Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Ablösung von Chiasmus

Vorstellung von Alternativprodukten und Hinweise zur Migration

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.2	27.07.2021	Veröffentlicht
1.3	28.10.2021	Ergänzungen
1.4	25.05.2022	Aktualisierung
1.4.5	29.08.2022	Aktualisierung
1.5	25.01.2023	Aktualisierung Kontakt D-Trust

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
D-53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: zulassung@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Ausgangslage

Chiasmus ist ein Programm für die Verschlüsselung von Dateien, das 2001 im BSI für das Betriebssystem Microsoft Windows und etwas später auch als Kommandozeilentool für Linux entwickelt wurde. Ursprünglich wurde das Programm für Ad-hoc-Anwendungen im öffentlichen Bereich konzipiert, um damit auf vergleichsweise einfache Weise sensible Daten gesichert über unsichere Kanäle, wie etwa E-Mail, zu übertragen. Das Programm ist bewusst schlicht gehalten. Es besteht aus einer einzigen ausführbaren Datei (chiasmus.exe), die komprimiert auf einer einzigen 3-1/2-Zoll-Diskette Platz fand. Aus haushaltsrechtlichen Gründen durfte Chiasmus nur dort eingesetzt werden, wo ein öffentliches Interesse bestand, also zum Beispiel, wenn es zur Erfüllung eines öffentlichen Auftrags notwendig ist, sensible Daten sicher auszutauschen. In der Funktionalität ist Chiasmus sehr begrenzt, was bei einigen Nutzern den Wunsch nach einem Alternativprodukt aufkommen ließ, welches mehr Möglichkeiten bietet und einfach zu bedienen ist. Um beispielsweise ein Dokument sicher mit einer E-Mail zu versenden, musste dieses in einem gesonderten Schritt mit Chiasmus verschlüsselt werden. Der dazu benutzte Schlüssel musste vorab mit den Kommunikationspartnern vertraulich ausgetauscht worden sein. Schließlich konnte die damit verschlüsselte Datei an die E-Mail angehängt und versendet werden. Insbesondere ließ sich Chiasmus nicht automatisiert in andere Anwendungen, wie etwa einen E-Mail-Client, einbinden. Auch wurden keine asymmetrischen Verfahren angeboten und keine PKI unterstützt. Dennoch fand Chiasmus im nationalen und internationalen Umfeld eine breite Verwendung. Ein Grund dafür ist, dass für lange Zeit Chiasmus das einzige für Verschlusssachen mit dem Geheimhaltungsgrad VS-NfD zugelassene Softwareprodukt war. Damit war es auch möglich, Dokumente auszutauschen, die NATO RESTRICTED oder RESTREINT UE/EU RESTRICTED klassifiziert sind.

Die in Chiasmus verwendeten Algorithmen und Standards sind nicht offen, und die Software steht unter einer proprietären Lizenz. Dies hat Auswirkungen auf die Ablösung von Chiasmus durch andere Produkte, da das bei Chiasmus eingesetzte Schlüsselmaterial nicht kompatibel zu anderen Produkten ist.

Für VS-NfD sind zugelassene bzw. freigegebene Alternativprodukte für Chiasmus erhältlich, die mehr Funktionen bieten. Am 30.06.2022 wurde Chiasmus in den Ruhestand geschickt, was heißt, dass die Zulassung für VS-NfD entzogen wurde. Der Vertrieb und Support für das Programm sind mittlerweile eingestellt. Da Chiasmus nicht weiterentwickelt wird, ist zudem bei zukünftigen Betriebssystemversionen nicht auszuschließen, dass die Ausführung von Chiasmus und somit die Entschlüsselung von mit Chiasmus verschlüsselten Dateien in Zukunft ggf. nicht mehr möglich ist. Wie in Abschnitt 5.6 beschrieben, müssen archivierte Dateien in einer VS-NfD zugelassenen Umgebung entschlüsselt werden. Anschließend können sie in einer solchen Umgebung entschlüsselt gespeichert oder nach erneuter Verschlüsselung mit einem der Ablöseprodukt auf einem Datenträger gespeichert werden, der nicht VS-NfD-konform sein muss.

In diesem Dokument werden die verfügbaren Alternativprodukte kurz vorgestellt, und es wird erläutert, wie Prozesse, die mit Chiasmus durchgeführt wurden, mit den Alternativprodukten bewerkstelligt werden können.

2 Alternativprodukte

Derzeit sind zwei für VS-NfD zugelassenen Produkte auf dem Markt erhältlich - „GnuPG VS-Desktop“ der Firma g10 Code und „GreenShield“ der Firma cryptovision. Beide Produkte können Dateien mit einem symmetrischen Schlüssel, der aus einem Passwort abgeleitet wird, ver- und entschlüsseln. Diese symmetrischen Verfahren entsprechen der Funktionsweise von Chiasmus, sind aber nicht mit dem in Chiasmus implementierten Verfahren interoperabel, so dass mit Chiasmus verschlüsselte Dateien mit den Ablöseprodukten nicht entschlüsselt werden können und umgekehrt.

Außerdem können mit beiden Produkten sowohl E-Mails als auch Dateien asymmetrisch (hybrid) ver- und entschlüsselt sowie signiert werden.

Die asymmetrische Verschlüsselung von Dateien und E-Mails bietet gegenüber der symmetrischen Verschlüsselung einige Vorteile, die beim jeweiligen Anwendungsfall (s. Kapitel 5) entsprechend berücksichtigt werden können. So entfällt z.B. die vergleichsweise aufwändige Verteilung symmetrischer Schlüssel. Stattdessen kann der öffentliche Teil des Schlüssels des asymmetrischen Verfahrens einfach verteilt werden. Die Erneuerung von Zertifikaten ist mit dem OpenPGP-Standard weniger aufwendig. Zudem gewährleistet asymmetrische Verschlüsselung durch das Signieren von Dateien und E-Mails deren Integrität und Authentizität. Weitere Details zu Zertifikaten können Kapitel 3 entnommen werden.

