Federal Office
for Information Security

Replacement of Chiasmus

Presentation of alternative products and hints for migration

Change history

Version	*Date*	*Name*	*Description*
1.3	29.10.2021		Published

Table 1: Change history

Federal Office for Information Security
PO Box 20 03 63
53133 Bonn
Phone:+49 22899 9582-0
Email: zulassung@bsi.bund.de
Internet: https://www.bsi.bund.de

Content

1 Current situation

Chiasmus is a program for encrypting files that was developed in 2001 at the BSI for the Microsoft Windows operating system and somewhat later as a command-line tool for Linux. Originally, the program was designed for ad hoc applications in the public sector in order to transfer sensitive data securely over insecure channels, such as e-mail, in a comparatively simple manner. The program is deliberately kept simple. It consists of a single executable file (chiasmus.exe) compressed to fit on a single 3-1/2 inch floppy disk. For budgetary reasons, Chiasmus may only be used where there is a public interest, such as when it is necessary to securely exchange sensitive data to fulfill a public contract. In terms of functionality, Chiasmus is very limited, which has led to a desire among some users for an alternative product that offers more options and is easy to use. For example, in order to send a document securely with an e-mail, it must be encrypted with Chiasmus in a separate step. The key used for this purpose must have been confidentially exchanged with the communication partners in advance. Finally, the encrypted file can be attached to the e-mail and sent. In particular, Chiasmus cannot be automatically integrated into other applications, such as an e-mail client. Also, no asymmetric methods are offered and no PKI is supported. Nevertheless, Chiasmus is widely used nowadays in national and international environments. One reason for this is that for a long time Chiasmus was the only software product approved for classified information with the classification level VS-NfD. Chiasmus makes it also possible to exchange documents classified NATO RESTRICTED or RESTREINT UE/EU RESTRICTED.

The algorithms and standards used in Chiasmus are not open and the software is under a proprietary license. This has implications for the replacement of Chiasmus by other products, as the key material used in Chiasmus is not compatible with other products.

In the meantime, alternative products for Chiasmus that have been approved or released for VS-NfD are available and offer more functions. Chiasmus is scheduled to be retired at the end of 2021, which means that approval for VS-NfD will be withdrawn. It will also cease distribution of the program and support for it. In addition, since Chiasmus will not be further developed, it cannot be ruled out in future operating system versions that the execution of Chiasmus and thus the decryption of files encrypted with Chiasmus may no longer be possible in the future. As described in Section 6.6, archived files must be decrypted in a VS-NfD approved environment. They can then be stored decrypted in such an environment or, after re-encryption with one of the alternative products, stored on a medium that does not have to be VS-NfD compliant.

This document briefly introduces the available alternative products and explains how current processes performed with Chiasmus can be accomplished with the alternative products.

2 Alternative products

Currently, two VS-NfD approved products are available on the market - "GnuPG VS-Desktop" from the company g10 Code and "GreenShield" from the company cryptovision. Both products can encrypt and decrypt files with a symmetric key derived from a password. However, they are only partially compatible with each other in this respect, as different standards are used (see Table 4 in Chapter 4). These symmetric procedures correspond to the functionality of Chiasmus, but are not interoperable with the procedure implemented in Chiasmus, so that files encrypted with Chiasmus cannot be decrypted with the replacement products and vice versa.

In addition, both products can be used to asymmetrically (hybridly) encrypt, decrypt and sign e-mails as well as files.

The asymmetric encryption of files and e-mails offers several advantages over symmetric encryption, which can be taken into account accordingly in the respective use case (see Chapter 6). For example, the comparatively time-consuming distribution of symmetric keys is eliminated by the possibility of simply distributing the public part of the key of the asymmetric procedure. The renewal of certificates is less costly with the OpenPGP standard. In addition, asymmetric encryption ensures the integrity and authenticity of files and e-mails by signing them. Further details on certificates can be found in chapter 3.

