Bundesamt für Sicherheit in der Informationstechnik

SECURITY OPERATING PROCEDURES AND OPERATIONAL COMSEC DOCTRINE
GnuPG VS-Desktop, Version 3.x

BSI-VSA-10584

Issued: 07.02.2022

Suitable for protecting: RESTREINT UE/EU RESTRICTED
NATO RESTRICTED

Version EU - NATO - Multi National

Change history

version	date	changed by	comments/reasons for change
V 1.0	15.07.2021	BSI	final version
V 1.1	07.02.2022	BSI	Changes in 2.7 and 5.3

Table of Contents

Annexes

Figures

Tables

Blank Page

FOREWORD

This Doctrine and Information Publication - Operational COMSEC Doctrine and Security Operating Procedures (SecOPs) for the GnuPG VS-Desktop is issued by the German National Communications and Information Systems (CIS) Security Authority (NCSA), the Bundesamt für Sicherheit in der Informationstechnik (BSI). This publication prescribes the minimum-security requirements for the installation, integration, configuration, control, safeguarding and use of the GnuPG VS-Desktop and its associated security management and documentation.

This publication complements the User Manual of GnuPG VS-Desktop in some security related areas and shall be read and applied in conjunction with them.

The information provided by this publication is not classified.

Extracts from this publication may be made for official purposes and the entire Publication may be duplicated locally without BSI authorisation.

This document is effective upon receipt. The provisions of this publication are prescriptive. Requests for waivers of such provisions shall be submitted to BSI through appropriate EU, NATO or national channels.

The EU, EU Member States, EU Agencies and EU civil and military Bodies as well as NATO Nations, NATO civil and military Bodies and NATO Commands and Agencies are encouraged to make this publication available for use by Communications and Information Systems (CIS) Planning and Implementation Authorities, CIS Operating Authorities, Security Management Staffs and Users in accordance with the need-to-know principle.

Questions concerning this Publication may be directed to BSI by message to:

Bundesamt für Sicherheit in der Informationstechnik
Postfach (POB) 200363
D-53133 Bonn
Germany

E-mail: zulassung@bsi.bund.de

1   INTRODUCTION

1.1   Purpose

This document including its Annexes constitute the Operational COMSEC Doctrine and Security Operating Procedures (SecOPs) for GnuPG VS-Desktop for the protection of information classified RESTREINT UE/EU RESTRICTED and NATO RESTRICTED and corresponding national classifications, or requiring EU and NATO Strength of Mechanism (SoM)-Level STANDARD.

GnuPG VS-Desktop meets the requirements for the Strength of Mechanism (SoM) Level STANDARD as defined in references E5 (EU) and N3 (NATO). In exceptional cases where a product which is approved for SoM STANDARD is intended to be used for classification levels higher than RESTREINT UE/EU RESTRICTED and NATO RESTRICTED, a risk assessment (considering Threat and Impact levels) according to the aforementioned references shall be made for the intended application and usage scenario. The necessary assessment shall be done by the national Crypto Approval Authority (CAA), resp. the National CIS Security Authority (NCSA), together with the responsible Security Accreditation Authority (SAA). The CAA, resp. NCSA, and the SAA can approve the use for special applications in special scenarios if the requirements given in the references are met, the assessment returned a positive result and the compliance to EU and NATO TEMPEST/EMSEC requirements is achieved.

This document prescribes the minimum-security requirements for the installation, integration, configuration, control, safeguarding and use of the GnuPG VS-Desktop , its security management, ancillaries, and documentation hereinafter referred to as GnuPG VS-Desktop.

1.2   Application

This publication applies to EU Member States, EU Bodies and EU Agencies as well as NATO Nations, NATO civil and military Bodies and NATO Commands and Agencies, national governments, institutions, agencies and companies that use the GnuPG VS-Desktop for the protection of classified information at the levels specified above and shall be made available to all staff responsible for controlling, shipping, installation and operation of GnuPG VS-Desktop.

