEDINGUNGEN FÜR

Gpg4 VS-NfD (Gpg4win und Gpg4KDE) Version 3.X

VORWORT

Die vorliegenden Einsatz- und Betriebsbedingungen für Gpg4 VS-NfD, international auch als Security Operating Procedures (SecOPs) bezeichnet, werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben und sind integraler Bestandteil der Zulassungsdokumentation von Gpg4 VS-NfD.

Sie beschreiben die Mindestanforderungen für die sichere Installation, Integration und Konfiguration sowie für die Kontrolle, den Schutz und den Betrieb von Gpg4 VS-NfD, und das zugehörige Sicherheitsmanagement und die gerätespezifische Dokumentation.

Diese Einsatz- und Betriebsbedingungen ergänzen das Nutzerhandbuch Gpg4win-Kompendium von Gpg4 VS-NfD in einigen sicherheitsrelevanten Bereichen und sind gemeinsam mit diesem zu lesen und anzuwenden.

Das Anfertigen von Kopien oder Auszügen dieser BSI-Richtlinie ist unter Beachtung des Einstufungsgrades für behördliche Zwecke ohne weitere Genehmigung des BSI erlaubt.

Die Beachtung und Umsetzung dieser BSI-Richtlinie ist verbindlich für den Betrieb von Gpg4 VS-NfD. Abweichende Regelungen bedürfen der ausdrücklichen schriftlichen Genehmigung durch das BSI.

Dieses Dokument sollte allen Stellen, die IT-Systeme mit Gpg4 VS-NfD planen, Gpg4 VS-NfD implementieren und betreiben, um damit VS zu schützen, sowie den verantwortlichen IT-Sicherheitsbeauftragten und Endnutzern, unter Beachtung des Prinzips „Kenntnis nur wenn nötig“ zur Verfügung gestellt werden.

Falls erforderlich, wird das BSI Ergänzungen zu dieser Richtlinie herausgeben.

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

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
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 Dokument beinhaltet die Einsatz- und Betriebsbedingungen für Gpg4 VS-NfD, international auch als Security Operating Procedures (SecOPs) bezeichnet, für den Schutz von Verschlusssachen (VS) mit dem maximalen Einstufungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH.

Es beschreibt die Mindestanforderungen für die sichere Installation, Integration und Konfiguration sowie für die Kontrolle, den Schutz und den Betrieb von Gpg4 VS-NfD, zugehörigem Sicherheitsmanagement, Zubehör und gerätespezifischer Dokumentation, nachfolgend als Gpg4 VS-NfD bezeichnet.

1.2 Verwendung

Diese Einsatz- und Betriebsbedingungen gelten national für alle Anwendungen, in denen Gpg4 VS-NfD zum Schutz von nationaler VS zum Einsatz kommt. Sie sollten allen, die für die Installation und Kontrolle, sowie für den Betrieb von Gpg4 VS-NfD verantwortlich sind, zur Verfügung gestellt werden.

1.3 Weitergabe

Im Falle einer Weitergabe von Gpg4 VS-NfD an ausländische Nationen oder nicht-deutsche Institutionen, gelten keine besonderen Bedingungen.

1.4 Referenzen

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

Nationale Sicherheitsvorschriften		
	National	
	[**SÜG**]	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG)
	[**VSA**]	Verschlusssachenanweisung - Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen, vom 31.03.2006 in der Fassung vom 26. 04.2010
Vorschriften mit kryptographischem Bezug		
	National	
	[**BSI-TL 03426**]	BSI - Technische Leitlinie -Vernichtung/Entsorgung von Kryptomaterial (Mai 2015)
Sonstige Referenzen		
	Zulassungen	
	[**Zulassung-National**]	Nationale Zulassung für den Schutz von VS - NUR FÜR DEN DIENSTGEBRAUCH: BSI-VSA-10187, vom 31.01.2019, inkl. Anlagen
	Nutzerhandbücher	
	Nutzerhandbuch	Gpg4win-Kompendium (deutsch) 4.0.1, 03.04.2018
	Zulassungshandbuch	Handbuch zur Zulassung von Gpg4win und Gpg4KDE 1.6, 24.04.2018

1.5 Begriffsbestimmungen

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

Allgemeine Begriffe und Abkürzungen	
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CAA	Crypto Approval Authority (EU-Begriff; in Deutschland das BSI)
CIS	Communications and Information Systems
DEUmilSAA	Beim Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) angesiedelte Stelle, die für den Bereich der Bundeswehr die Aufgaben einer SAA übernimmt.
IT	Informationstechnik
Kryptomaterial	Unter dem Begriff Kryptomaterial werden zusammengefasst: Schlüsselmaterial in jeglicher Form, sowie Produkte und Geräte, die Kryptoanteile zur Ver-/Entschlüsselung oder Authentisierung enthalten, um die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von VS-IT-Systemen sicherzustellen.
NCSA	National CIS Security Authority (in Deutschland das BSI)
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
SAA	Security Accreditation Authority
SecOPs	Security Operating Procedures (Einsatz und Betriebsbedingungen)
SoM	Strength of Mechanism
VS	Verschlusssache(n)
VS-NfD	VS-NUR FÜR DEN DIENSTGEBRAUCH
VSA	Verschlusssachenanweisung (bindend für alle Bundesbehörden)

1.6 Parteien und Instanzen

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

- **Administrator / Systemadministrator**
  Die Person(en), die das VS-IT-Produkt oder -System administrieren. Diese ist (sind) verantwortlich für sichere Einrichtung des VS-IT-Produktes oder -Systems. In der Regel hat der Administrator volle Zugriffsrechte für die Konfiguration und Bedienung des VS-IT-Produktes oder -Systems.
- **Betreiber (des IT-Systems)**
  Die Stelle, die für den Betrieb des IT-Systems verantwortlich ist . Der Betreiber ist u.a. zuständig für:
  - die geschäftlichen und betrieblichen Anforderungen an das IT-System, Vorgaben für dessen Betrieb und Anforderungen bzgl. des Informationsaustausches;
  - Zuarbeit für die SAA bei der Erstellung einer Risikobewertung für das IT-System (wenn erforderlich);
  - die Erstellung eines Planes um das bei einer Risikobewertung ermittelte Restrisiko zu handhaben;
  - die Sicherstellung, dass Servicevereinbarungen (Service Level Agreements (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 (evtl. zusammen mit der SAA) im Falle eines Sicherheitsvorfalls, Feststellung des Schadens und Berichterstattung (an die SAA, falls vorhanden und an den Krypto-Support des BSI).