2.1 *GnuPG VS-Desktop* from the manufacturer *g10 code GmbH*

GnuPG VS-Desktop (formerly known as Gpg4VS-NfD) is a software suite of the encryption software GnuPG. For the asymmetric (hybrid) encryption and decryption of files and e-mails, GnuPG VS-Desktop supports both the S/MIME and the OpenPGP standard, both of which are asymmetric public-key encryption methods. Symmetric encryption and decryption of files is basically performed using the OpenPGP standard. In addition, files symmetrically encrypted using the S/MIME standard can be decrypted using GnuPG VS-Desktop (see chapter 4).

GnuPG VS Desktop can be used in two different VS-NfD-compliant operating modes: the approval for use with smart card (BSI-VSA-10573) requires the use of a smartcard to store the private key material, the (conditional) approval for use without smart card (BSI-VSA-10584) allows operation without a smartcard. In this case, the private key material is stored as a so-called soft token in a protected area on the workstation computer.

GnuPG VS-Desktop is currently offered for the following operating systems:

- For Microsoft Windows (originally under the name Gpg4Win)
  Further information at: https://gnupg.com/gnupg-desktop.de.html
- For Linux (under the name Gpg4KDE)
  Further information at: https://www.gpg4kde.de/

GnuPG VS-Desktop can be purchased from the manufacturer or via a framework agreement at the federal department store. The price depends on the licence volume. Services such as support and consulting can also be purchased from the manufacturer.

Contact details of the manufacturer g10code GmbH

Phone:	+49 2104 4938797
E-mail:	info@gnupg.com
Internet:	gnupg.com/index.html
KdB framework contract:	21061

GnuPG VS-Desktop is open source software and is licensed under the GNU GPL and other open source software licenses.

2.2 *GreenShield* from the manufacturer *cv cryptovision GmbH*

GreenShield uses the S/MIME standard for asymmetric (hybrid) encryption and decryption of files and e-mails. OpenPGP is not currently supported, but according to the manufacturer is in planning. Please refer to the manufacturer for further information on the support of OpenPGP. Symmetric encryption and decryption of files is performed using the S/MIME standard.

For VS-NfD-compliant operation, GreenShield must be used in accordance with the requirements of the approval for use with smart card (BSI-VSA-10552 and BSI-VSA-10600), which requires the use of a smartcard to store the private key material. Technically, operation without a smart card is possible, but not VS-NfD compliant.

GreenShield is available for the following operating system:

- Microsoft Windows

The program can be obtained directly from the manufacturer or via a framework agreement at the federal department store. The price depends on the version used (file and/or e-mail encryption) and the licence volume. Services such as support and consulting can also be purchased from the manufacturer.

Contact details of the manufacturer cryptovision GmbH

Phone: +49 209 1672450

E-mail: info@cryptovision.de

Internet: www.cryptovision.com/produkte/sichere-verschluesselung/GreenShield/

KdB framework contract: 21230

GreenShield is under a proprietary license.

2.3 Summary of the functionalities of the alternative products

The use cases covered by the products presented in sections 2.1 and 2.2 are summarized in the table below.

Functionality	*GnuPG VS-DesktopVersion 3.x (BSI-VSA-10584)*	*GnuPG VS-DesktopVersion 3.x (BSI-VSA-10573)*	*GreenShieldVersion 1.2.1 (BSI-VSA-10552) (BSI-VSA-10600)*
E-mail encryption and decryption with Smartcard S/MIME (X.509)	✓	✓	✓
E-mail encryption and decryption with smartcard OpenPGP	✓	✓	-
Encryption and decryption of files certificate-based S/MIME with smartcard (asymmetric)	✓	✓	✓
Encryption and decryption of files certificate-based OpenPGP with smartcard (asymmetric)	✓	✓	-
E-mail encryption and decryption with Softtoken S/MIME (X.509)	✓	-	-
E-mail encryption and decryption with Softtoken OpenPGP	✓	-	-
Encryption and decryption of files certificate-based S/MIME with Softtoken (asymmetric)	✓	-	-
Encryption and decryption of files certificate-based OpenPGP with Softtoken (asymmetric)	✓	-	-
Encryption and decryption of files with passphrase OpenPGP (symmetric)	✓	✓	-
Encryption of files with passphrase S/MIME (symmetric)	-	-	✓
Decryption of files with passphrase S/MIME (symmetric)	✓	✓	✓
Simultaneous encryption and decryption of multiple files and folders, also recursively	✓	✓	✓
Encrypted Drafts e-mail S/MIME	✓	✓	✓
Encrypted drafts e-mail OpenPGP	✓	✓	-