2.1 *GnuPG VS-Desktop* vom Hersteller *g10 code GmbH*

Bei GnuPG VS-Desktop (vormals als Gpg4VS-NfD bezeichnet) handelt es sich um eine Software-Paketierung der Verschlüsselungssoftware GnuPG. Bei der asymmetrischen (hybriden) Ver- und Entschlüsselung von Dateien und E-Mails unterstützt GnuPG VS-Desktop sowohl den S/MIME- als auch den OpenPGP-Standard, die beide asymmetrische Public-Key-Verschlüsselungsverfahren sind. Die ebenfalls mögliche symmetrische Ver- und Entschlüsselung von Dateien wird grundsätzlich mit dem OpenPGP-Standard durchgeführt. Darüber hinaus können mittels S/MIME-Standard symmetrisch verschlüsselte Dateien mit nuPG VS-Desktop entschlüsselt werden (siehe Kapitel 4).

GnuPG VS Desktop kann in zwei verschiedenen VS-NfD-konformen Betriebsarten genutzt werden: die Zulassung BSI-VSA-10573 setzt den Einsatz einer Smartcard zur Speicherung des privaten Schlüsselmaterials voraus, die Regelungen der Freigabeempfehlung BSI-VSA-10584 ermöglichen den Betrieb ohne Smartcard. Das private Schlüsselmaterial wird in diesem Fall als so genanntes Softtoken in einem geschützten Bereich auf dem Arbeitsplatzrechner abgespeichert.

GnuPG VS-Desktop wird derzeit für folgende Betriebssysteme angeboten:

- Für Microsoft Windows
  Weiterführende Informationen unter: https://gnupg.com/gnupg-desktop.de.html
- Für Linux (unter dem Namen Gpg4KDE)
  Weiterführende Informationen unter: https://www.gpg4kde.de/

GnuPG VS-Desktop kann beim Hersteller oder über einen Rahmenvertrag im Kaufhaus des Bundes (KdB) bezogen werden. Der Preis richtet sich nach dem Lizenzvolumen. Es können zudem Dienstleistungen wie Support und Consulting beim Hersteller eingekauft werden.

Kontaktdaten des Herstellers g10code GmbH:

Telefon:	+49 2104 4938797
E-Mail:	info@gnupg.com
Internet:	gnupg.com/index.de.html
KdB-Rahmenvertrag:	21061

GnuPG VS-Desktop ist Open Source Software und steht unter der GNU GPL sowie anderen Open-Source-Software-Lizenzen.

2.2 *GreenShield* vom Hersteller *cv cryptovision GmbH*

Ebenso wie GnuPG VS-Desktop unterstützt GreenShield von cryptovision bei der asymmetrischen (hybriden) Ver- und Entschlüsselung von Dateien und E-Mails sowohl den S/MIME- als auch den OpenPGP-Standard, die beide asymmetrische Public-Key-Verschlüsselungsverfahren sind. Die ebenfalls mögliche symmetrische Ver- und Entschlüsselung von Dateien kann mit Hilfe beider Standards durchgeführt werden (voreingestellt ist S/MIME).

GreenShield 1.3 kann in zwei verschiedenen VS-NfD-konformen Betriebsarten genutzt werden: die Zulassung BSI-VSA-10602 setzt den Einsatz einer Smartcard zur Speicherung des privaten Schlüsselmaterials voraus. Die Regelungen der Freigabeempfehlung BSI-VSA-10632 ermöglichen den Betrieb ohne Smartcard. Das private Schlüsselmaterial wird in diesem Fall als so genanntes Softtoken in einem geschützten Bereich auf dem Arbeitsplatzrechner abgespeichert. GreenShield ist für folgendes Betriebssystem erhältlich:

- Microsoft Windows
- Linux, Ubuntu (nur Dateiverschlüsselung)

Das Programm kann direkt beim Hersteller oder über einen Rahmenvertrag im Kaufhaus des Bundes bezogen werden. Der Preis richtet sich nach der verwendeten Version (Datei- und/oder E-Mail-Verschlüsselung) und dem Lizenzvolumen. Es können zudem Dienstleistungen, wie Support und Consulting beim Hersteller eingekauft werden. Für die Vorgängerversion 1.2 von GreenShield gilt nach wie vor die Zulassung (BSI-VSA 10552). Da diese Version den OpenPGP-Standard nicht unterstützt und nur mit einer SmartCard betrieben werden darf, wird die Version 1.2 im Folgenden nicht betrachtet.

Kontaktdaten des Herstellers cryptovision GmbH:

Telefon:	+49 209 1672450
E-Mail:	info@cryptovision.de
Internet:	www.cryptovision.com/produkte/sichere-verschluesselung/GreenShield/
KdB-Rahmenvertrag:	21230

GreenShield steht unter einer proprietären Lizenz.

2.3 Zusammenfassung der Funktionalitäten der Alternativprodukte

Die durch die in den Abschnitten 2.1 und 2.2 vorgestellten Produkte abgedeckten Anwendungsfälle sind in der nachfolgenden Tabelle zusammengefasst.

Funktionalität	*GnuPG VS-Desktop Version 3.x (BSI-VSA-10584) Freigabe-empfehlung*	*GnuPG VS-Desktop Version 3.x (BSI-VSA-10573) zugelassen*	*GreenShield Version 1.3 (BSI-VSA-10632) Freigabe-empfehlung*	*GreenShield Version 1.3 (BSI-VSA-10602) zugelassen*
E-Mail Ver- und Entschlüsselung mit Smartcard S/MIME (X.509)	✓	✓	✓	✓
E-Mail Ver- und Entschlüsselung mit Smartcard OpenPGP	✓	✓	✓	✓
Ver- und Entschlüsselung von Dateien zertifikatsbasiert S/MIME mit Smartcard (asymmetrisch)	✓	✓	✓	✓
Ver- und Entschlüsselung von Dateien zertifikatsbasiert OpenPGP mit Smartcard (asymmetrisch)	✓	✓	✓	✓
E-Mail Ver- und Entschlüsselung mit Softtoken S/MIME (X.509)	✓	-	✓	-
E-Mail Ver- und Entschlüsselung mit Softtoken OpenPGP	✓	-	✓	-
Ver- und Entschlüsselung von Dateien zertifikatsbasiert S/MIME mit Softtoken (asymmetrisch)	✓	-	✓	-
Ver- und Entschlüsselung von Dateien zertifikatsbasiert OpenPGP mit Softtoken (asymmetrisch)	✓	-	✓	-