- **BSI**
  Das BSI ist als nationale IT-Sicherheitsbehörde u.a. zuständig für IT-sicherheitstechnische Bewertungen (Evaluierungen) von Sicherheitsprodukten/-systemen und deren Zulassung oder Zertifizierung. 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.
- **Endnutzer (End User)**
  Die Person(en), die das VS-IT-Produkt oder -System als Anwender nutzen und bedienen. Diese ist (sind) verantwortlich für die Umsetzung der in den vorliegenden Einsatz- und Betriebsbedingungen aufgestelltem 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.
- **Geheimschutzbeauftragter**
  Der Geheimschutzbeauftragte sorgt für die Umsetzung der Verschlusssachenanweisung (VSA) und berät die Dienststellenleitung in allen Fragen des Geheimschutzes. Der Geheimschutzbeauftragte hat ein unmittelbares Vortragsrecht bei der Dienststellenleitung und ist bei allen geheimschutzrelevanten Maßnahmen zu beteiligen.
  Er ist in der Regel verantwortlich für:
  - o die korrekte Umsetzung und Einhaltung von allgemeinen Sicherheits- und Schutzmaßnahmen (materielle Sicherheit, Sicherheit von Personen, Sicherheit von Liegenschaften, usw.) für die Einsatzumgebung, in der ein VS-System betrieben wird;
  - o ggf. die Mitprüfung und Bestätigung der Akkreditierungsunterlagen der SAA;
  - o Durchführung regelmäßiger Überprüfungen, zur Bestätigung, dass in seinem Verantwortungsbereich alle vorgegebenen Sicherheitsmaßnahmen zum Schutz der betriebenen VS-Systeme eingehalten werden.
- **Hersteller**
  Der Hersteller eines zugelassenen IT-Sicherheitsproduktes 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.
- **IT-Sicherheitsbeauftragter**
  Soweit in Behörden IT-Sicherheitsbeauftragte bestellt sind, unterstützen diese die Geheimschutzbeauftragten bei der Umsetzung der VSA. Sie sind verantwortlich für alle Fragen des Einsatzes von IT zur Handhabung von VS. Sind keine IT-Sicherheitsbeauftragten bestellt, bestellen die Behörden einen IT-Geheimschutzbeauftragten, der diese Aufgaben wahrnimmt.
  Der Verantwortungsbereich eines IT-Sicherheitsbeauftragten umfasst in der Regel folgende Zuständigkeiten:
  - o Beratung der Endnutzer und Führungskräfte in Fragen der IT-Sicherheit und Stärkung des IT-Sicherheitsbewusstseins;
  - o Dokumentation aller Personen, die Zugang zu einem VS-IT-System haben, sowie deren Zugriffsrechte und VS-Ermächtigungen;
  - o Mitprüfung der Implementierung und Wartung von Hard-, Soft- und Firmware-Modifikationen und -Erweiterungen von VS-IT-Systemen unter dem Aspekt der Aufrechterhaltung der IT-Sicherheit.

- Sicherstellung der korrekten Anwendung und Einhaltung der Sicherheitsvorgaben für ein VS-IT-System (z.B. Übertragung, Verschlüsselung, Abstrahlsicherheit), sowie für die Handhabung und den Schutz von Kryptomaterial;
- Prüfung von Protokolldaten (Log-files) bzgl. der Nutzung eines VS-IT-Systems zur Feststellung einer unbefugten Nutzung oder Systemaktivität;
- periodische Durchführung, bzw. Koordination von Risiko- und Bedrohungsanalysen für ein VS-IT-System;
- Unterrichtung der SAA (falls vorhanden) im Falle entdeckter Schwachstellen oder Verwundbarkeiten eines VS-IT-Systems;
- Management und Untersuchung von IT-Sicherheitsvorfällen, in Zusammenarbeit mit dem Geheimschutzbeauftragten, der SAA (falls vorhanden) und falls erforderlich, dem BSI.