1.3   Prerequisite

A prerequisite for the purchase, lease, loan and use of GnuPG VS-Desktop by a nation is a General Security Agreement (GSA) being in force between Germany and that nation. Otherwise, the German CAA/NCSA shall be contacted beforehand.

1.4   References

The following references are cited in this publication. When GnuPG VS-Desktop is used to protect EU- or NATO-classified information, the referenced EU-, resp. NATO-documentation shall be applied. In all other cases, e.g. when GnuPG VS-Desktop is used to protect national classified information or GnuPG VS-Desktop is used by an EU- and/or NATO-Nation outside the EU- or NATO-context, the referenced EU-, resp. NATO-documents shall be applied by analogy.

Nations which are not a member of the EU and/or NATO and do not have access to the referenced documentation, shall get in touch with the Point of Contact given here for specific advice.

Security Policies		
	EU	
E1	**2013/488/EU**	Council Decision of 23 September 2013 on the Council Security Rules

E2	**2001/844/EC**	Commission Decision of 29 November 2001 amending its internal Rules of Procedure (Commissions Provisions on Security)
E3	**2013/C 190/01**	EEAS Decision of the HR on the Security Rules for the European External Action Service
	NATO	
N1	**C-M(2002)49**	NATO Security Policy (NATO UNCLASSIFIED)
Cryptographic Policies, Directives and Guidelines		
	EU	
E4	**IASG 2-03**	IA Security Guidelines on Crypto and COMSEC Management (RESTREINT UE / EU RESTRICTED)
E5	**IASP 2**	EU Council 10745/11 – IASP 2 – Information Assurance Security Policy on Cryptography, 30 May 2011 (RESTREINT UE/EU RESTRICTED)
	NATO	
N2	**SDIP-293/1**	Instructions for the Control and Safeguarding of NATO Cryptomaterial (NATO RESTRICTED)
N3	**AC/322-D/0047**	AC/322-D/0047-REV2 – INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms (NATO RESTRICTED)
N4	**AC/322-D/0048-REV3 (INV)**	AC/322-D/0048-REV3 - Technical and Implementation Directive on CIS Security (18.11.2019)
TEMPEST/EMSEC		
	EU	
TE1	**IASP 7**	IA Security Policy on TEMPEST (RESTREINT UE/EU RESTRICTED)
TE2	**IASG 7-01**	IA Security Guidelines on Selection and Installation of TEMPEST Equipment (RESTREINT UE/EU RESTRICTED)
TE3	**IASG 7-02**	IA Security Guidelines on TEMPEST Zoning Procedures (RESTREINT UE/EU RESTRICTED)
TE4	**IASG 7-03**	IA Security Guidelines on EU TEMPEST Requirements and Evaluation Procedures (CONFIDENTIEL UE/EU CONFIDENTIAL)
	NATO	
TN1	**AC/322-D(2019)0021**	INFOSEC Technical and Implementation Directive on Emission Security (NATO RESTRICTED)
TN2	**SDIP-27**	NATO TEMPEST Requirements and Evaluation Procedures (NATO CONFIDENTIAL)
TN3	**SDIP-28**	NATO Zoning Procedures (NATO RESTRICTED)
TN4	**SDIP-29**	Selection and Installation of Equipment for the Processing of Classified Information (NATO RESTRICTED)
Other References		
	Approvals	

A1	**National Approval**	National approval for the protection of VS - NUR FÜR DEN DIENSTGEBRAUCH, BSI-VSA-10584, dated 07.02.2022, incl. Annexes
	<u>**Compliance**</u>	
C1	**Declaration of Compliance**	**Declaration of Compliance** (see Chapter 5.2)
	<u>**Operating Manuals/Handbooks**</u>	
H1	**User Manual**	Gpg4win compendium 3.0.0, 21 September 2010
H2	**Approval Manual**	Manual on the approval of Gpg4win and Gpg4KDE 1.6, 24 April 2018