Funktionalität	*GnuPG VS-Desktop Version 3.x (BSI-VSA-10584) Freigabe-empfehlung*	*GnuPG VS-Desktop Version 3.x (BSI-VSA-10573) zugelassen*	*GreenShield Version 1.3 (BSI-VSA-10632) Freigabe-empfehlung*	*GreenShield Version 1.3 (BSI-VSA-10602) zugelassen*
Ver- und Entschlüsselung von Dateien mit Passphrase OpenPGP (symmetrisch)	✓	✓	✓	✓
Verschlüsselung von Dateien mit Passphrase S/MIME (symmetrisch)	-	-	✓	✓
Entschlüsselung von Dateien mit Passphrase S/MIME (symmetrisch)	✓	✓	✓	✓
Gleichzeitige Ver- und Entschlüsselung von mehreren Dateien und Ordnern, auch rekursiv	✓	✓	✓	✓
Verschlüsselte Entwürfe E-Mail S/MIME	✓	✓	✓	✓
Verschlüsselte Entwürfe E-Mail OpenPGP	✓	✓	✓	✓
Unterstützung Kommandozeile / Eingabeaufforderung	✓	✓	✓	✓
Script gesteuert / API Schnittstelle - E-Mail	✓	✓	✓	✓
Script gesteuert / API Schnittstelle - Dateiverschlüsselung (Chiasmus-Ablöse)	✓	✓	✓	✓
Windows	✓	✓	✓	✓
Linux	✓	✓	✓*	✓*

*Tabelle 2: Zusammenfassung der Funktionalitäten und Interoperabilität der Ablöseprodukte. Bedeutung: ✓ = unterstützt, - = nicht unterstützt (oder nicht von der Zulassung abgedeckt, * = nur Dateiverschlüsselung)*

3 Zertifikate

Um eine asymmetrische Verschlüsselung nutzen zu können, wird von jedem Nutzer ein eigenes Zertifikat bzw. Schlüsselpaar benötigt. Dieses besteht jeweils aus einem privaten und einem öffentlichen Teil. Während der öffentliche Teil jedem zugänglich gemacht werden kann, muss der private Teil geheim gehalten werden. Es kommen dabei die beiden Standards S/MIME (X.509 Zertifikate) und OpenPGP zum Einsatz, die aufgrund ihres unterschiedlichen Vertrauensmodells nicht miteinander kompatibel sind.

Bevor verschlüsselt zwischen Sender und Empfänger kommuniziert werden kann, müssen beide jeweils den öffentlichen Teil des Zertifikates/Schlüssels miteinander austauschen und importieren. Die möglichen Wege sind weiter unten beschrieben. Wird nun eine Nachricht an einen Kommunikationspartner gesendet, so wird mit dem öffentlichen Zertifikat/Schlüssel des Empfängers die Nachricht verschlüsselt. Damit wird die Vertraulichkeit gewährleistet. Mit dem privaten Teil des Zertifikates/Schlüssels des Senders wird die Nachricht signiert. Der Empfänger der Nachricht kann diese mit seinem privaten Zertifikat/Schlüssel wieder entschlüsseln. Und mit dem öffentlichen Zertifikat/Schlüssel des Senders kann er die Signatur überprüfen. Ist diese korrekt, so weiß der Empfänger, dass sowohl Authentizität des Senders als auch Integrität der Nachricht gewährleistet sind.

Damit ein System zur E-Mail und Dateiverschlüsselung für VS-NfD genutzt werden kann, ist es nicht unbedingt notwendig, dass alle privaten Schlüssel auf einem Hardware-Token (z. B. Smartcard) gespeichert werden. Der genaue Umfang der BSI-Anforderungen zur E-Mail und Dateiverschlüsselung findet sich in dem VS-Anforderungsprofil BSI-VSAP-0014. Die Evaluierung eines entsprechenden Produktes muss ergeben, dass die Anforderungen des BSI generell erfüllt sind.

Weitere Informationen zum Einsatz der zugelassenen Produkte gehen aus deren Security Operations (SecOps, vormals „Einsatz- und Betriebsbedingungen“) hervor. Diese Dokumente können dabei durchaus die Anforderungen enthalten, dass für den zugelassenen Betrieb des Produktes alle Schlüssel auf einem Hardware-Token zu speichern sind. Dies liegt dann aber an der Konstruktion des Produktes selbst sowie seiner Einsatzumgebung und nicht an den generellen Anforderungen des BSI, s. die entsprechenden SecOps und das VS-AP.

Wird zu einem Produkt eine Freigabeempfehlung des BSI ausgesprochen, so sind mit dem Einsatz eines solchen Produktes im Vergleich zu einem zugelassenen Produkt im Normalfall weitere Anforderungen, Vorgaben oder Risiken zu beachten, die bei der Freigabe der VS-IT durch die Dienststellenleitung gemäß §50 VSA zu beachten und zu berücksichtigen sind. Die für das jeweilige Produkt relevanten SecOps sind ebenfalls einzuhalten.

Für den VS-NfD zugelassenen Betrieb beider Produkte ist der private Teil des Zertifikates/Schlüssels auf einem Hardware-Token zu speichern (siehe Annex A der Einsatz- und Betriebsbedingungen (SecOps) des jeweiligen Produktes zu den erlaubten SmartCards).

Im Falle der Freigabeempfehlung kann der private Teil auch durch ein Passwort geschützt im Zertifikatmanager des Produktes innerhalb einer VS-NfD-konformen Umgebung gespeichert werden.

3.1 X.509-Zertifikate

Ein eigenes X.509-Zertifikat (privater und öffentlicher Teil) für mit S/MIME-abgesicherte Daten muss in der eigenen Organisation beantragt werden. Entsprechende Anleitungen zur Vorgehensweise sollten in der Organisation verfügbar sein. Der private Teil des Zertifikates wird seinem Besitzer auf einem Hardware-Token gespeichert ausgeliefert. Wird die jeweils freigegebene Variante genutzt, kann der private Teil des Zertifikates als Softtoken zum Import in den Zertifikatsspeicher ausgeliefert werden. Bei der Auslieferung ist auf eine ausreichende Absicherung des Softtokens zu achten. Der öffentliche Teil des Zertifikats wird automatisch an andere Nutzer über die Public-Key-Infrastructure (PKI) über verschiedene Schnittstellen (z. B. LDAP) zur Verfügung gestellt und ist automatisch durch die CA

authentisiert. Damit die Zertifikate für VS-NfD benutzt werden dürfen, müssen sie den Anforderungen aus den SecOps der Ablöseprodukte und der BSI TR-02102-1 entsprechen.