- **Kryptoverwalter**
  Behörden/Dienststellen, die Kryptomaterial handhaben, bestellen einen Kryptoverwalter, der im Rahmen der VSA für die ordnungsgemäße Verwaltung von Kryptomaterial sorgt.
  Im Falle von Gpg4 VS-NfD kann der Kryptoverwalter für die Verteilung von Smartcards an die Mitarbeiter zuständig sein.
- **Security Accreditation Authority (SAA)**
  VS-IT-Systeme erfordern vor der Inbetriebnahme eine Prüfung und Akkreditierung durch die zuständige SAA.
  Die SAA ist zuständig für die Prüfung und Akkreditierung von IT-Systemen, unter Beachtung nationaler oder EU-/NATO-Vorschriften, je nach vorgesehenem Einsatz des IT-Systems. Eine Akkreditierung durch die SAA bezieht sowohl die operationellen Rahmenbedingungen, als auch eine Risikobewertung und eine Restrisikoabschätzung in die Bewertung mit ein.
  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.
  Gegenüber der EU und der NATO nimmt das BSI die Rolle der obersten nationalen Instanz für Systemakkreditierungen wahr.
  Der Aufgabenbereich einer SAA umfasst normalerweise:
  - Beratung der Endnutzer bzgl. der Anwendung und Umsetzung von IT-Sicherheitsvorschriften und flankierenden Maßnahmen;
  - Etablierung eines Akkreditierungsprozesses für IT-Systeme, Definition der Akkreditierungsanforderungen und der Anforderungen für eine Anbindung an andere IT-Systeme.
  - Prüfung und Genehmigung sicherheitsrelevanter Dokumentation
  - Durchführung und Berücksichtigung einer Risikobewertung für das zu akkreditierende IT-System
  - Akkreditierung, bzw. Re-akkreditierung für IT-Systeme und Nennung evtl. vorgegebener Auflagen/Vorgaben für den Betrieb.
  - Durchführung periodischer Sicherheitsinspektionen, bzw. von Prüfungen, in Übereinstimmung mit dem Akkreditierungsprozess.
  - Unterstützung des Geheimschutzbeauftragten und des IT-Sicherheitsbeauftragten bei der Untersuchung von Sicherheitsvorfällen.
  - Beratung und Unterstützung, bzw. Vermittlung der richtigen Ansprechpartner zur Durchführung von entsprechenden Korrekturmaßnahmen nach erfolgten Sicherheitsvorfällen.
  - Beratung (z.B. des Geheimschutzbeauftragten und des IT-Sicherheitsbeauftragten) hinsichtlich der entstehenden Sicherheitsrisiken und Risiken für die eingesetzten Schutzmaßnahmen im Falle von Änderungen am IT-System.
  - Zusammenarbeit mit den SAAs (falls vorhanden) anderer IT-Systeme, die mit einem akkreditierten / zu akkreditierenden System vernetzt werden sollen.
  - Beratung bei der Anbindung von VS-IT-Systemen an andere IT-Systeme.
  - Zusammenarbeit und Koordination mit dem BSI, wenn zugelassene IT-Sicherheitsprodukte (z.B. Kryptogerät) in dem IT-System eingesetzt werden sollen.

2 SYSTEMBERSCHREIBUNG

2.1 Einsatzzweck

Gpg4 VS-NfD soll in Form der Produkte Gpg4win und Gpg4kde den VS-NfD-konformen verschlüsselten Austausch von E-Mails sowie die VS-NfD-konforme Verschlüsselung von Dateien ermöglichen. Gpg4 VS-NfD kann auf den Plattformen Windows und GNU/Linux 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 (Gpg4win) oder für Kontact unter Linux (Gpg4KDE) mit einer Zertifikatsverwaltung. Es unterstützt den S/MIME-Standard mit X.509-Zertifikaten sowie den OpenPGP-Standard mit OpenPGP-Zertifikaten zum Austausch und zur Speicherung öffentlicher Schlüssel. (Zu OpenPGP siehe aber Abschnitt 2.2!)

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

Mit dem Produkt Gpg4win/Gpg4KDE lassen sich E-Mails, Dateien und Datei-Ordner einfach ver- und entschlüsseln, sowie ihre Integrität (Unversehrtheit) und Authentizität (Herkunft) mittels digitaler Signaturen absichern und überprüfen.

Die zulassungsrelevanten Gpg4win-/Gpg4KDE-Kompenenten setzen sich wie folgt zusammen:

Gpg4win ist ein Installationspaket für Windows und besteht aus verschiedenen Freien-Software-Komponenten, die wahlweise installiert werden können.

Gpg4KDE sind einzelne Software-Pakete, die über den jeweiligen Paketmanager der Linux-Distribution installiert werden können.

GnuPG:

Das Kernstück; das eigentliche Verschlüsselungsprogramm.

Kleopatra:

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

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

In der Regel wird Gpg4 VS-NfD vom Hersteller an den Endnutzer mit folgenden System- und Zubehörkomponenten ausgeliefert (siehe auch Nutzerhandbuch Gpg4win-Kompendium (Referenz H1)):

Bei den Produkten Gpg4win und Gpg4KDE 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. Die unterstützten Versionen von Microsoft Outlook und Kontact werden im Konstruktionsstand aufgeführt.

Das Produkt unterstützt den S/MIME- und den OpenPGP-Standard, verwendet X.509- und OpenPGP-Zertifikate zum Austausch und zur Speicherung öffentlicher Schlüssel. Optional kann für den zugelassenen Betrieb eine Smartcard zur Speicherung von Langzeitgeheimnissen, wie die geheimen Signatur- oder Entschlüsselungsschlüssel, eingesetzt werden. Zurzeit ist keine zugelassene SmartCard für den OpenPGP-Standard verfügbar, aber für den S/MIME-Standard. Sobald eine zugelassene SmartCard für OpenPGP verfügbar ist, finden die Anforderungen in diesem Dokument auch darauf Anwendung.

Die wesentlichen Sicherheitsleistungen des Produkts bestehen aus:

- Bearbeitung empfangener E-Mails von S/MIME- und OpenPGP-verschlüsselter oder signierter E-Mails sowie deren Entschlüsselung und Signaturverifikation,
- Erstellung von S/MIME- und OpenPGP-verschlüsselten oder signierten E-Mails.
- 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 in einem modifizierten CFB-Modus bei OpenPGP
- Verwalten von Schlüsseln bzw. Schlüsselzertifikaten

Dazu gehört beim Empfang einer signierten Nachricht sowie beim Versenden einer S/MIME verschlüsselten 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. Der Arbeitsplatz erfüllt die folgenden Bedingungen:

- Der Arbeitsplatzrechner ist direkt oder über eine VPN-Verbindung in ein lokales Netz (LAN) eingebunden und kommuniziert über einen dedizierten Gateway-Rechner mit dem Internet. Auch Stand-Alone-Rechner sind möglich.
- Das lokale Netz, in dem sich der Arbeitsplatz befindet, ist für die Verarbeitung von Verschlusssachen mit der Einstufung VS-NfD freigegeben.
- Der Arbeitsplatz inklusive Hardware, installierter Software etc. ist für die Verarbeitung von Verschlusssachen mit der Einstufung VS-NUR FÜR DEN DIENSTGEBRAUCH freigegeben.
- Zutritt zum Arbeitsplatz haben nur berechtigte Personen.