Table 1: References

1.5 Terminology

The following specialized terminology, used in this Publication, is provided for ease of reference:

Common Terms and Abbreviations	
ATO	Approval To Operate
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAA	Crypto Approval Authority
CCI	Controlled Cryptographic Item
CIS	Communications and Information Systems
CISOA	CIS Operational Authority
COMSEC	Communications Security
Cryptomaterial	The term Cryptomaterial describes material, including keymaterial in all forms and devices, or equipment, which contain cryptocomponents and are essential to the encryption, decryption or authentication of telecommunications necessary for maintaining confidentiality, integrity, authenticity or availability for CIS.
DoC	Declaration of Compliance
EMSEC	Abbreviation for „Emission Security"
IA Operational Authority	Information Assurance Operational Authority
IT	Information Technology
MEP	German acronym for a "TAMPER Detection Sticker" (Sticker for securing equipment housings against tampering. Manipulations can be detected.)
NCSA	National CIS Security Authority (NATO terminology; in Germany the BSI)
NDA	National Distribution Authority
QATT	Quality Assurance TEMPEST Test
SAA	Security Accreditation Authority
SecOPs	Security Operating Procedures

SoM	Strength of Mechanism (References E5 and N3)
TEMPEST	Synonym for „Emission Security"
Product Specific Terms and Abbreviations	
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
OCSP	Online Certificate Status Protocol
PKCS#1	Basic definitions of and recommendations for implementing the RSA algorithm for public-key cryptography
PKI	Public Key Infrastructure
RSA	(Rivest–Shamir–Adleman) one of the first public-key, used for secure data transmission
S/MIME	Secure Multipurpose Internet Mail Extensions
X.509	Standard defining the format of public key certificates

Table 2: Terminology

1.6   Parties and Instances

The following parties and instances are involved in the implementation of these SecOPs with the tasks and responsibilities as described:

- **BSI**
  The BSI is the German National Communications and Information Systems (CIS) Security Authority (NCSA) and Crypto Approval Authority (CAA), responsible for the evaluation and approval and certification of IT-security products/systems.

- **CIS Administrator (System and Network Administrator)**
  The person(s) who administrate the secure IT-product or CIS and is (are) responsible for the secure setup and installation of the product/system. Normally the CIS Administrator has full access rights for the configuration and use of the secure IT-product/-system.

- **CIS Operational Authority (CISOA)/Information Assurance (IA) Operational Authority**
  The authority which is i.a. responsible for
    o defining the business and operational requirements, operating principles and concept of operation of a CIS, including the information exchange requirements;
    o liaising, if applicable, with the SAA during the development of the security risk assessment process for a CIS to provide inputs to the assessment and to set specific requirements;
    o formally accepting the residual risk, if applicable, resulting from the security risk assessment process and agreeing on a plan to manage the residual risk;
    o ensuring that the Service Level Agreements (SLA) or similar mechanisms established for the provision of CIS services include the requirements for implementation, operation, monitoring and change management of security measures;
    o conducting operational evaluation of the CIS and validating/authorizing the CIS for operational use, once the security accreditation is granted by the SAA
    o investigating, in conjunction with the SAA, breaches or suspected breaches of security within the CIS, assessing the damage caused and reporting the conclusions to the SAA.

- **CIS Security Officer**
  The Security Officer i.a. is responsible for
  - o providing CIS Security advice to, and maintaining CIS Security awareness of, CIS administrators and users, including managers;
  - o maintaining a record of all persons authorised to use any part of the CIS and the extent of their authorisation and ensuring that those persons have the security clearance, if required, and need-to-know for the information handled in the CIS;
  - o checking the implementation and maintenance of hardware, firmware and software modifications and enhancements to the CIS to ensure that security is maintained;
  - o ensuring the correct application of transmission, cryptographic and emission security provisions, including the handling, maintenance and protection of cryptographic material, in accordance with the requirements of relevant regulations;
  - o checking security related logs for event/process failure and unauthorised user and system activity;
  - o conducting or coordinating the execution of periodic security risk and vulnerability assessment of CIS;
  - o reporting to the SAA on any detected CIS security weaknesses and vulnerabilities;
  - o managing and investigating CIS Security incidents in close coordination with the security organisation (e.g. Security Officer), the SAA and, if required, the NCSA of the crypto producing nation.