Anmerkung: Um Zertifikate aus einer anderen PKI als der eigenen VS-NfD-konform nutzen zu können, muss der Root-CA der fremden PKI durch die eigene Institution vertraut werden. Dies setzt voraus, dass die Anforderungen der TR-03145-1 und TR-03145-VS-NfD Secure CA Operation erfüllt sind. Wie die Dokumente bezogen werden können, ist in Kapitel 9 beschrieben.

Behörden erhalten ihre Zertifikate z. B. über kommerzielle Anbieter oder über eine eigene Sub-CA der V-PKI. Für Dienststellen der Bundesverwaltung können S/MIME-Zertifikate über die IVBB-CA, für Landesbehörden und Kommunen aus der DOI-CA bezogen werden. Ansprechpartner können im BSI (V-PKI) erfragt werden. Diese Institutionen können auch eine eigene PKI betreiben, die den Anforderungen der TR-03145-VS-NfD Secure CA Operation gerecht wird. Unternehmen der geheimschutzbetreuten Wirtschaft können beim BMWK nach geeigneten Betreiber einer CA (TR-03145-1, TR-03145-VS-NfD) nach X.509-Zertifikaten nachfragen. VS-NfD Zertifikate der V-PKI können bezogen werden bei den Unternehmen T-Systems und D-Trust.

Ansprechpartner:

T-Systems International GmbH

IT Security Engineering & Operations
Telekom Security
Trust Center Solutions 2 (TCS 2)
Querstraße 1
04103 Leipzig
Jens Ewe, E-Mail: jens.ewe@t-systems.com
Katrin Winkler, E-Mail: katrin.winkler@t-systems.com

D-Trust GmbH

Kommandantenstr. 15
10969 Berlin
E-Mail: vertrieb@d-trust.net

Der Preis und die Gültigkeitsdauer für ein X.509-Zertifikat sind bei den jeweiligen CAs zu erfragen.

3.2 OpenPGP Zertifikate

Ein eigenes OpenPGP-Zertifikat (privater und öffentlicher Teil) für mit dem OpenPGP-Standard abgesicherte Daten kann mithilfe der Ablöseprodukte erstellt oder ein vorhandenes Zertifikat importiert werden. Genaue Hinweise finden sich im Benutzerhandbuch der Produkte. Der öffentliche Teil des Zertifikats kann über verschiedene Wege verteilt werden, z. B.

- bei einem persönlichen Kontakt,
- als E-Mail-Anhang,
- als Veröffentlichung auf öffentlichen Key-Servern oder
- mittels Web Key Directory (WKD) / Web Key Service (WKS) (nur GnuPG VS-Desktop), s. https://wiki.gnupg.org/WKD.

Auf dem gleichen Weg kann das öffentliche Zertifikat des Kommunikationspartners bezogen und anschließend importiert werden. Der Betrieb einer PKI ist im OpenPGP-Standard nicht vorgesehen. Vor der Nutzung eines Zertifikates muss dieses daher auf seine Authentizität überprüft werden. Siehe hierzu etwa die Ausführungen in diesem Dokument zu Möglichkeit 3 in Use-Case 5.1.3.

Für OpenPGP-Zertifikate entstehen keine Kosten. Die Gültigkeitsdauer kann vom Nutzer selbst festgelegt werden und ist üblicherweise mit 2 Jahren voreingestellt. Die Gültigkeitsdauer kann vom

Benutzer selbst verlängert werden. Damit die Zertifikate für VS-NfD benutzt werden dürfen, müssen sie den Anforderungen aus den SecOps der Ablöseprodukte und der BSI TR-02102-1 entsprechen.

4 Grundsätzliche Arbeitsweise der Alternativprodukte

Auf Details zur Funktionsweise der in Kapitel 2 aufgeführten Ablöseprodukte kann in diesem Dokument nicht eingegangen werden. Hier wird auf die entsprechenden Handbücher der Hersteller verwiesen. Weiterhin sind vom Nutzer die Vorgaben in den Einsatz- und Betriebsbedingungen im Zulassungs-/Freigabeempfehlungsdokument der entsprechenden Produkte zu beachten bzw. umzusetzen. Diese sind direkt vom Hersteller oder über das Kaufhaus des Bundes erhältlich.

Sowohl GnuPG VS-Desktop als auch GreenShield lassen sich in einen E-Mail-Client einbinden, sodass E-Mails automatisiert verschlüsselt und signiert werden können. Es ist also nicht (wie bei Chiasmus) notwendig, Dateien separat zu verschlüsseln und der E-Mail als Anhang beizufügen. Zudem werden nicht nur die Anhänge, sondern die komplette E-Mail verschlüsselt.

GnuPG VS-Desktop wird von Microsoft Outlook unter Windows und Kmail unter Linux unterstützt. Hierbei ist das Plugin mit seiner GUI in die Oberfläche des E-Mail-Clients integriert. Verschlüsselte oder signierte Mails können sowohl im Vorschaufenster als auch in einem separaten Fenster dargestellt werden. Die Nutzung von GnuPG VS-Desktop GpgEX zur Bearbeitung von Dateien erfolgt mittels einer dedizierten GUI.

GreenShield wird sowohl von Microsoft Outlook und IBM/HCL Notes unter Windows unterstützt. Die Nutzung von GreenShield erfolgt dabei in einem separaten Fenster. Verschlüsselte oder signierte Mails können nur in einem separaten Fenster dargestellt werden. Die Nutzung von GreenShield File erfolgt mittels einer dedizierten GUI die auch Ubuntu 20.04 LTS unterstützt.

Eine Einbindung der Produkte in Web-Anwendungen ist nicht möglich.

5 Use-Cases

In diesem Abschnitt werden Anwendungsfälle (sog. Use-Cases) betrachtet, bei denen vertrauliche Daten ausgetauscht werden. Für jeden aufgeführten Use-Case wird im Folgenden beschrieben, wie er momentan mit Chiasmus gelöst wird und wie eine Lösung mit den in Abschnitt 2 aufgeführten Alternativprodukten aussehen kann.