Functionality	*GnuPG VS-DesktopVersion 3.x (BSI-VSA-10584)*	*GnuPG VS-DesktopVersion 3.x (BSI-VSA-10573)*	*GreenShieldVersion 1.2.1 (BSI-VSA-10552) (BSI-VSA-10600)*
Support command line / command prompt	✓	✓	-
Script controlled / API interface – E-mail	✓	✓	-
Script controlled / API interface - File encryption (Chiasmus replacement)	✓	✓	-
Windows	✓	✓	✓
Linux	✓	✓	-

Table 2: Summary of functionality and interoperability of replacement products.
Meaning: ✓ = Supported, - = Not supported (or not covered by the approval)

3 Certificates

In order to be able to use asymmetric encryption, each user requires their own certificate or key pair. These consist of a private and a public part. While the public part can be made accessible to everyone, the private part must be kept secret. The two standards S/MIME (X.509 certificates) and OpenPGP are used, which are not compatible with each other due to their different trust models.

Before encrypted communication can take place between sender and recipient, both must exchange and import the public part of the certificate/key with each other. The possible ways are described below. If a message is now sent to a communication partner, the message is encrypted with the recipient's public certificate/key. This ensures confidentiality. With the private part of the sender the message is signed. The recipient of the message can decrypt it again with his private certificate/key. And with the public certificate/key of the sender he can check the signature. If this is correct, the recipient knows that both the authenticity of the sender and the integrity of the message are guaranteed.

In order for a system for e-mail and file encryption to be used for VS-NfD, it is not absolutely necessary for all private keys to be stored on a hardware token (e.g. smartcard). The exact scope of the BSI requirements for e-mail and file encryption can be found in the VS requirements profile BSI-VSAP-0014. The evaluation of a corresponding product must show that the BSI requirements are generally met.

Further information on the use of the approved products can be found in their Security Operations (SecOps, formerly Deployment and Operating Conditions). These documents may contain requirements that all keys must be stored on a hardware token for the approved operation of the product. However, this is then due to the design of the product itself and its operational environment and not to the general requirements of the BSI, see the corresponding SecOps and the VS-AP.

If a (conditional) approval for use without smart card is issued by the BSI for a product, the use of such a product in comparison to a product with approval for use with smart card normally involves further requirements, specifications or risks. These must be observed and taken into account when the VS-IT is released by the department management in accordance with §50 VSA. The SecOps relevant for the respective product must also be complied with.

For both products operated in correspondence to the approval for use with smart card, the private part of the certificate / key must be stored on a hardware token (see Annex A of the conditions of use and operation (SecOps) of the respective product for the permitted smart cards).

In case of the (conditional) approval for use without smart card (GnuPG VS-Desktop only), the private part can also be stored, protected by a password, in the product's certificate manager within a VS-NfD compliant environment.

3.1 X.509 certificates

An own X.509 certificate (private and public part) for data secured with S/MIME must be applied in the associated organization. Appropriate instructions on how to do this should be available within the organization. The private part of the certificate is delivered to its owner stored on a hardware token. If GnuPG VS-Desktop is used corresponding to (conditional) approval for use without smart card, the private part of the certificate can be delivered as a soft token for import into the certificate store. When delivering the certificate, it is important to ensure that the soft token is sufficiently secure. The public part of the certificate is automatically made available to other users via the Public Key Infrastructure (PKI) using various interfaces (such as LDAP) and is automatically authenticated by the CA. In order for the certificates to be used for VS-NfD, they must comply with the requirements from the SecOps of the replacement products and BSI TR-02102-1.