- **Crypto Custodian**
  Each organization requesting the establishment of a formal COMSEC account for receiving and handling cryptomaterial, normally has to appoint a Crypto Custodian who is familiar with the respective Policy and Directive. The Crypto Custodian has responsibility for the safeguarding and control of all cryptomaterial in his custody.

  His duties are i.a.:
  - o managing the cryptomaterial in his account to prevent loss or possible physical compromise;
  - o ensuring cryptomaterial is issued only to appropriately cleared and crypto-authorised individuals whose duties require it and advising them of their responsibility for properly safeguarding and controlling the cryptomaterial in their possession;
  - o maintaining COMSEC accounting;
  - o conducting physical inventory checks;
  - o establishing procedures to ensure strict control of each item of keymat whenever operational requirements necessitate this material being passed from one individual to another at work shift change.
  - o performing routine and emergency destruction or disposition of cryptomaterial in accordance with approved methods;
  - o ensuring that cryptomaterial is properly prepared and shipped;
  - o verifying the contents of a shipment of cryptomaterial on initial receipt (completeness, physical integrity);
  - o ensuring the integrity of cryptomaterial prior to use;
  - o issuing or transferring cryptomaterial as directed to authorised COMSEC accounts (including sub-accounts) or individual users. If the material is classified, verifying that the individuals are cleared to the classification level of the material.
  - o being familiar with current plans for the destruction, disposal, evacuation, or protection of cryptomaterial in the event of fire, disaster, or other emergency;

- o reporting immediately to the CIS Security Officer any known or suspected physical compromise, loss, or unauthorised destruction/disposal of cryptomaterial;
- o reporting keymat that is suspected to be defective or faulty to CIS Security Officer.

- **End User**
  The person(s) operating the secure IT-product/-system, responsible for the implementation of the end user specific requirements stated in this SecOPs to guarantee the correct and secure operation of the product/system. Normally an end user has limited user rights to operate the product/system.

- **Information Assurance (IA) Operational Authority**
  EU term for "CIS Operational Authority (CISOA)". See above.

- **Manufacturer**
  The manufacturer g10 code GmbH of the approved CIS security product GnuPG VS-Desktop has to meet special requirements for the development, production, evaluation, approval and sales for his product, depending on the classification level of the information to be protected. Apart from this, he is obliged to obey the German export legislation.

- **Security Accreditation Authority (SAA)**
  The SAA is responsible for performing the following functions:
  - o providing advice and guidance on CIS Security policy and directives (and supporting security measures);
  - o establishing a security accreditation process, clearly stating the security accreditation conditions for CIS under their authority and for the connections of external CIS to these CIS;
  - o reviewing and approving security-related documentation;
  - o performing a risk assessment and applying risk management for CIS being accredited;
  - o providing a statement of security accreditation resp. re-accreditation for CIS and stating the conditions and activities which have to be applied for use;
  - o performing periodic security inspections or reviews in accordance with the security accreditation process;
  - o providing direction to security management staff (e.g. Security Officer, CIS Security Officer) in investigating any breach, or suspected breach, of the security arrangements and in assessing the damage caused;
  - o providing advice/recommendations on corrective measures to be implemented (or recommending sources for appropriate advice);
  - o advising the security management staff (e.g. Security Officer, CIS Security Officer) on the security risk and countermeasures implications of any proposed changes to the CIS;
  - o liaising with other SAAs in respect to interconnected CIS for such purposes as agreeing System Interconnection Security Requirement Statements (SISRS) or national equivalent;
  - o providing advice on the interconnection of CIS handling classified information to any CIS;
  - o if a CIS is required to use assured products, liaising and coordinating with the appropriate Evaluation and Approval Authority (e.g. the NCSA of the crypto producing nation).