Die in diesem Abschnitt aufgeführten Use-Cases beziehen sich hauptsächlich auf die GUI-Version von Chiasmus. Auf spezielle freigegebene Anwendungsfälle, die die Chiasmus-Kommandozeilenversion verwenden, wird in Use-Case 5.4 eingegangen.[1]

5.1 Kommunikation mit wenigen anderen Nutzern

5.1.1 Beschreibung

Ein Nutzer tauscht mit einer überschaubaren Menge anderer Nutzer sensible Dokumente aus. Es handelt sich dabei nur um einzelne Kommunikationspartner oder eine kleine, sich dynamisch verändernde Gruppe, so dass der Verteiler der Adressaten oft neu angepasst werden muss. Der Informationsaustausch zwischen den Nutzern erfüllt dabei das Prinzip „Kenntnis nur wenn nötig“.

5.1.2 Bisheriges Vorgehen mit Chiasmus

Jedes Paar von Kommunikationspartnern benötigt einen gemeinsamen individuellen Chiasmus-Schlüssel. Dieser Schlüssel muss vor der ersten Übermittlung sensibler Daten erzeugt und zwischen den Kommunikationspartnern auf vertraulichem Wege ausgetauscht werden. Laut Einsatz- und Betriebsbedingungen von Chiasmus sind für die VS-NfD-Kommunikation die Schlüssel auszutauschen

- bei einem persönlichen Kontakt,
- über eine mindestens VS-NfD zugelassene verschlüsselte Verbindung oder
- per Post, vornehmlich in einem versiegelten Umschlag oder als Wertbrief.

Der Schlüssel kann in Form einer Datei (Dateiendung .xis), ausgedruckt auf einem Blatt Papier oder mündlich als Zeichenkette weitergegeben/übermittelt werden. Eine vom Programm automatisch errechnete Checksumme erleichtert dem Nutzer die korrekte Eingabe, wenn der Schlüssel über die Tastatur eingegeben wird.

Eine mit Chiasmus verschlüsselte Datei kann dann einer E-Mail angehängt oder auf einem Datenträger dem Empfänger zugestellt werden. Kann diese beim Empfänger fehlerfrei entschlüsselt werden, kann der Empfänger üblicherweise davon ausgehen, dass die Datei tatsächlich von einem Besitzer des Schlüssels verschlüsselt und anschließend nicht verfälscht wurde.

5.1.3 Mögliches Vorgehen mit den Ablöseprodukten GnuPG VS-Desktop oder GreenShield

1. Da GnuPG VS-Desktop und GreenShield die Möglichkeit bieten, mithilfe eines aus einem Passwort abgeleiteten Schlüssels Dateien zu verschlüsseln, kann das mit Chiasmus praktizierte Verfahren prinzipiell beibehalten werden. Bei der eigenen Wahl eines Passworts ist bei beiden Alternativprodukten dieses wesentlich komplexer zu gestalten, als es bei anderen Anwendungen (etwa Zugangspasswort für eine Webanwendung oder PIN für eine Bankkarte) üblich ist. Der Grund dafür ist, dass es für einen Angreifer zum Entschlüsseln einer Datei keinen Fehlbedienungszähler gibt; von einem Angreifer können vielmehr beliebig viele Passwörter

[1] Sofern Sie Ihren Prozess nicht unter den aufgeführten Use-Cases wiederfinden oder weitere Fragen haben, wenden Sie sich bitte an chiasmus@bsi.bund.de

systematisch getestet werden, bis eine Entschlüsselung erfolgreich endet. In den Einsatz- und Betriebsbedingungen ist festgelegt, dass ein Passwort mindestens 20 bis 25 zufällig gewählte Zeichen enthalten soll.
Werden mit dem Passwort VS-NfD-Daten geschützt, ist das Passwort selbst VS-NfD einzustufen und entsprechend zu behandeln.

2. Sofern zwei Nutzer jeweils ein Zertifikat einer CA (X.509 Zertifikat) besitzen, kann der Sender der Daten das Zertifikat des Empfängers herunterladen und die Daten mit dem im Zertifikat enthaltenen Schlüssel verschlüsseln. Beide CAs müssen dabei derselben PKI oder aber PKIen angehören, die untereinander kompatibel (zertifiziert) sind. Die Suche und Verifikation des Empfängerzertifikats wird bei Nutzung eines E-Mail-Clients automatisiert unterstützt. Der Absender muss sich jedoch vergewissern, dass von der Software das korrekte Zertifikat ausgewählt wurde. Eine geeignete Konfiguration des Arbeitsplatzes kann diese Entscheidung automatisieren. Zudem soll der Absender die verschlüsselte Datei (bzw. E-Mail) mit einer digitalen Signatur versehen. Diese wird beim Empfänger (mithilfe des Zertifikats des Absenders) auf Gültigkeit überprüft. Auf diese Weise kann der Empfänger sicher sein, dass der vorgebliche Absender tatsächlich der Sender der verschlüsselten Daten ist und diese nicht manipuliert wurden.
   Auch eine manuelle Verifikation der Gültigkeit eines Zertifikats über LDAP und/oder OCSP und die Konfiguration zur Offline Nutzung und der Auswertung von CRLs ist möglich.
   GnuPG VS-Desktop und GreenShield bieten eine Anzeige der verwendeten Algorithmen und zeigen Warnhinweise, sofern diese nicht VS-NfD-konform sind.
3. Sender und Empfänger tauschen die öffentlichen Teile ihrer OpenPGP-Zertifikate aus, welche sie selbstständig erzeugt haben. Das Zertifikat (welches den für die Verschlüsselung bzw. die Signaturverifikation benötigten Schlüssel enthält) kann dabei über einen unsicheren Kanal (etwa via E-Mail) übermittelt werden.[2] Es ist jedoch erforderlich, dass sich Sender und Empfänger über die Echtheit der empfangenen Zertifikate vergewissern, etwa indem sie die Fingerprints der Zertifikate abgleichen. Dieser Abgleich kann mündlich in einem Telefonat geschehen, sofern sich Sender und Empfänger persönlich kennen.