2.3 Zulassung und zugelassener Konstruktionsstand

Die Art der Zulassung und der aktuell zugelassene Konstruktionsstand von Gpg4 VS-NfD sind ANNEX A zu entnehmen.
Vor einer Installation und Inbetriebnahme des Produktes ist eine Überprüfung des Konstruktionsstandes des ausgelieferten Produktes vorzunehmen sowie dessen Konformität mit dem zugelassenen Konstruktionsstand zu verifizieren. Dies sollte durch den Betreiber des IT-Systems und die SAA (falls vorhanden), ggf. unterstützt durch den IT-Sicherheitsbeauftragten, erfolgen. Vor der ersten Nutzung ist der Betrieb des Produktes von dem Betreiber des IT-Systems für den Einsatz freizugeben (für die entsprechenden Einstufungsgrade (national, EU, NATO) oder SoM Level).
Weitere Einzelheiten sind in ANNEX A beschrieben.

2.4 Kompatibilität, Interoperabilität, Konformität

Die Software ist für den Einsatz auf Standard-PCs und Laptops mit Windows- oder Linux-Betriebssystem zur sicheren Übertragung von Informationen mit der Einstufung "VS-NfD" mittels S/MIME oder OpenPGP kodierter Mails und zur Verschlüsselung von Dateien geeignet. (Zu OpenPGP siehe aber Abschnitt 2.2!) Die

Rechner müssen dazu für VS-NfD freigegeben sein und sich in einem für VS-NfD freigegebenen Netz befinden. Auch Stand-Alone-Rechner sind möglich. Die Integrität der Rechner und der darauf installierten Software ist eine wesentliche Voraussetzung dafür, dass die Sicherheitsfunktionen wirksam werden können.

2.5 Betriebsarten

Die Software GPG4Win und GPG4KDE muss in der Betriebsart: „Konformität VS-NfD“ betrieben werden.

2.6 Installation, Systemintegration und Konfiguration

Anforderungen für die Installation und Integration von Gpg4 VS-NfD in einem IT-System, sowie eine systemspezifische Konfiguration sind im Zulassungshandbuch „Handbuch zur Zulassung von Ggp4win und Gpg4KDE“ aufgeführt. Die Umsetzung dieser Anforderungen sind vom Betreiber und der SAA (falls vorhanden) im Rahmen der Installation, Konfiguration und Akkreditierung sicherzustellen.

Zusätzlich zu den im Zulassungshandbuch beschriebenen Installations-, Integrations- und Konfigurationshinweisen 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 ist die Integrität des Installationspakets zu prüfen, welches von der Internetseite heruntergeladen wurde. Dazu ist ein SHA-256 Hashwert über das Installationspaket mittels eines geeigneten Tools zu bilden.
- Der jeweils gültige Hashwert wird vom BSI zur Verfügung gestellt. (Annex A)
- Bei der Installation und Administration der Rechner, auf denen Gpg4 VS-NfD 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 Gpg4 VS-NfD zu beachten sind, können dem Nutzerhandbuch Gpg4win-Kompendium entnommen werden.

Darüber hinausgehende Anforderungen sind nachfolgend aufgeführt:

1. Keine Schadprogramme auf den verwendeten Rechnern:

Die Systeme, auf denen Gpg4 VS-NfD zum Einsatz kommt, müssen frei von Schadsoftware und Viren sein. Ist dies nicht der Fall, können Informationen von den infizierten Systemen unbemerkt abfließen. Die eingesetzten Rechner und das Netzwerk, in dem sich die Rechner befinden, müssen zur Verarbeitung, Speicherung und Weiterleitung von Verschlusssachen mit der Einstufung VS-NUR FÜR DEN DIENSTGEBRAUCH freigegeben sein.

2. Aktivierung der VS-Konfiguration

Die VS-Konfiguration ist durch die IT-Administration zu aktivieren.

3. 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 Gpg4 VS-NfD nach S/MIME-Standard zum Schutz von Daten mit der Einstufung VS-NUR FÜR DEN DIENSTGEBRAUCH muss eine PKI verwendet werden, welche den Anforderungen der TR-03145-VS-NfD Secure CA operation gerecht wird.

4. 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.

5. 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.

6. PIN-Cache:

Die Funktionalität PIN-Cache der Smartcard ist zu deaktivieren, da hierdurch die Gefahr einer unberechtigten Nutzung deutlich erhöht wird.

7. Eingesetzte Smartcard:

Für den zugelassenen Betrieb sollen nur solche Smartcards eingesetzt werden, welche im Konstruktionsstand vermerkt sind. Zur Nutzung alternativer Smartcards müssen sich Anwender an den Hersteller wenden, der diese Nutzung mit dem BSI abstimmt.

8. Nutzung der Smartcard:

Die Smartcard darf nicht weitergegeben werden. Die in Verbindung mit Gpg4win und Gpg4KDE genutzten Hardware-Schlüsselspeicher sollten grundsätzlich nicht in anderen Anwendungen zum Einsatz kommen. Zu erwägen ist ein Einsatz bei solchen anderen Anwendungen, in denen die PIN sicher eingegeben werden kann.

9. Smartcard-PINs:

Die PINs der Smartcard zum Schutz der geheimen Signatur- und Entschlüsselungsschlüssel dürfen nur dem Eigentümer zugänglich sein, da anderenfalls unbefugte Dritte die elektronischen Signaturen im Namen des Eigentümers erzeugen oder für den Eigentümer bestimmte Nachrichten entschlüsseln können.

10. 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.

11. Auswahl der kryptographischen Algorithmen für den S/MIME-Standard:

Durch die genutzte PKI (etwa Bundeswehr-PKI oder Verwaltungs-PKI) werden kryptographische Algorithmen aus dem S/MIME-Standard vorgegeben. Diese sind bei Gpg4 VS-NfD durch den Hersteller voreingestellt.

Für den Anwender kann wählbar sein:

- Die Schlüssellänge (128, 192 oder 256) des Blockchiffre-Algorithmus AES,
- die Schlüssellänge des Public-Key-Verschlüsselungs-/Signatur-Verfahrens (RSA), mindestens aber 3072 Bit,
- der Hashalgorithmus (SHA-256, SHA-384 oder SHA-512)

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

TripleDES darf nur zum Entschlüsseln von E-Mails oder Dateien verwendet werden.

