GRP: Zulassungsstelle BSI

Digital unterschrieben von GRP: Zulassungsstelle BSI
Datum: 2019.12.03 11:01:14 +01'00'

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Einschreiben mit Rückschein
g10 code GmbH
Hüttenstr. 61
40699 Erkrath
Deutschland

[redacted]

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

POSTANSCHRIFT
Postfach 20 03 63, 53133 Bonn

TEL +49 (0) 228 99 9582[redacted]
FAX +49 (0) 228 99 10 9582[redacted]

Referat-KM12@bsi.bund.de
https://www.bsi.bund.de

Betreff: Freigabeempfehlung Gpg4 VS-NfD, Version 3.x Gpg4win und Gpg4KDE
BSI-VSA-10412

Bezug: Antrag auf Erteilung einer Freigabeempfehlung
Az.: KM12-730-00-08/324
Datum: 15.11.2019
Anlage: Report und SecOps zu Verfahren BSI-VSA-10412

Information über die Freigabeempfehlung BSI-VSA-10412

Hiermit teilen wir Ihnen mit, dass für das Produkt Gpg4 VS-NfD, Version 3.x der g10 code GmbH mit Datum vom 15.11.2019 die Freigabeempfehlung BSI-VSA-10412 erteilt wurde. Die Freigabeempfehlung ermöglicht die Verarbeitung und Übertragung von eingestuften Informationen bis einschließlich zum Geheimhaltungsgrad VS - NUR FÜR DEN DIENSTGEBRAUCH unter den in den zugehörigen Anlagen aufgeführten Bedingungen. Zur Definition von VS - NUR FÜR DEN DIENSTGEBRAUCH siehe §4 Abs. 2 Nr. 4 SÜG (§2 Abs. 2 Nr. 4 VSA).

Die Freigabeempfehlung ist befristet bis 31.08.2020.

Bundesamt
für Sicherheit in der
Informationstechnik

Das BSI übernimmt keine Gewährleistung für das Produkt.

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

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Abteilungsleiter

Bundesamt
für Sicherheit in der
Informationstechnik

Einsatz- und Betriebsbedingungen Gpg4 VS-NfD 3.x

BSI-VSA-10412

Stand: 15.11.2019

Geeignet zum Schutz von: VS - NUR FÜR DEN DIENSTGEBRAUCH

Nationale Version

Änderungshistorie

Version	Datum	Geändert von	Bemerkungen / Gründe für Änderung
V 1.0	15.11.2019	BSI	Finale 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

Inhaltsverzeichnis

Leere Seite

Annexe

ANNEX A – ZULASSUNG UND KONSTRUKTIONSSTAND

ANNEX B – EINSTUFUNGSLISTE

ANNEX C – entfällt

ANNEX D – entfällt

ANNEX E – entfällt

ANNEX F – entfällt

ANNEX G – entfällt

ANNEX H – entfällt

Abbildungsverzeichnis

Tabellenverzeichnis

Leere Seite

EINSATZ- UND BETRIEBSBEDINGUNGEN FÜR

Gpg4 VS-NfD, Version 3.x

VORWORT

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

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

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

Die Beachtung und Umsetzung dieses Dokumentes 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, 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 dieser Richtlinie 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

Diese Einsatz- und Betriebsbedingungen betreffen eine **Freigabeempfehlung** zur Nutzung von Gpg4 VS-NfD für Verschlusssachen bis zu einem VS-Einstufungsgrad von maximal VS-NUR FÜR DEN DIENSTGEBRAUCH (VD-NfD), RESTREINT UE/EU RESTRICTED und NATO RESTRICTED. Diese Freigabeempfehlung ergänzt die Einsatz- und Betriebsbedingungen für die Zulassung von Gpg4 VS-NfD für VS-NfD und beschreiben abgeschwächte Voraussetzungen, unter denen Gpg4 VS-NfD genutzt werden kann.

Gpg4 VS-NfD 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 Einstufungsgraden 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 (falls vorhanden) 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.