Für die Punkte 2 und 3 wird eine zu versendende E-Mail oder Datei dann mit dem öffentlichen Teil des Zertifikats des Empfängers verschlüsselt und mit dem privaten Teil des Zertifikats des Senders digital signiert.

5.2 Kommunikation innerhalb einer großen Nutzergruppe

5.2.1 Beschreibung

Ein Nutzer tauscht mit einer potenziell großen Menge anderer Nutzer unregelmäßig Dokumente aus. Hierbei ist im Vorhinein nicht bekannt, wer genau die möglichen Kommunikationspartner des Nutzers sind, d. h. die Zusammensetzung und Größe einer solchen Gruppe können sich kurzfristig ändern. Der Informationsaustausch zwischen an der Kommunikation beteiligten Nutzern erfüllt dabei das Prinzip „Kenntnis nur wenn nötig“. Für den Fall, dass die Zusammensetzung und Größe der Gruppe sich nicht ändert und bekannt ist, treffen die Use-Cases 5.3 oder 5.4 zu.

5.2.2 Bisheriges Vorgehen mit Chiasmus

Für diesen Use-Case war Chiasmus nicht vorgesehen.

[2] Keinesfalls dürfen die zugehörigen privaten Schlüssel ausgetauscht werden

5.2.3 Mögliches Vorgehen mit den Ablöseprodukten

Es kann im Wesentlichen identisch wie bei den Vorgehensweisen 2 oder 3 im Use-Case 5.1 vorgegangen werden.

5.3 Verwendung eines Gruppenschlüssels

5.3.1 Beschreibung

Innerhalb einer Arbeitsgruppe oder eines Projekts werden Dokumente ausgetauscht. Die Zusammensetzung einer solchen Gruppe ist statisch, so dass der gruppeninterne Informationsaustausch über einen festen Verteiler von Adressaten abläuft. Alle Gruppenmitglieder entsprechen dabei dem Prinzip „Kenntnis nur wenn nötig“.

5.3.2 Bisheriges Vorgehen mit Chiasmus

Ein Mitarbeiter der Gruppe erstellt vorab einen Chiasmus-Schlüssel. Der Schlüssel wird wie unter 5.1.2 angegeben an die übrigen Gruppenmitglieder verteilt, z. B. während eines gemeinsamen Treffens der Gruppe. In der Folge können die Gruppenmitglieder mithilfe des Schlüssels Daten verschlüsseln und diese an einzelne oder alle anderen Mitglieder der Gruppe versenden, welche die Daten mit demselben Schlüssel wieder entschlüsseln können.

5.3.3 Mögliches Vorgehen mit den Ablöseprodukten

1. Da GnuPG VS-Desktop und GreenShield die Möglichkeit bieten, mithilfe eines Passwortes Dateien zu verschlüsseln, kann das mit Chiasmus praktizierte Verfahren prinzipiell beibehalten werden.
   Die in Möglichkeit 1 im Abschnitt 5.1.3 gemachten Anmerkungen sind auch hier zu beachten.
2. Ein Mitarbeiter der Gruppe erstellt einen nur für diese Gruppe bestimmten OpenPGP-Schlüssel. Dieser Gruppenschlüssel (d. h. die beiden Zertifikate, die den privaten und den öffentlichen Schlüssel enthalten) wird wie unter 5.1.2 angegeben an die übrigen Gruppenmitglieder verteilt, z. B. während eines gemeinsamen Treffens der Gruppe. In der Folge können die Gruppenmitglieder mithilfe des Gruppenschlüssels Daten verschlüsseln und signieren und diese an einzelne oder alle anderen Mitglieder der Gruppe versenden.
3. Alternativ kann bei der zugehörigen CA ein X.509-Gruppenzertifikat von dem für das Gruppenpostfach zuständigen Gruppenmitglied beantragt werden. Dieses verteilt dann auf sicherem Wege, wie unter 5.1.2 angegeben, das Zertifikat mit seinem privaten und öffentlichen Teil an die übrigen Gruppenmitglieder.

Anmerkung 1: Ein Gruppenschlüssel sollte regelmäßig gewechselt werden, insbesondere dann, wenn Mitglieder die Gruppe verlassen. Ein neuer Gruppenschlüssel darf nicht mit dem alten Gruppenschlüssel verschlüsselt und an die Mitglieder über einen nicht geschützten Weg versandt werden.

Anmerkung 2: Ein Gruppenschlüssel mit X.509-Zertifikaten ist weit aufwändiger zu verwalten als mit OpenPGP-Zertifikaten, insbesondere, wenn die Mitglieder der Gruppe häufig wechseln.

Anmerkung 3: Nachdem alle Mitglieder der Gruppe untereinander ihre öffentlichen OpenPGP oder S/MIME Zertifikate ausgetauscht haben bzw. diese Zertifikate allen Gruppenmitgliedern anderweitig zur Verfügung stehen, kann für diesen Use-Case die Kommunikation wie in den Möglichkeiten 2 und 3 unter dem Use-Case 5.1.3 beschrieben stattfinden. Die abgesicherten Nachrichten oder Dateien werden an den entsprechenden Verteiler geschickt.

5.4 Versendung von Dokumenten von einer Stelle an eine große Gruppe (skriptgesteuerte Verschlüsselung, Kommandozeile)

5.4.1 Beschreibung

Eine Stelle versendet an eine sehr große Gruppe von Nutzern regelmäßig Dokumente, z. B. einen nicht für die Allgemeinheit bestimmten Newsletter. Ein gegenseitiger Austausch zwischen der versendenden Stelle und der Gruppe ist in diesem Use-Case nicht primäres Ziel (vgl. Use-Case 5.2).

5.4.2 Bisheriges Vorgehen mit Chiasmus

Mithilfe der Kommandozeilenversion von Chiasmus werden skriptgesteuert mit einem vorab an die Empfänger versendeten Schlüssel (wie unter 5.1.2 angegeben) E-Mail-Anhänge verschlüsselt, E-Mails generiert und an eine Empfängerliste versendet. Die Empfänger können die E-Mail-Anhänge mithilfe der GUI-Version von Chiasmus entschlüsseln.