Die Generierung von RSA-Schlüsseln ist an geeigneter Stelle so zu konfigurieren, dass sie den Empfehlung der BSI TR-02102-11 entspricht.

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

Die kryptographischen Algorithmen sind durch den Hersteller voreingestellt.

Für den Anwender kann wählbar sein:

- Die Schlüssellänge (128, 192 oder 256) des Blockchiffre-Algorithmus AES,
- das Public-Key-Verschlüsselungs-/Signatur-Verfahren und dessen Schlüssellänge:
  - RSA mit mindestens 3072 Bit oder
  - ECDH/ECDSA mit den Brainpoolkurven P256r1, P384r1 oder P512r1
- der Hashalgorithmus (SHA-256, SHA-384 oder SHA-512)

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

TripleDES darf nur zum Entschlüsseln von E-Mails oder Dateien verwendet werden.

Die Generierung von RSA-Schlüsseln ist an geeigneter Stelle so zu konfigurieren, dass sie den Empfehlung der BSI TR-02102-12 entspricht.

13. Empfangen von OpenPGP-Zertifikaten/-Schlüsseln

Der Empfänger eines OpenPGP-Schlüssels hat sich von dessen Authentizität zu vergewissern. Hierzu prüft der Empfänger, dass der Fingerprint vom empfangenen Schlüssel authentisch ist. Wenn der Sender des Schlüssels persönlich bekannt ist, kann der Empfänger den Sender anrufen und den Fingerprint telefonisch vergleichen.

14. Sicherstellung der Qualität empfangener OpenPGP-Zertifikate/-Schlüssel

Der Empfänger eines OpenPGP-Schlüssels muss sich beim Sender erkundigen, mit welchem Programm der Schlüssel erzeugt wurde. Nur folgende Programme darf dabei vom Empfänger akzeptiert werden.

- Gpg4win ab Version 3.1
- Gpg4KDE ab Version 3.1

Sollte der Schlüssel mit einem anderen Programm erstellt worden sein, darf er vom Empfänger nicht zum Verschlüsseln von Dateien oder E-Mails mit der VS-Einstufung VS-NfD verwendet werden.

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 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. Verschlüsselte Speicherung der E-Mails auf dem Server:

Unverschlüsselte 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 Verwechselung bei der Auswahl eines Adressaten.

Der Nutzer muss daher die Empfängeradresse und die zugeordneten Schlüssel sorgfältig prüfen und sich vergewissern, dass keine Verwechslungen vorliegen. Um das Risiko einer Verwechslung zu verringern, empfiehlt es sich, auf eine Nutzung von Fremdadressen im Adressbuch zu verzichten bzw. die Nutzung und

Speicherung solcher Adressen stark einzuschränken. Es ist auch empfehlenswert über eine Gruppenrichtlinie oder in der Registry den Wert "PROMPT_RCV_CERT" mit '1' zu belegen, damit eine Bestätigung der Schlüssel, welche den Adressaten zugeordnet sind, vor dem Versenden einer verschlüsselten E-Mail erfolgen muss.

18. Nutzung von RAM-Disks für temporäre Dateien:

Besteht die Möglichkeit, eine RAM-Disk zu nutzen, sollten temporär erzeugte Files hierin abgelegt werden. Dies hat den Vorteil, dass mit Ausschalten des Rechners sämtliche dort gespeicherten Informationen verloren gehen.

19. Automatisch signieren:

Die Einstellung „Nachrichten automatisch signieren“ sollte immer aktiv sein.

20. Vermeiden von HTML-Inhalten:

Die E-Mail-Clients Outlook bzw. Kontact sollten grundsätzlich keine HTML Inhalte anzeigen und das Nachladen externer Inhalte muss ausgeschaltet sein.

21. Beachtung der Hinweise in der Benutzerdokumentation und den Release-Notes:

Das Benutzerhandbuch Gpg4win-Kompendium und die Release-Notes enthalten wichtige Hinweise, wie mit dem Produkt umzugehen ist sowie Warn- und Fehlermeldungen zu interpretieren sind. Insbesondere sind die Hinweise zur Konfiguration und sicheren Nutzung des Produkts Gpg4 VS-NfD zum Schutz gegen die unter dem Begriff „Efail“ unter CVE-2017-17689 bekannt gewordenen Angriffe zu beachten.

2.8 Abstrahlsicherheit

2.8.1 Schutz nationaler VS

Es bestehen keine speziellen Anforderungen bzgl. der Abstrahlsicherheit, wenn Informationen, die VS-NUR FÜR DEN DEINSTGEBRAUCH (VS-NfD) eingestuft sind, mit Gpg4 VS-NfD geschützt werden.

2.8.2 Schutz von EU-VS

Es bestehen keine speziellen Anforderungen bzgl. der Abstrahlsicherheit, wenn Informationen, die RESTREINT UE/EU RESTRICTED eingestuft sind, mit Gpg4 VS-NfD geschützt werden.

Für alle anderen Anwendungen, die eine vorherige Risikobewertung (Threat und Impact) nach dem EU „Requirements Model“ erfordern, das in Referenz [IASP 2] beschrieben ist, ist auch eine Überprüfung der Einhaltung der EU-Anforderungen zur Abstrahlsicherheit (Referenzen [IASP 7], [IASG 7-01], [IASG 7-02], [IASG 7-03]) erforderlich.
Wie bereits in Abschnitt 1.1 erläutert, ist diese Überprüfung und Bewertung durch das BSI, zusammen mit der SAA, falls nicht vorhanden, zusammen mit dem Betreiber vorzunehmen. In Abhängigkeit von der Anwendung und dem Einsatzszenario sind vor einem Einsatz ggf. zusätzliche Maßnahmen zur Herstellung der Abstrahlsicherheit erforderlich.