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 produktspezifischer Dokumentation.

1.2 Verwendung

Diese Einsatz- und Betriebsbedingungen gelten national für alle Anwendungen, in denen Gpg4 VS-NfD zum Schutz von nationaler, EU- oder NATO-VS zum Einsatz kommt. Sie sollten allen, die für die Installation und Kontrolle sowie für den Versand und 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 besondere Bedingungen, auf die im Weiteren (Kapitel 5.3.2) 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		
	National	
	[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
	EU Security Policy	
	[2013/488/EU]	Council Decision of 23 September 2013 on the Council Security Rules
	[2001/844/EC]	Commission Decision of 29 November 2001 amending its internal Rules of Procedure (Commissions Provisions on Security)
	[2013/C 190/01]	EEAS Decision of the HR on the Security Rules for the European External Action Service
	NATO Security Policy	
	[C-M(2002)49]	NATO Security Policy (NU)
Vorschriften mit kryptographischem Bezug		
	National	
	[BSI-TL 03426]	BSI - Technische Leitlinie -Vernichtung/Entsorgung von Kryptomittel (Mai 2015)
	[Merkblatt]	Merkblatt zur Handhabung der BSI-Manipulationserkennungsplakette (BSI-MEP), 01. Dezember 2017, VS-NfD
	EU	
	[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
	NATO	
	[SDIP-293]	Instructions for the Control and Safeguarding of NATO Cryptomaterial (NR)
	[AC/322-D/0047]	AC/322-D/0047-REV2 – INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, NATO RESTRICTED
Sonstige Referenzen		
	Zulassungen/Freigabeempfehlungen	
	[Zulassung-National]	Nationale Zulassung für den Schutz von VS - NUR FÜR DEN DIENSTGEBRAUCH: BSI-VSA-10412, vom 15.11.2019, 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

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
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
GHB	Geheimschutzhandbuch
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.
MEP	Manipulationserkennungsplakette (Klebeetikett, mit dem Gerätegehäuse gegen Manipulation gesichert werden können. Manipulation können erkannt werden.)
NCSA	National CIS Security Authority (in Deutschland das BSI)
SAA	Security Accreditation Authority
SecOPs	Security Operating Procedures (Einsatz und Betriebsbedingungen)
SoM	Strength of Mechanism
TEMPEST	Akronym für den Begriff „Abstrahlsicherheit“
TOE	Target of Evaluation, engl. Bezeichnung für EVG
VS	Verschlusssache(n)
VS-NfD	VS-NUR FÜR DEN DIENSTGEBRAUCH
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
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:

- **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:
  - 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;
  - 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);
  - Ermittlungen 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

2 Zur Vereinfachung und leichteren Lesbarkeit wird im gesamten Text für die einzelnen Parteien und Instanzen nur die männliche Form verwendet, nichtsdestoweniger beziehen sich die Angaben auf Angehörige aller Geschlechter.

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 zugelassenen IT-Sicherheitsproduktes Gpg4 VS-NfD 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.
- **Geheimschutzbeauftragter**
  Nach § 8 [VSA] sorgt der Geheimschutzbeauftragte für die Umsetzung der Verschlusssachen-anweisung und berät die Dienststellenleitungen in allen Fragen des Geheimschutzes. Geheimschutzbeauftragte haben ein unmittelbares Vortragsrecht bei den Dienststellenleitungen. Geheimschutzbeauftragte sind bei allen geheimschutzrelevanten Maßnahmen zu beteiligen.
- **IT-Sicherheitsbeauftragter**
  IT-Sicherheitsbeauftragte unterstützen und beraten nach § 9 [VSA] die Geheimschutzbeauftragten in allen Fragen des Einsatzes von Informationstechnik zur Handhabung von Verschlusssachen (VS-IT).
- **Sicherheitsbevollmächtigter**
  Der Sicherheitsbevollmächtigte ist im Bereich der geheimschutzbetreuten Wirtschaft gemäß Kap. 3.1 des GHB das zentrale Sicherheitsorgan im Unternehmen. Die Geschäftsleitung überträgt ihm die Zuständigkeit für die Durchführung aller Geheimschutzmaßnahmen und bevollmächtigt ihn entsprechend.
- **Security Accreditation Authority (SAA)**
  Die SAA ist unter Beachtung nationaler oder EU-/NATO-Vorschriften für die Prüfung und Akkreditierung von IT-Systemen zuständig. Dies gilt nicht für nationale VS-IT-Systeme, die außerhalb der Bundeswehr betrieben werden; diese erfordern gemäß § 50 [VSA] vor der Inbetriebnahme die Freigabe durch die Dienststellenleitung, gemäß § 50 Abs 2 [VSA] ist hier ggfls. ein Votum des BSI einzuholen.
  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.