Anmerkung: Die Kommandozeilenversion von Chiasmus besaß keine allgemeine Zulassung für VS-NfD. Um sie für die Verarbeitung von VS-NfD zu nutzen bedurfte es einer speziellen Einzelzulassung.

5.4.3 Mögliches Vorgehen mit den Ablöseprodukten

1. Beide Produkte können ebenfalls skriptgesteuert betrieben werden. Der skriptgesteuerte Betrieb ist Bestandteil der Zulassung. Die Vorgaben und Anwendungen dazu sind den Einsatz- und Betriebsbedingungen der Zulassung zu entnehmen. Daher kann das mit Chiasmus praktizierte Verfahren prinzipiell beibehalten werden.
2. GnuPG VS-Desktop bietet mit der Software Kleopatra die Möglichkeit, Gruppen zu definieren. Den Gruppenmitgliedern können dabei ihre S/MIME- oder OpenPGP-Zertifikate zugeordnet werden. Innerhalb einer Gruppe werden beide Standards unterstützt. Dadurch können verschlüsselte E-Mails für eine große Verteilerliste ohne großen Aufwand versendet werden.

5.5 Verschlüsselung zum persönlichen Datenaustausch

5.5.1 Beschreibung

- Ein Nutzer tauscht mit sich selbst (auf einem anderen Rechner) Dokumente über einen unsicheren Kanal aus, etwa zwischen Home-Office und Büroarbeitsplatz.
- Ein Nutzer speichert zum Transport Daten auf einen Datenträger und befürchtet den eventuellen Verlust des Datenträgers und damit die Kompromittierung der Daten.

5.5.2 Bisheriges Vorgehen mit Chiasmus

Das Vorgehen ist analog zum Use-Case 5.1.2. Ein Austausch des Schlüssels mit anderen Nutzern entfällt hierbei.

5.5.3 Mögliches Vorgehen mit GnuPG VS-Desktop oder GreenShield

1. Da GnuPG VS-Desktop und GreenShield die Möglichkeit bieten, mithilfe eines Passwortes Dateien zu verschlüsseln, kann das mit Chiasmus praktizierte Verfahren prinzipiell beibehalten werden. Der Austausch des Schlüssels mit anderen Nutzern entfällt dabei. Selbstverständlich darf das zur Verschlüsselung verwendete Passwort nicht über denselben Kanal übertragen werden bzw. nicht auf denselben Datenträger gespeichert werden wie die zu schützenden Daten.
   Die in Möglichkeit 1 von Use-Case 5.1.3 gemachten Anmerkungen sind auch hier zu beachten.

2. Der Nutzer verwendet zur Verschlüsselung und Signaturbildung seinen eigenen S/MIME- oder OpenPGP-Schlüssel. Hierbei können im Anwendungsfall 5.1.3 mit den Möglichkeiten 2 und 3 auf Quell- und Zielrechner unterschiedliche oder dieselben Zertifikate genutzt werden.

5.6 Ablageverschlüsselung („Data at Rest“)

5.6.1 Beschreibung

Daten werden verschlüsselt auf einem Datenträger gespeichert, z. B. zur Archivierung.

5.6.2 Bisheriges Vorgehen mit Chiasmus

Mit Chiasmus können einzelne Dateien oder ganze Ordner (samt Unterordnern) mit einem einheitlichen Schlüssel verschlüsselt werden. Die verschlüsselten Daten können dann etwa auf einen externen Datenträger gespeichert werden. Während es für die verschlüsselten Daten keine Anforderungen bzgl. der Vertraulichkeit gibt (der Ablageort muss nicht NfD-geeignet sein), muss der verwendete Schlüssel vor Kenntnisnahme durch Unbefugte geschützt werden. Keinesfalls darf der Schlüssel gemeinsam mit den Daten gespeichert werden, auch nicht als passwortgeschützte Datei.

5.6.3 Mögliches Vorgehen mit GnuPG VS-Desktop oder GreenShield

1. Da GnuPG VS-Desktop und GreenShield die Möglichkeit bieten, mithilfe eines Passwortes Dateien oder ganze Ordner zu verschlüsseln, kann das mit Chiasmus praktizierte Verfahren prinzipiell beibehalten werden. Das Passwort ist anderen Nutzern, die auf die gespeicherten Daten Zugriff haben sollen, mitzuteilen. Selbstverständlich darf das zur Verschlüsselung verwendete Passwort nicht auf denselben Datenträger gespeichert werden wie die zu schützenden Daten.
   Die in Möglichkeit 1 von Use-Case 5.1.3 gemachten Anmerkungen sind auch hier zu beachten.
2. Es kann wie in 5.1.3 gemäß der Möglichkeiten 2 und 3 vorgegangen werden, wobei statt eines Passworts das eigene X.509- oder OpenPGP-Zertifikat zum Verschlüsseln und Signieren ausgewählt wird. Es können auch Zertifikate weiterer Nutzer ausgewählt werden, sofern diese für die Daten zugriffsberechtigt sein sollen.
3. Es kann wie im vorangegangenen Punkt 2 vorgegangen werden, nur, dass statt individuellen X.509- oder OpenPGP-Zertifikaten der zugriffsberechtigten Nutzer ein Gruppenzertifikat verwendet wird. (Vgl. 5.3.3, Möglichkeiten 2 und 3.)

5.6.4 Konvertierung von Chiasmus-verschlüsselten Ablagedaten

Vorhandene, mit Chiasmus verschlüsselte Dateien können nicht mit den Alternativprodukten entschlüsselt werden. Um solche Bestandsdateien (zum Beispiel in Archiven) für die Nutzung mit den alternativen Produkten um zu schlüsseln, kann nach folgenden Schritten vorgegangen werden.

1. Chiasmus-verschlüsselte Dateien in eine VS-NfD-geeignete Umgebung kopieren
2. Verschlüsselte Dateien mit Chiasmus entschlüsseln
3. Dateien mit dem Ablöseprodukt verschlüsseln
4. Verschlüsselte Dateien wieder auf den Ablageort kopieren (dieser muss nicht VS-NfD-geeignet sein)

Die Schritte 3 und 4 können entfallen, falls sich der Ablageort der Dateien schon in einer VS-NfD-geeigneten Umgebung befindet.