- **Security Officer**
  The Security Officer is responsible for
  - o ensuring the correct implementation and maintenance of the protective measures (e.g. physical security, personnel security, security of information, industrial security) of the overall security environment in which the CIS is located and which may have a bearing on the security posture of the CIS;
  - o verifying the security accreditation statements for any CIS in use to ensure that they achieve and maintain an appropriate security accreditation status;

- o ensuring that regular security audits are conducted to verify that CIS Security measures are implemented and maintained in accordance with the security Policy and supporting directives.

2   SYSTEM DESCRIPTION

2.1   Purpose

GnuPG VS-Desktop is to facilitate – by means of the Gpg4win and Gpg4kde products – the encrypted exchange of emails and the encryption of files in compliance with the classification level "VS-NfD" (Restricted).
GnuPG VS-Desktop may be used on the Windows (Gpg4win) and GNU/Linux (Gpg4KDE) platforms;

This product is a crypto library with different components based on it. The components relevant for approval are a plugin (i.e. a supplementary program) for the Microsoft Outlook email system under Windows and for Kontact under Linux including a certificate management. It supports the S/MIME standard with X.509 certificates for the exchange and storage of public keys.

The product's main security services are as follows: to receive files or emails encrypted and/or signed by means of S/MIME standard and thereby to be able to decrypt and/or verify or to be able to send files or emails which are encrypted and/or signed by means of S/MIME standard.

The GnuPG VS-Desktop product makes it possible to encrypt and decrypt files and emails based on S/MIME and to secure and verify their integrity and authenticity (i.e. their origin) by means of digital signatures.

The GnuPG VS-Desktop components relevant for approval are composed as follows:

Gpg4win is an installation package for Windows and consists of various free software components that can be optionally installed.

Gpg4KDE are individual software packages which can be installed by means of the respective Linux distribution package manager.

GnuPG:

The core element; the actual encryption program.

Kleopatra:

A certificate manager for X.509 (S/MIME); provides standardized user guidance for all crypto dialogs.

GpgOL:

A program extension for Microsoft Outlook 2010/2013/2016/2019 (email encryption). Exchange servers are supported as of exchange version 2010.

GpgEX:

A program extension for Microsoft Explorer (file encryption).

2.2   System Components and Function

Usually, GnuPG VS-Desktop is delivered from the manufacturer to the end user with the following system and accessory components (see also the user manual ("Gpg4win compendium") (reference H1)).

The Gpg4win and Gpg4KDE products consist of several components which can be installed as a package. These include a plugin (i.e. a supplementary program) for the Microsoft Outlook email program and for Kontact under Linux, the Kleopatra program for file encryption and for the key management as well as the GpgEX extension for file encryption in Windows Explorer and in Dolphin under Linux.

The product supports the S/MIME standard and uses X.509 certificates for the exchange and storage of public keys. For approved operation, it requires a smartcard for the storage of long-term secrets, such as secret signature and decryption keys.

The product's main security services are:

- Processing of received emails encrypted or signed by means of S/MIME as well as their decryption and signature verification;

- Processing of received emails encrypted or signed by means of OpenPGP as well as their decryption and signature verification;

- preparing emails encrypted or signed by means of S/MIME;

- preparing emails encrypted or signed by means of OpenPGP;

- symmetric encryption and decryption using passwords;

- creating of OpenPGP keys;

- using RSA with PKCS#1 Padding in version 1.5 and AES in the CBC mode applying S/MIME;

- using RSA and ECC with Brainpool curves in a modified CFB mode applying OpenPGP;

- using as backend in automated solutions (command line);

- managing keys and/or key certificates.