2 SYSTEMBESCHREIBUNG

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 (Gpg4win) und GNU/Linux (Gpg4KDE) eingesetzt werden.

Bei dem Produkt handelt es sich um eine Kryptobibliothek mit verschiedenen darauf aufbauenden Komponenten. Die für diese Freigabeempfehlung relevanten 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 den S/MIME-Standard mit X.509-Zertifikaten sowie den OpenPGP-Standard zum Austausch und zur Speicherung öffentlicher Schlüssel.

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

Mit dem Produkt Gpg4win/Gpg4KDE lassen sich S/MIME- oder 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 mithilfe eines Passworts ver- und entschlüsselt werden.

Die für diese Freigabeempfehlung relevanten 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 X.509 (S/MIME) und OpenPGP-Zertifikate; 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.

Das Produkt unterstützt sowohl den S/MIME-Standard und verwendet dabei X.509-Zertifikate als auch den OpenPGP-Standard mit OpenPGP-Zertifikaten zum Austausch und zur Speicherung öffentlicher Schlüssel. Es benötigt für den zugelassenen Betrieb nach §51 Abs. 1 VSA eine Smartcard zur Speicherung von Langzeitgeheimnissen, wie die geheimen Signatur- und Entschlüsselungsschlüssel. Diese Freigabeempfehlung sieht vor, dass Langzeitgeheimnisse auch auf der Festplatte des Nutzers gespeichert werden können. Hierzu sind allerdings zusätzliche Sicherheitsmaßnahmen zu ergreifen.3

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 in einem modifizierten CFB-Modus bei OpenPGP
- 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 Gpg4 VS-NfD sind ANNEX A zu entnehmen.

Vor einer Installation und Inbetriebnahme des Produktes hat sich Betreiber 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 VS-Grad vorliegt. Im anderen Falle ist der Betreiber des IT-Systems für die Freigabe für den Einsatz zuständig (für die entsprechenden Einstufungsgrade (national, EU, NATO) oder SoM Level).

Weitere Einzelheiten sind in ANNEX A beschrieben.

3 Siehe hierzu auch Kapitel 2.7, Ziffer 15

2.4 Kompatibilität, Interoperabilität, Konformität

Gpg4 VS-NfD ist kompatibel zu anderen zugelassenen oder für VS-NfD freigegebenen Produkte, die den S/MIME-Standard mit X.509-Zertifikaten oder den OpenPGP-Standard zum Austausch und zur Speicherung öffentlicher Schlüssel unterstützen.

Der Benutzer hat sich vor einer Kommunikation mit einem anderen Nutzer (z. B. telefonisch) von diesem bestätigen zu lassen, dass auch dieser ein zugelassenes oder freigegebenes Produkt nutzt. Insbesondere dürfen nur solche fremden Schlüsselzertifikate verwendet werden, die von zugelassenen oder freigegebenen Produkten erzeugt wurden und die technischen Anforderungen an VS-NfD-konforme Schlüssel erfüllen.

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 oder freigegebenen Betrieb von Gpg4 VS-NfD zu beachten sind, können dem Nutzerhandbuch Gpg4win-Kompendium entnommen werden.

Darüberhinausgehende 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 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 Gpg4 VS-NfD 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 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.