Note: In order to be able to use certificates from a PKI other than one's own PKI in a VS-NfD-compliant manner, the root CA of the foreign PKI must be trusted by one's own institution. This implies that the requirements of TR-03145-1 and TR-03145-VS-NfD Secure CA Operation are met. How to obtain the documents is described in chapter 9.

Public authorities obtain their certificates e.g. via commercial providers or via their own sub-CA of the V-PKI. For federal administration departments, S/MIME certificates can be obtained from the IVBB-CA, for state authorities and municipalities from the DOI-CA. Contacts of authorized persons can be obtained from the BSI (V-PKI). These institutions can also operate their own PKI that meets the requirements of TR-03145-VS-NfD Secure CA Operation. Companies in the context of Security of Classified Material can ask the German Federal Ministry for Economic Affairs and Energy (Bundesminsterium für Wirtschaft und Energie, BMWi) for suitable CA / X.509 certificates.

The price and validity period for an X.509 certificate can be obtained from the respective CAs.

3.2 OpenPGP certificates

A separate OpenPGP certificate (private and public part) for data secured with the OpenPGP standard can be created using GnuPG VS-Desktop or an existing certificate can be imported. Detailed instructions can be found in the product's user manual. The public part of the certificate can be distributed in various ways, e.g.

- In a personal contact,
- as an e-mail attachment,
- as a publication on public key servers or
- via Web Key Directory (WKD) / Web Key Service (WKS).
  cf. https://wiki.gnupg.org/WKD

The public certificate of the communication partner can be obtained in the same way and then imported. The operation of a PKI is not provided in the OpenPGP standard. Before using a certificate, its authenticity must therefore be checked. See the explanations in this document for option 3 in use case 6.1.3.

There are no costs for OpenPGP certificates. The validity period can be defined by the user and is preset at 2 years. The validity period can be extended by the user. In order for the certificates to be used for VS-NfD, they must satisfy the requirements from the SecOps of the replacement products and BSI TR-02102-1.

4 Interoperability of the alternative products

When using the S/MIME standard, the asymmetric encryption and decryption of files and e-mails are compatible with each other and both should be able to be exchanged between the replacement products without any problems. The OpenPGP standard is currently only supported by GnuPG VS-Desktop for asymmetric encryption and decryption of files and e-mails as well as for symmetric encryption and decryption of files. GreenShield uses the S/MIME standard for symmetric encryption and decryption. In addition, files symmetrically encrypted with GreenShield using the S/MIME standard can be decrypted with GnuPG VS-Desktop. Therefore, the two products are only partially compatible with each other for the use case of symmetric encryption and decryption of files.

The following table shows the use of the OpenPGP and S/MIME standards with regard to symmetrical encryption and decryption of files and the associated interoperability for both products:

Symmetric encryption with passphrase	*S/MIME*	*OpenPGP*
GnuPG VS Desktop	Decrypt	Encrypt/Decrypt
GreenShield	Encrypt/Decrypt	-

Table 3: Overview of product interoperability for symmetric encryption with passphrase

If interoperability is required for all use cases, both products can be installed and used. A common key and certificate management is not possible in this case and is dealt with separately by each product. A parallel integration of both products in the used e-mail program (Outlook) is possible according to the manufacturer cryptovision.

5 Basic operation of the alternative products

Details on the mode of operation of the replacement products listed in chapter 2 cannot be explained in this document. Instead, references are made to the corresponding manufacturer manuals. Furthermore, the user must comply with and implement the specifications in the conditions of use and operation in the document of the corresponding products (i. e. approval for use with smart card or (conditional) approval for use without smart card). These can be obtained directly from the manufacturer or from the Federal Department Store (Kaufhaus des Bundes, KdB).

Both GnuPG VS-Desktop and GreenShield can be integrated into an e-mail client so that e-mails can be encrypted and signed automatically. It is therefore not necessary (as with Chiasmus) to encrypt files separately and attach them to the e-mail. In addition, not only the attachments, but the entire message content is encrypted.