Anmerkung zu Schritt 2:

Um große Mengen Chiasmus-verschlüsselter Dateien zu entschlüsseln, kann mit der Windows-Version von Chiasmus ein Dateiordner ausgewählt und alle sich darin befindlichen Dateien in einem einzigen

Arbeitsschritt entschlüsselt werden. Voraussetzung dafür ist jedoch, dass die zu entschlüsselnden Dateien mit demselben Chiasmusschlüssel verschlüsselt sind.

Mit der Linux-Version von Chiasmus können nicht mehrere Dateien gleichzeitig in einem Arbeitsschritt entschlüsselt werden. Da es sich bei der Linux-Version um ein Kommandozeilentool handelt, kann es aber über ein Skript angesteuert werden und so automatisiert große Mengen von Dateien in einem einzigen Arbeitsschritt entschlüsseln. Hierfür empfiehlt es sich, den Passwortschutz der betreffenden Chiasmus-Schlüsseldatei zu entfernen, um nicht für jede Datei das Passwort eintippen zu müssen. Dies geschieht mit dem Befehl „**chiasmus –m p –s Datei.xis**“. Hierbei enthält Datei.xis den Chiasmus-Schlüssel dessen Passwort geändert werden soll. Sie werden dann aufgefordert, das alte und ein neues Passwort einzugeben. Beim neuen Passwort tippen sie die Entertaste (ohne zuvor ein Passwort einzugeben).

6 Kriterien zur Eignung der Ablöseprodukte

Um für den eigenen Einsatz bewerten zu können, welches der beiden Ablöseprodukte das geeignetere ist, sollten folgende Punkte berücksichtigt werden:

- Welche Standards und Funktionalitäten werden benötigt, um mit Partnern kommunikationsfähig zu bleiben?
- Welche Funktionalitäten werden bei internen Prozessen benötigt?
- Sind die Anforderungen gemäß der SecOps an den korrekten Einsatz des Produktes erfüllbar? Insbesondere die Voraussetzungen, die auch vom IT-Umfeld erfüllt werden müssen, damit die Produkte integriert und ausgerollt werden können.

7 Zu beachtende Punkte vor der Inbetriebnahme

Bevor die Produkte ausgerollt und in Betrieb genommen werden, sollte geklärt sein, dass bei Inbetriebnahme die benötigten Zertifikate den Nutzern zur Verfügung stehen. Die Beantragung und Verteilung der Zertifikate sollte mit ausreichend zeitlichem Vorlauf erfolgen, damit sie bei Inbetriebnahme importiert und genutzt werden können. Gegebenenfalls muss auch für den Anschluss an oder den Aufbau von einer PKI Sorge getragen werden. Falls benötigt, sind auch rechtzeitig Gruppenzertifikate zu erzeugen und zu verteilen sowie Skriptlösungen zu erstellen.

8 Weiterführende Dokumente

Download von der Seite www.bsi.bund.de/Zulassung:

Von dieser Seite können mit Zugangsdaten (dort nachzulesen, wie diese erhalten werden können) folgende Dokumente heruntergeladen werden:

- *BSI-VSA-10573* (SecOps Zulassung GnuPG VS-Desktop)
- *BSI-VSA-10584* (SecOps Freigabeempfehlung GnuPG VS-Desktop)
- *BSI-VSA-10602* (SecOps Zulassung GreenShield)
- *BSI-VSA-10632* (SecOps Freigabeempfehlung GreenShield)

Das Dokument *BSI-VSAP-0014-2018* (VS-Anforderungsprofil für sichere Übertragung von E-Mails und Dateien) kann per E-Mail angefordert werden. Details dazu sind unter obiger Web-Adresse verfügbar.

Die Technischen Richtlinien des BSI

- *BSI TR-02102-1* (Kryptographische Verfahren: Empfehlungen und Schlüssellängen)
- *TR-03145-1*
- *TR-03145-VS-NfD Secure CA Operation*

können entweder von der Seite www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/technische-richtlinien_node.html herunter geladen oder beim Referat KM 35 (referat-km35@bsi.bund.de) angefordert werden.

Benutzerhandbücher und weitere Dokumentationen der Ablöseprodukte können beim jeweiligen Hersteller nachgefragt werden.

9 Abkürzungen

API	Application Programming Interface
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CRL	Certificate Revocation List
DOI	Deutschland-Online-Infrastruktur (Bund-Länder-Kommunen-Verbindungsnetz, jetzt NdB-Verbindungsnetz)
GNU	ein freies, unixähnliches Betriebssystem
Gpg/GnuPG	GNU Privacy Guard
GPL	General Public License
GUI	Graphic User Interface
IMAP(S)	Internet Message Access Protocol (over TLS); Verfahren, mit einem Mailprogramm E-Mails von einem Mailserver abzurufen
iOS	ein von Apple entwickeltes mobiles Betriebssystem für das iPhone und den iPod touch
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
KdB	Kaufhaus des Bundes
KDE	ursprünglich: K Desktop Environment; Community, die sich der Entwicklung freier Software verschrieben hat
LDAP	Lightweight Directory Access Protocol
MAPI	Messaging Application Programming Interface
NdB	Netze des Bundes, ehemals IVBB (Informationsverbund Berlin-Bonn)
OCSP	Online Certificate Status Protocol
OpenPGP	Ein standardisiertes Datenformat für verschlüsselte und digital signierte Daten. Auch wird das Format eines Zertifikats festgelegt, welches den öffentlichen Schlüssel des Zertifikatsinhabers enthält. PGP steht für Pretty Good Privacy.
PC/SC	Personal Computer/Smart Card; ein Standard für Chipkartenleser
PIN	Persönliche (geheimzuhaltende) Identifikationsnummer

PKI	Public Key Infrastructure
SecOps	Security Operations; vormals „Einsatz- und Betriebsbedingungen“
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP(S)	Simple Mail Transfer Protocol (over TLS); ein Protokoll zum Austausch von E-Mails
TLS	Transport Layer Security
TR	Technische Richtlinie
V-PKI	Verwaltungs-PKI
VS	Verschlusssache
VSA	Verschlusssachenanweisung
VS-NfD	VS – Nur für den Dienstgebrauch
WKD/WKS	Web Key Directory / Web Key Service
X.509	Ein ITU-T-Standard für eine PKI zum Erstellen digitaler Zertifikate