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

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

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

7. Empfangen von OpenPGP-ZertifikatenZertifikaten/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 Schlüsselserver, 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).

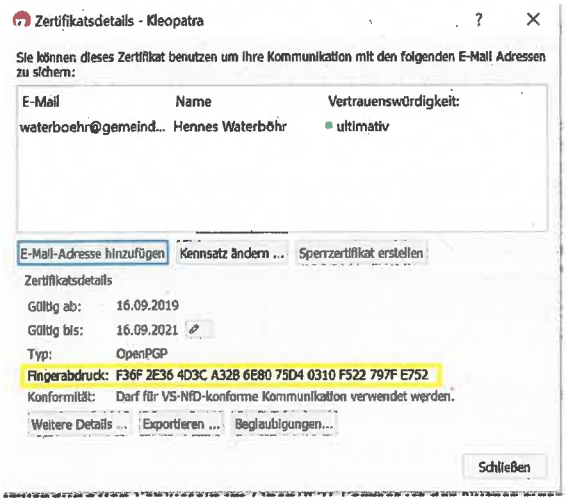

Abbildung 1: Zertifikatsdetails - Kleopatra

8. 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. (Hinweis: Es ist legitim das Passwort aufzuschreiben und vergleichbar sicher zu verwahren wie VS-NfD.)

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 telefonisch 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 ihn das erste Mal zum Verschlüsseln verwendet.

9. 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.

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

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

11. 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.

12. Automatisch signieren:

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

13. Vermeiden von HTML-Inhalten:

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

14. 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.

15. Für den freigegebenen Betrieb ist eine Verwendung ohne Smartcard möglich. Hierzu muss das System, auf dem privates Schlüsselmaterial für die VS-NfD-Kommunikation gespeichert und genutzt wird, für die Bearbeitung von VS-NfD-Daten freigegeben sein.

2.8 Abstrahlsicherheit

Es bestehen keine speziellen Anforderungen bzgl. der Abstrahlsicherheit an das System, auf dem Gpg4 VS-NfD betrieben wird, wenn Informationen, die VS - NUR FÜR DEN DIENSTGEBRAUCH, RESTREINT UE/EU RESTRICTED und/oder NATO 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 erforderlich.
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 erforderlich.

Diese Überprüfung und Bewertung ist durch das BSI zusammen mit dem Betreiber und ggfls. der SAA vorzunehmen. In Abhängigkeit von der Anwendung und dem Einsatzszenario sind vor einem Einsatz ggf. zusätzliche Maßnahmen zur Herstellung der Abstrahlsicherheit erforderlich.

3 SICHERHEITSMANAGEMENT

Nachfolgend werden besondere Anforderungen an das Sicherheitsmanagement bzw. Schlüsselmanagement von Gpg4 VS-NfD beschrieben.

3.1 Zuständigkeiten für Sicherheits-/Schlüsselmanagement

Der IT-Sicherheitsbeauftragte, der IT-System-Administrator und, soweit vorhanden der Kryptoverwalter, sind in ihrem Zuständigkeitsbereich verantwortlich für 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 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 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. Eine Weitergabe an andere Nationen oder Organisationen bedarf im Einzelfall einer schriftlichen Genehmigung des BSI.

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 [VSA], [BSI-TL 03426] und [Merkblatt] gemacht werden, sind falls zutreffend 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.

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 Schlüsselmaterials 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

6.4.1 Vernichten/Löschen von Schlüsseln/Zertifikaten

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

6.4.2 Produktentsorgung und -vernichtung

Bzgl. der Entsorgung und Vernichtung von Gpg4 VS-NfD bestehen keine besonderen Anforderungen.

7 PERSONELLE SICHERHEIT

Zusätzlich zu den Maßnahmen und Kriterien, die in den Referenzen [SÜG], [VSA], [2013/488/EU], [2001/844/EC], [2013/C 190/01], [IASG 2-03] und [C-M(2002)49], [SDIP-293] 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, Sicherheitsbevollmächtigten und dem IT-Sicherheitsbeauftragten zu beachten und umzusetzen.