GnuPG VS-Desktop is supported by Microsoft Outlook on Windows and Kmail on Linux. Here, the plugin with its GUI is integrated into the interface of the e-mail client. Encrypted or signed mails can be displayed in the preview window as well as in a separate window. The module for file encryption GpgEX of GnuPG VS-Desktop is provided via a dedicated GUI.

GreenShield is supported by both Microsoft Outlook and IBM/HCL Notes under Windows. GreenShield is used in a separate window. Encrypted or signed mails can only be displayed in a separate window. GreenShield File provides a dedicated GUI.

An integration of the products into web applications is not possible.

6 Use cases

This section considers use cases where confidential data is exchanged. For each use case listed, the following sections describe the status quo with Chiasmus and how a solution might look like with the alternative products listed in section 2. [1]

The use cases listed in this section refer to the GUI version of Chiasmus. Specially approved use cases that make use of the Chiasmus command line version are discussed in Use Case 6.4.

6.1 Communication with few other users

6.1.1 Description

A user exchanges sensitive documents with a manageable amount of other users. These are only individual communication partners or a small, dynamically changing group, so that the distribution list of addressees must often be readjusted. The exchange of information between users fulfils theneed-to-know principle.

6.1.2 Previous procedure with chiasmus

Each pair of communication partners requires a common individual chiasmus key. This key must be generated before the first transmission of sensitive data and exchanged between the communication partners in a confidential manner. According to the conditions of use and operation of Chiasmus, the keys must be exchanged for VS-NfD communication

- with a personal contact,
- via an at least VS-NfD approved encrypted connection or
- by mail, primarily in a sealed envelope or insured letter.

The key can be passed on/transmitted in the form of a file (file extension .xis), printed out on a sheet of paper or orally as a character string. A checksum automatically calculated by the program makes it easier for the user to enter the key correctly when it is typed via the keyboard.

A file encrypted with Chiasmus can then be attached to an e-mail or delivered to the recipient on a data carrier. If this can be decrypted without error at the recipient's end, the recipient can usually assume that the file was actually encrypted by an owner of the key and not subsequently tampered with.

6.1.3 Possible procedure with GnuPG VS-Desktop or GreenShield

1. Since GnuPG VS-Desktop and GreenShield offer the possibility of encrypting files using a key derived from a password, the procedure practiced with Chiasmus can in principle be retained. When choosing your own password, both alternative products require it to be much more complex than is usual for other applications (e.g. access password for a web application or PIN for a bank card). The reason for this is that there is no failure counter for an attacker to decrypt a file; rather, an attacker can systematically test any number of passwords until a decryption ends successfully. The conditions of use and operation specify that a password should contain at least 20 to 25 randomly chosen characters.
   If the password is used to protect VS-NfD data, the password itself must be classified VS-NfD and treated accordingly.
   Note: Encrypting an entire e-mail with a password is not possible.
2. If two users each have a certificate of a CA (X.509 certificate), the sender of the data can download the certificate of the recipient and encrypt the data with the key contained in the certificate. Both CAs must belong to the same PKI or to PKIs that are compatible (certified) with each other. The search and verification of the recipient's certificate is supported automatically when using an e-mail client. However, the sender must make sure that the correct certificate

has been selected by the software. A suitable configuration of the workstation can automate this decision. In addition, the sender should provide the encrypted file (or e-mail) with a digital signature. This is checked for validity at the recipient (using the sender's certificate). In this way, the recipient can be sure that the alleged sender is actually the sender of the encrypted data and that it has not been manipulated.
Manual verification of the validity of a certificate via LDAP and/or OCSP and configuration for offline use and evaluation of CRLs is also possible.
GnuPG VS-Desktop and GreenShield offer to display the algorithms used and show warnings if they are not VS-NfD compliant.

3. Only possible with GnuPG VS-Desktop: Sender and recipient exchange the public parts of their OpenPGP certificates, which they have generated themselves. The certificate (which contains the key required for encryption or signature verification) can be transmitted over an insecure channel (e.g. via e-mail). [2] However, it is necessary for the sender and recipient to verify the authenticity of the certificates received, for example by comparing the fingerprint of the certificates. This comparison can take place verbally in a telephone call, provided that the sender and recipient know each other personally.