2.8.3 Schutz von NATO-VS

Es bestehen keine speziellen Anforderungen bzgl. der Abstrahlsicherheit, wenn Informationen, die NATO RESTRICTED eingestuft sind, mit Gpg4 VS-NfD geschützt werden.

Für alle anderen Anwendungen, die eine vorherige Risikobewertung (Threat und Impact) nach dem NATO „Requirements Model“ erfordern, das in Referenz [AC/322-D/0047] beschrieben ist, ist auch eine Überprüfung der Einhaltung der NATO-Anforderungen zur Abstrahlsicherheit (Referenzen [AC/322-D(2007)0036], [SDIP-27], [SDIP-28], [SDIP-29]) erforderlich. Wie bereits in Abschnitt 1.1 erläutert, ist diese Überprüfung und Bewertung durch das BSI, zusammen mit der SAA, falls nicht vorhanden, zusammen mit

dem Betreiber vorzunehmen. In Abhängigkeit von der Anwendung und dem Einsatzszenario sind vor einem Einsatz ggf. zusätzliche Maßnahmen zur Herstellung der Abstrahlsicherheit erforderlich.

3 SICHERHEITSMANAGEMENT

3.1 Zuständigkeiten für Sicherheits-/Schlüsselmanagement

Nachfolgend werden besondere Anforderungen an das Sicherheitsmanagement, bzw. Schlüsselmanagement von Gpg4 VS-NfD beschrieben. Der IT-Sicherheitsbeauftragte, der IT-System-Administrator sowie der Kryptoverwalter sind, in ihrem Zuständigkeitsbereich, verantwortlich für die Umsetzung der Anforderungen. Diese sind ggf. von der SAA (falls vorhanden) in geeigneter Weise in die Akkreditierungsdokumentation einzubinden und im Rahmen der Systemakkreditierung zu überprüfen.

3.2 Beschreibung des Sicherheits-/ Schlüsselmanagements

Das Sicherheitsmanagement für Gpg4 VS-NfD ist im Nutzerhandbuch Gpg4win-Kompendium beschrieben.

4 VS-EINSTUFUNGEN

4.1 VS-Behandlungshinweise

Die für Kontroll- und Schutzmaßnahmen für Gpg4 VS-NfD zugrunde zu legenden VS-Einstufungen, sind der als ANNEX B beigefügten Einstufungsliste zu entnehmen.

5 NACHWEISFÜHRUNG UND KONTROLLE

5.1 Verkauf, Ausleihe und Export

Für Gpg4 VS-NfD gibt es keine Einschränkungen hinsichtlich des Verkaufes, der Ausleihe und des Exports.

5.2 Konformitätserklärung

In Gpg4 VS-NfD werden ausschließlich Typ B-Algorithmen eingesetzt. Die Unterzeichnung einer Konformitätserklärung ist daher nicht erforderlich.

5.3 VS-Nachweisführung und VS-Kontrolle

5.3.1 VS-Nachweisführung

Eine VS-Nachweisführung wird für Gpg4 VS-NfD nicht gefordert.

5.3.2 Lieferung oder Weitergabe an Dritte

Über eventuelle Exportbestimmungen hinaus (vergleiche Kapitel 5.1), unterliegt Gpg4 VS-NfD keinen Weitergabebeschränkungen innerhalb der EU und NATO sowie deren Mitgliedsstaaten.

6 MATERIELLE SICHERHEIT

6.1 Zuständigkeiten

Dieses Kapitel beschreibt sicherheitsrelevante Aspekte hinsichtlich des Einsatzes von Gpg4 VS-NfD. Die strikte Einhaltung der nachfolgend aufgeführten Anweisungen ist erforderlich, um dauerhaft die Sicherheit der mit Gpg4 VS-NfD zu schützenden eingestuften Informationen zu gewährleisten. Für die Umsetzung und Einhaltung dieser Vorgaben sind der Geheimschutzbeauftragte, der Kryptoverwalter sowie der IT-

Sicherheitsbeauftragte verantwortlich. Sie sind von der SAA (falls vorhanden) in geeigneter Weise in die Akkreditierungsdokumentation einzubinden und von dieser im Rahmen der Systemakkreditierung zu überprüfen.

6.2 Anforderungen an die Materielle Sicherheit

Die Vorgaben, die für die materielle Sicherheit in den Referenzen gemacht werden, sind umzusetzen. Darüber hinaus gelten nachstehende Sicherheitsvorgaben.

6.2.1 Allgemein

Für Gpg4 VS-NfD sind Sicherheitsvorkehrung in Übereinstimmung mit der Einstufungsliste in ANNEX B zu treffen.

- Gpg4 VS-NfD 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 Gpg4 VS-NfD 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 Gpg4 VS-NfD zu verhindern.
- Gpg4 VS-NfD 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 ist unverzüglich dem zuständigen IT-Sicherheitsbeauftragten zu melden (siehe Kapitel 10, Sicherheitsvorfälle).

6.2.2 Betriebsbereites Gerät, Schlüsselmaterial nicht geladen

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

6.2.3 Betriebsbereites Gerät, Schlüsselmaterial geladen

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

6.2.4 Lagerung und Transport

Für Lagerung und Transport gelten keine besonderen Vorgaben.

6.2.5 Behandlung von Schlüsselmaterial

Insbesondere der Kryptoverwalter und der Endnutzer sind für eine sichere Handhabung des Kryptomaterials verantwortlich.

6.3 Geräteschutzmechanismen

Gpg4 VS-NfD 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

Vernichten/Löschen von Schlüsseln/Zertifikaten

Bei Entsorgung der Festplatte, die Schlüsselmaterial (geheime oder private Schlüssel) enthält, muss diese mit einer freigegebenen Software gelöscht oder physikalisch vernichtet werden.

6.5 Produktentsorgung und –Produktvernichtung

Gpg4 VS-NfD besitzt keine besonderen Vorgaben zur Produktentsorgung- und zur Produktvernichtung.

7 PERSONELLE SICHERHEIT

Zusätzlich zu den Maßnahmen und Kriterien, die in den Referenzen beschrieben sind, gelten die nachfolgend aufgeführten Sicherheitsanforderungen für Gpg4 VS-NfD.