7.2 Ermächtigung und Autorisierung

VS 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 V zur Verschlusssachenanweisung [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)

Der Zugang zu Gpg4 VS-NfD 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 Gpg4 VS-NfD zu beachten. In der Regel sind der Betreiber (ggf. unterstützet durch den Kryptoverwalter, den IT-Sicherheitsbeauftragte, 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 (ggf. unterstützet durch den Kryptoverwalter, den IT-Sicherheitsbeauftragte, den Systemadministrator) und der Nutzer in ihrem jeweiligen Verantwortungsbereich zuständig für die Umsetzung und Einhaltung der nachfolgend aufgeführten Maßnahmen.

9.2 Notfallplan

Der Schutz von Gpg4 VS-NfD und zugehörigem Schlüsselmittel 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.

9.3 Notlöschung

Dieser Punkt ist für Gpg4 VS-NfD nicht anwendbar.

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.

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, sicherheitsrelevanten Produktupdates sowie Aktualisierungen dieser Zulassung kontaktieren.

10.2 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.

10.3 Maßnahmen nach entdeckter Kompromittierung

Das kompromittierte System darf nicht weiter betrieben werden.

Der Geheimschutzbeauftragte und die zuständige Stelle für das Schlüsselmaterial bzw. das Sicherheitsmanagement von Gpg4 VS-NfD (z.B. Kryptoverwalter) sind unverzüglich über eine Verletzung der Kommunikationssicherheit zu informieren.

11 KONTAKTE

11.1 Hersteller

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

Intevation GmbH
Neuer Graben 17
49074 Osnabrück
Deutschland
https://intevation.de
E-Mail: intevation@intevation.de

Anfragen und Support: vsnfd@gpg4win.org

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

von
Gpg4 VS-NfD, 3.X

Zulassungs-ID BSI-VSA-10412

1 Zulassung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für Gpg4 VS-NfD, 3.X mit der Zulassungs-ID BSI-VSA-10412 mit Stand 15.11.2019 eine Freigabeempfehlung ausgestellt 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 2.6, 3 und 5) sind einzuhalten.

Nachfolgend ist der aktuell zugelassene Konstruktionsstand von Gpg4 VS-NfD 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 Gpg4 VS-NfD mit dem korrekten, zugelassenen Konstruktionsstand 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 Gpg4 VS-NfD 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 3.1.10 und folgende

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

1. Gpg4win 3.1.10 (gpg4win-3.1.10.exe)
   SHA256: 7f3ceaf54bcff0f63716900f6769b93597aae33e188e88792aa484a93d056dc9
2. 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
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-----

ANNEX B

EINSTUFUNGSLISTE

für
Gpg4 VS-NfD (Gpg4win und Gpg4KDE), Version 3.x

Zulassungs-ID BSI-VSA-10412

		VS-EINSTUFUNG[1]		OFFEN[1]	
		VS-VERTRAULICH	VS-NfD		
1	Gpg4 VS-NfD SW-Installationsmedium			X	1)
2	Gpg4 VS-NfD, installiert, betriebsbereit		X		
3	Gpg4 VS-NfD, ausgeschalteter Zustand, Schlüssel geladen		X		2)
4	Gpg4 VS-NfD, ausgeschalteter Zustand, Schlüssel gelöscht		X		2)

1) Das Installationsmedium ist nicht eingestuft, jedoch bezüglich seiner Integrität zu schützen.

2) Eine personenbezogene Nachweisführung ist nicht erforderlich.

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

1 Kryptomittel gem. §59, Abs. 2 VSA verfügen bei vorliegender Einstufung über den Warnvermerk „CRYPTO" bzw. „KRYPTO" oder bei nicht vorliegender Einstufung den Warnvermerk „CCI". Kryptomittel sind gem. Abschnitt IX, VSA insbesondere mittels Kryptoverwalter zu handhaben.