In case of options 2 and 3, an e-mail or file to be sent is encrypted with the public part of the recipient's certificate and digitally signed with the private part of the sender's certificate.

6.2 Communication within a large user group

6.2.1 Description

A user exchanges documents with a potentially large number of other users on an irregular basis. It is not known in advance who exactly the user's possible communication partners are, i.e. the composition and size of such a group can change on a short time scale. The exchange of information between users involved in the communication fulfils the need-to-know principle. If the composition and size of the group does not change and is known, use cases 6.3 or 6.4 apply.

6.2.2 Previous procedure with chiasmus

Chiasmus is not intended for this use case.

6.2.3 Possible procedure with GnuPG VS-Desktop or GreenShield

Essentially the same procedure can be used as for procedures 2 or 3 in use case 6.1.

6.3 Use of a group key

6.3.1 Description

Documents are exchanged within a working group or a project. The composition of such a group is static, so that the group-internal exchange of information takes place via a fixed distribution list of addressees. All group members comply with the need-to-know principle.

6.3.2 Previous procedure with chiasmus

A member of the group creates a chiasmus key in advance. The key is distributed to the other group members as specified in 6.1.2, e.g. during a joint meeting of the group. Subsequently, the group members can use the key to encrypt data and send it to individual or all other members of the group, who can decrypt the data again using the same key.

6.3.3 Possible procedure with GnuPG VS-Desktop or GreenShield

1. Since GnuPG VS-Desktop and GreenShield offer the option of encrypting files using a password, the procedure practiced with Chiasmus can in principle be retained.
   The comments made in option 1 in section 6.1.3 should also be observed here.
2. A member of the group creates an OpenPGP key intended only for this group (only possible with GnuPG VS-Desktop). This group key (i.e. the two certificates containing the private and the public key) is distributed to the other group members as specified in 6.1.2, e.g. during a joint meeting of the group. Subsequently, the group members can use the group key to encrypt and sign data and send it to individual or all other members of the group.
3. Alternatively, an X.509 group certificate can be requested from the associated CA by the group member responsible for the group mailbox. This member then distributes the certificate with its private and public parts to the other group members in a secure manner, as specified in 6.1.2.

Note 1: A group key should be changed regularly, especially when members leave the group. A new group key must not be encrypted with the old group key and sent to members via an unprotected route.

Note 2: A group key with X.509 certificates is far more complex to manage than with OpenPGP certificates, especially if the members of the group change frequently.

NOTE 3: After all members of the group have exchanged their public OpenPGP or S/MIME certificates with each other or these certificates are otherwise available to all group members, communication for this use case can take place as described in options 2 and 3 under use case 6.1.3. The secured messages or files are sent to the corresponding distribution list.

6.4 Sending documents from one point to a large group (scripted encryption, command line)

6.4.1 Description

An entity regularly sends documents to a very large group of users, e.g. a newsletter that is not intended for the general public. In this use case, a mutual exchange between the sending entity and the group is not the primary goal (cf. use case 6.2).

6.4.2 Previous procedure with chiasmus

The command line version of Chiasmus is used to encrypt e-mail attachments, generate e-mails, and send them to a list of recipients, scripted with a key sent to the recipients in advance (as specified in 6.1.2). The recipients can decrypt the e-mail attachments using the GUI version of Chiasmus.

Note: The command line version of Chiasmus has no general approval for VS-NfD. In order to use it for processing VS-NfD, a special individual approval is required.

6.4.3 Possible procedure with GnuPG VS-Desktop

1. GnuPG VS-Desktop can also be operated script-controlled. Script-controlled operation is part of the approval. The specifications and applications for this can be found in the SecOps of the approval. Therefore, the procedure practiced with Chiasmus can be retained in principle.
2. GnuPG VS-Desktop offers the option of defining groups with the Kleopatra software. The group members can be assigned their S/MIME or OpenPGP certificates. Both standards are supported within a group. This means that encrypted e-mails can be sent for a large distribution list without much effort.