7.1 Zuständigkeiten

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

7.2 Ermächtigung und Autorisierung

Verschlusssachen des Geheimhaltungsgrades VS-NfD dürfen nur den Personen zugänglich gemacht werden, die im Rahmen der Auftragsdurchführung oder -anbahnung Kenntnis davon erhalten müssen.

Ihnen ist das "Merkblatt zur Behandlung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD-Merkblatt)", Anlage 7 zur VS-Anweisung des BMI [VSA] vor dem Zugang nachweislich bekannt zu geben. Sie sind zur Einhaltung des VS-NfD-Merkblattes zu verpflichten und auf ihre besondere Verantwortung für den Schutz von VS-NfD, mögliche straf- oder vertragsrechtliche Konsequenzen bei Zuwiderhandlung ausdrücklich hinzuweisen.

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

Gpg4 VS-NfD besitzt keine besonderen Vorgaben bezüglich dieses Arbeitspunktes.

8 WARTUNG UND REPARATUR

8.1 Zuständigkeiten

Folgende Vorgaben sind bei Wartung und Reparatur von Gpg4 VS-NfD zu beachten. In der Regel sind der Betreiber (ggf. unterstützet durch den Kryptoverwalter, den IT-Sicherheitsbeauftragten, den Systemadministrator) 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 Gpg4 VS-NfD keine speziellen Notfallprozeduren vorgesehen.

9.1 Zuständigkeiten

In der Regel sind der Betreiber, der Kryptoverwalter, der IT-Sicherheitsbeauftragte, der Systemadministrator und der Nutzer in ihrem jeweiligen Verantwortungsbereich zuständig für die Umsetzung und Einhaltung der nachfolgend aufgeführten Maßnahmen.

9.2 Notfallplan
Gpg4 VS-NfD besitzt keine besonderen Vorgaben bezüglich dieses Arbeitspunktes.

9.3 Notlöschung
Gpg4 VS-NfD besitzt keine besonderen Vorgaben bezüglich dieses Arbeitspunktes.

10 SICHERHEITSVORFÄLLE

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

10.2 Meldepflichtige Vorfälle
Bei Verdacht auf Manipulation oder Feststellung sonstiger Auffälligkeiten (unerklärliche Störungen etc.) ist Gpg4 VS-NfD außer Betrieb zu nehmen und der zuständige Geheimschutzbeauftragte oder IT-Sicherheitsbeauftragte und ggf. das BSI zu informieren.

10.3 Maßnahmen nach entdeckter Kompromittierung
Der Bedarfsträger bzw. Nutzer des Produktes ist verpflichtet, dem Hersteller einen Ansprechpartner für Sicherheitsthemen z. B. den 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, sicherheitsrelevanten Produktupdates sowie Aktualisierungen dieser Zulassung kontaktieren.

11 KONTAKTE

11.1 Hersteller
Intevation GmbH
Neuer Graben 17
49074 Osnabrück
Deutschland
https://intevation.de

---

g10 code GmbH
Hüttenstr. 61
40699 Erkrath
Deutschland
https://g10code.com

Anfragen und Support: vsnfd@gpg4win.org

11.2 BSI Krypto-Support
Bei entdeckter oder vermuteter Manipulation nennen Sie bitte nur die Versionsnummer 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/DE/Service/FAQ/EvaluierungundZulassung/faq_node.html

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

von
Gpg4NfD (Gpg4win und Gpg4KDE)**, Version 3.X**

Zulassungs-ID BSI-VSA-10187

1 Zulassung

Gpg4NfD, 3.X ist mit der Zulassungs-ID BSI-VSA-10187 mit Stand 31.08.2018 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen für den Schutz von Informationen, die national als VS - NUR FÜR DEN DIENSTGEBRAUCH eingestuft sind.

Die in den Einsatz- und Betriebsbedingungen getroffenen Regelungen (insbesondere der Kapitel 2.3, 2.6, 3 und 5) sind einzuhalten.

Nachfolgend ist der aktuell zugelassene Konstruktionsstand von Gpg4NfD 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 Gpg4NfD mit dem korrekten, zugelassenen Konstruktionsstande und der korrekten Version verantwortlich. Vor einer Installation und Inbetriebnahme ist vom Betreiber des IT-Systems und die SAA (falls vorhanden), ggf. unterstützt durch den IT-Sicherheitsbeauftragten zu prüfen, ob der Konstruktionsstand des ausgelieferten Produktes mit dem nachfolgend aufgeführten, zugelassenen Konstruktionsstand übereinstimmt. Vor der ersten Nutzung ist der Betrieb des Produktes von dem Betreiber des IT-Systems für den Einsatz freizugeben (für die entsprechenden Einstufungsgrade (national, EU, NATO) oder SoM Level).

3 Abweichungen vom Konstruktionsstand

Werden irgendwelche 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 Gpg4NfD aufgeführt. Der Konstruktionsstand wird für jede zugelassene Produktversion festgehalten und ist integraler Bestandteil der Zulassungsdokumentation.

Die Zulassung bezieht sich auf die folgende Version:

Nr	Software
1	Version 3.X, ab Unterversion 3.1.5 und folgende

In der Regel wird Gpg4 VS-NfD vom Hersteller an den Endnutzer mit folgenden System- und Zubehörkomponenten ausgeliefert:

1. Gpg4win 3.1.5 (gpg4win-3.1.5.exe)
   SHA256: 4749ab2d02d384abc2b0fd045c86380e6f840b540a2081e6c0f7d538a3397b23
2. Smartcard:
   TeleSec NetKey 3.0
3. Die Softwarepakete der Produkte Gpg4win und Gpg4KDE werden mit dem öffentlicher OpenPGP-Schlüssel 42D876082688DA1A signiert der unter der URL https://ssl.intevation.de/Intevation-Distribution-Key-2016.asc bezogen werden kann:

   pub 3072R/42D876082688DA1A 2016-11-03 [expires: 2021-11-02]

   Key fingerprint = 13E3 CE81 AFEA 6F68 3E46 6E0D 42D8 7608 2688 DA1A

   uid Intevation File Distribution Key <distribution-key@intevation.de>

   -----BEGIN PGP PUBLIC KEY BLOCK-----

   Version: GnuPG v1

   mQGNBFgbBWABDACr63sgJWA1skGcPJ6keBztF+kvnQoGqjomSs+/wHEoPRECi77X
   YSVxxmN7mOn/qx8plbYfB8FtqQGqbqwdsHY2bR9NHbZlvrbqQdMK/BxB/GUv/g0F
   RO/VpwQFlZODksJXs4mjAE/srim3lFLNp9VNvh1gCwIPisKJwD3ay6rWodZ21mBY
   kZQckklOAT5w/kR7VkXhaa0XjDO3lLd2qg30ikjdFNe5EI4bjVt218zPDw94LuK9
   nkmk/ZFkjidZuzwyz9jo6iTi3huQMsR3oHFwMR7sgEMWetfLGubh04BbJXZQ6SSQ
   JFu9K9rKZ6/NJjZC0Is9taOMlMEibTncUOyHxAHHYLnsJyDeKFBZxQWi47e4AsT8
   /WLIw88GGIafq9eyrzXZLA7P+VkAaaWY7TzgiVORah9Ed8eObdpHERqthxNKHFOr
   gXLcKf1a04WGWCXngPvvjnTVmoe/4syBOOA256EcMNCQ35n1SgwnTVrkBchAF395
   JpwEhlo9y4XmWasAEQEAAbRBSW50ZXZhdGlvbiBGaWxlIERpc3RyaWJ1dGlvbiBL
   ZXkgPGRpc3RyaWJ1dGlvbi1rZXlAaW50ZXZhdGlvbi5kZT6JAboEEwECACQFAlgb
   BWACGwMFCQlmAYADCwkDBBUKCQgFFgIDAQACHgECF4AACgkQQth2CCaI2hpZBgwA
   osW8qBA2Y+4Z/IhW+RSA5d2fOwdo9KmXe1S8y8Tr/XRuFAs84aKNDaVSRUzMiDA6
   NSI6wpjg59NY6/yFljFZK0L2/WylKaDw/04R9i2lCx8V1vSfLYVWE58SNy+ZOo28
   sZ3KEHO6bxSre0t7xBJLMZxVchXaELcNxAgHlN42+OGgglWozfm37s1KpdcJfh6t
   RISwdH5nZZosP5bvydJjN5ZPPIqqT/Bsp+KWO1gaYiU+5fN312U4sZ0+ESKYjZxu

keine

WaZUZ2niKBuZZ1iVDjomYfZk+xsk7NyKaFQGIcJtpFixYrfGYxrj87SOXqHzKlzr
KpkFeR7g3rszAUCoP5el+Zu1G4Vu5lSiKZAK0NM76U0ygWsBsA/zP1ofxKaDya2U
RUCd/L7BNmsvDkznrrE4xmXtt97aIRAlSC/rrmXrYOPmOJJevSq59UBp7+MqS/+9
WPP65I78dae1QIQvgg1MCsWK0PzTeV0X4Wa/ZuUvnhDReJFiQWlWhqB/hrUp916W
iEwEExECAAwFAlgbCMwFgwll/hQACgkQW7P1GVgWeRrIgwCffyU0+K5AczcDfNDQ
BfakjQ/tEK8AoKOIvS9r3Hav4vPc99DZW1fnjGyviQGzBBABCAAdFiEElKXJoDwv
5co7CV2OH99yPPRitrEFAlgbDusACgkQH99yPPRitrF4Fwv/ViLY+1wsaRXXYfda
itA53WgDow2sP3Gz1BD3IxTdFqHVoDxUXRhT9+dNDdtgxm06dy2FL3C2TVHEPRzV
jdqvC/NGibUEdcdHzvtNUKarUd4/rYPGBlV2wBmrF+S7lB8QhBWYgCdNxiMr47JV
iHf9/B5bFdKEzPIJ+ssm9tTaXnQvU97zH3HBuChHLDOSLN9We5IYGijlEe1yOJ7I
pazhi2CENWUSJ1UG04FHuhKFCuVByqEbAHA/8fnScM9IzVh80kifwK3fdKaHml4g
9jev5gXoV5JXMVORKFFIvVORB3bGCgW95Tob2mtJQYtT4Jk0LTcyrtpUjsTl1xJ8
l00e4U/GPrwAngP3jXGSzAqb69oI+tQNRMsF3ImpPB/Tqf+e++XlyLPKJxN2TWeD
zV2ppxDfre3ua/qTIxtou9p9axMFdMHoY2ac4rXNoBIg9LxQpPAu9BeC3VIVORDg
aacxrD0HyvQKJtdFWw6Sh0CmZc2TkSV4FxHwUznZakPcXRAq
=XiRR
-----END PGP PUBLIC KEY BLOCK-----

keine

ANNEX B

EINSTUFUNGSLISTE

für
Gpg4 VS-NfD (Gpg4win und Gpg4KDE), Version3.X

Zulassungs-ID BSI-VSA-10187

		VS-EINSTUFUNG		Kenn-zeichnung	Keine Einstufung oder Kennzeichnung	HINWEIS
		VS-VERTRAU-LICH	**VS-NfD**	**CCI**	**OFFEN**	
1	Gpg4 VS-NfD SW-Installationsmedium				X	1)
2	Nutzer Smartcard				X	2) 4)
3	Gpg4 VS-NfD, installiert, betriebsbereit		X			
4	Gpg4 VS-NfD, ausgeschalteter Zustand, Schlüssel geladen		X			3) 5)
5	Gpg4 VS-NfD, 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) Gpg4 VS-NfD und Chipkarten sind separate zu lagern und zu transportieren.

Abkürzungen Einstufungen/Kennzeichnungen :
VS-NfD (VS-NUR FÜR DEN DIENSTBEGRAUCH)