6.4.4 Possible procedure with GreenShield

GreenShield cannot currently cover this use case.

6.5 Encryption for personal data exchange

6.5.1 Description

- A user exchanges documents with himself (on another computer) over an insecure channel, for example between home office and office workstation.
- A user stores data on a data carrier for transport and fears the possible loss of the data carrier and thus the compromise of the data.

6.5.2 Previous procedure with chiasmus

The procedure is analogous to Use Case 6.1.2. There is no need to exchange the key with other users here.

6.5.3 Possible procedure with GnuPG VS-Desktop or GreenShield

1. Since GnuPG VS-Desktop and GreenShield offer the option of encrypting files using a password, the procedure practiced with Chiasmus can in principle be retained. There is no need to exchange the key with other users. Of course, the password used for encryption must not be transmitted over the same channel or stored on the same data carrier as the data to be protected.
   The comments made in option 1 of use case 6.1.3 must also be observed here.
2. The user uses his own S/MIME or OpenPGP key for encryption and signature creation. In use case 6.1.3 with options 2 and 3, different or the same certificates can be used on the source and target computers.

6.6 Storage encryption ("Data at Rest")

6.6.1 Description

Data is stored in encrypted form on a data carrier, e.g. for archiving.

6.6.2 Previous procedure with chiasmus

With Chiasmus, individual files or entire folders (including subfolders) can be encrypted with a uniform key. The encrypted data can then be stored on an external data carrier. While there are no confidentiality requirements for the encrypted data (the storage location does not have to be NfD-suitable), the key used must be protected against unauthorized access. Under no circumstances may the key be stored together with the data, not even as a password-protected file.

6.6.3 Possible procedure with GnuPG VS-Desktop or GreenShield

1. Since GnuPG VS-Desktop and GreenShield offer the possibility to encrypt files or entire folders using a password, the procedure practiced with Chiasmus can in principle be retained. The password must be communicated to other users who are to have access to the stored data. Of course, the password used for encryption must not be stored on the same data carrier as the data to be protected.
   The comments made in option 1 of use case 6.1.3 must also be considered here.

2. You can proceed as described in 6.1.3 according to options 2 and 3, whereby your own X.509 or OpenPGP certificate is selected for encryption and signing instead of a password. Certificates of other users can also be selected if they are to be authorized to access the data.
3. The procedure can be the same as in the previous option 2, except that a group certificate is used instead of the individual X.509 or OpenPGP certificates of the users with access rights. (Cf. 6.3.3, options 2 and 3).

6.6.4 Conversion of chiasmus-encrypted archived data

Existing files encrypted with Chiasmus cannot be decrypted with the alternative products. To recode such existing files (for example in archives) for use with the alternative products, the following steps can be followed.

1. Copy Chiasmus-encrypted files to a VS-NfD-suitable environment
2. Decrypt encrypted files with Chiasmus
3. Encrypt files with an alternative product
4. Copy encrypted files back to the storage location (this does not have to be VS-NfD suitable)

Steps 3 and 4 can be omitted if the location where the files are stored is already a VS-NfD-suitable environment.

Note on step 2:

To decrypt large numbers of Chiasmus-encrypted files, the Windows version of Chiasmus can be used to select a file folder and decrypt all the contained files in a single operation. However, this requires that the files to be decrypted are encrypted with the same Chiasmus key.

The Linux version of Chiasmus cannot decrypt multiple files simultaneously in one step. However, since the Linux version is a command line tool, it can be controlled via a script and thus automatically decrypt large numbers of files in a single step. For this purpose it is recommended to remove the password protection of the respective chiasmus key file in order not to have to type in the password for each file. This is done with the command "**chiasmus -m p -s file.xis**". Here, file.xis contains the chiasmus key whose password is to be changed. You will then be asked to enter the old and a new password. For the new password, type the Enter key (without entering a password first).

[1] If you do not find your process among the listed use cases or have further questions, please contact chiasmus@bsi.bund.de.

[2] Under no circumstances may the associated private keys be exchanged.

7 Criteria for the suitability of the alternative products

In order to be able to evaluate for your own use case which of the two replacement products is the more suitable, the following criteria should be considered:

- Which standards and functionalities are needed to stay in communication with partners?
- Which functionalities are required for internal processes?
- Can the requirements according to the SecOps for the correct product use be fulfilled? In particular, the requirements that must also be met by the IT environment so that the products can be integrated and rolled out.

8 Points to note before the initial operation

Before the products are rolled out and put into operation, it should be clarified that the required certificates are available to the users when they go live. The certificates should be applied for and distributed with sufficient lead time so that they can be imported and used during commissioning. If necessary, care must also be taken to connect to or set up a PKI. If required, group certificates must also be generated and distributed in good time and script solutions created.

9 Related documents

The following documents can be downloaded from www.bsi.bund.de/Zulassung with access data (see there how to obtain them):

- *BSI-VSA-10573* (SecOps for approval for use with smart card GnuPG VS-Desktop)
- *BSI-VSA-10584* (SecOps for (conditional) approval for use without smart card GnuPG VS-Desktop)
- *BSI-VSA-10552, BSI-VSA-10600* (SecOps approval for use with smart card GreenShield)

The document *BSI-VSAP-0014-2018* (VS requirement profile for secure transmission of e-mails and files) can be requested by e-mail. Details are available at the above web address.

The BSI Technical Guidelines

- *BSI TR-02102-1* (Cryptographic methods: recommendations and key lengths)
- *TR-03145-1*
- *TR-03145-VS-NfD Secure CA Operation*

can either be downloaded from https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/technische-richtlinien_node.html or requested from BSI-department KM 35 (referat-km35@bsi.bund.de).

User manuals and further documentation of the alternative products can be requested from the respective manufacturer.

10 Abbreviations

API	Application Programming Interface
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (Federal Agency for Digital Radio of Security Authorities and Organisations)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
CA	Certification Authority
CRL	Certificate Revocation List
DOI	Germany Online Infrastructure (Bund-Länder-Kommunen-Verbindungsnetz, now NdB-Verbindungsnetz)
GNU	free unix-like operating system
Gpg/GnuPG	GNU Privacy Guard
GPL	General Public License
GUI	Graphic User Interface
IMAP(S)	Internet Message Access Protocol (over TLS); method of retrieving e-mails from a mail server with a mail program
iOS	mobile operating system developed by Apple for the iPhone and iPod touch
IT	Information Technology
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
KdB	Kaufhaus des Bundes (Federal department store)
KDE	originally: K Desktop Environment; community dedicated to the development of free software
LDAP	Lightweight Directory Access Protocol
MAPI	Messaging Application Programming Interface
NdB	Netze des Bundes (federal network), formerly IVBB (Information Network Berlin-Bonn)
OCSP	Online Certificate Status Protocol
OpenPGP	A standardized data format for encrypted and digitally signed data. It also defines the format of a certificate, which contains the public key of the certificate holder. PGP stands for Pretty Good Privacy.
PC/SC	Personal Computer/Smart Card; a standard for smart card readers
PIN	Personal identification number (to be kept secret)
PKI	Public Key Infrastructure
SecOps	Security Operations; formerly "Deployment and Operating Conditions
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP(S)	Simple Mail Transfer Protocol (over TLS); a protocol for exchanging e-mails.
TLS	Transport Layer Security
TR	Technische Richtlinie (technical guideline)
V-PKI	Verwaltungs-PKI (management PKI)
VS	Verschlusssache (classified information)
VSA	Verschlusssachenanweisung (instruction for classified information)

VS-AP	VS-Anforderungsprofil (profile of requirements for classified information)
VS-NfD	VS - Nur für den Dienstgebrauch (classified information for official use only)
WKD/WKS	Web Key Directory / Web Key Service
X.509	An ITU-T standard for a PKI for creating digital certificates