As regards receiving a file or email signed by means of S/MIME or sending a file or email encrypted by means of S/MIME this includes checking the certificate chain on the basis of certificate revocation lists (CRL), OCSP requests and trusted root certificates.

The processing of unclassified information and information not classified higher than VS-NUR FÜR DEN DIENSTGEBRAUCH, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED is carried out at the respective workplace. The workplace must be released for this purpose. In particular only authorized persons may have access to the workplace.

2.3   Approval and Approved Design Status

The type of the approval and the currently approved design status of GnuPG VS-Desktop are listed in Annex A. Prior to installation and operation of the product, the design status of the delivered product shall be checked and its conformity to the approved design status shall be verified. This should be done by the CIS Operational Authority (CISOA) (or the IA Operational Authority, resp.) and the SAA. The CISOA (or the IA Operational Authority, resp.) shall also ensure that the system has an "Approval to Operate (ATO)" by the responsible SAA for the type of classification (e.g. EU, NATO, multinational, national, …) and the classification levels to be protected, resp. the SoM levels required.

2.4   Compatibility, Interoperability and Conformity

GnuPG VS-Desktop is compatible with other approved products, which support the S/MIME standard with X.509 certificates or the OpenPGP standard for the exchange and storage of public keys.

2.5   Operating Modes

The GPG4Win and GPG4KDE software must be operated in the "VS-NfD conformity" mode of operation.

2.6   Installation, System Integration and Configuration

Requirements for the installation and the integration of GnuPG VS-Desktop in a system and for the system-specific configuration are given in the Operating/User Manual (Reference H1). The SAA and the CISOA are responsible to verify the implementation of these requirements during the installation, configuration and accreditation.

In addition to the installation, integration and configuration instructions described in the approval manual the following requirements are to be observed and complied with:

- During the first initialization, the administration, installation and configuration of the software must be carried out in a secure area by authorized personnel.

- Prior to the installation, the integrity of the installation package which was downloaded from the website is to be checked. To this end, a SHA-256 hash value is to be determined via the installation package by means of an appropriate tool.

- The currently valid hash value will be provided by BSI (Annex A).

- As regards the installation and administration of computers on which GnuPG VS-Desktop is used there must be a separation between user and administrator at the operating system level. In this context, the administrator is responsible for the installation of the product and the execution of the respective options for the approved version by means of group policies.

2.7   Operation

Requirements for the operation of GnuPG VS-Desktop are given in the Operating/User Manual (Reference H1).

Further requirements are as follows:

1. No malware on the computers that are used

    The systems on which GnuPG VS-Desktop is used must be free of malware.

2. Use of certificates of the administration PKI or a comparable PKI for the S/MIME standard

    By using a PKI and implementing it within the scope of the applicable policy (which encompasses the certification authority up to the participant) it is ensured that signatures, encryption and authentication can be employed in a trustworthy manner. As regards the use of the GnuPG VS-Desktop product in accordance with the S/MIME standard for the protection of the RESTREINT UE/EU RESTRICTED or NATO RESTRICTED classification a PKI must be used which meets the requirements of the TR-03145-VS-NfD Secure CA operation.

3. Verification of certificates subject to revocation for the S/MIME standard

    An important security measure is the verification of a certificate prior to its use – and subject to revocation – by retrieving certificate revocation lists (CRL) or making OCSP requests at the issuing CA. Certificates that are declared invalid will be marked accordingly by the issuing certification authority. The verification which is subject to revocation should always be performed prior to using a certificate and should, if possible, be specified in the group policies applicable to all users.

4. Certificates for the S/MIME standard and certificate revocation lists may among others be retrievable via LDAP

Certificates and certificate revocation lists are issued by CAs in directories. There, they can be searched and retrieved among others by the "LDAP" (Lightweight Directory Access Protocol). Access to the directory is to be configured by the IT administration.

5. Selection of the cryptographic algorithms for the OpenPGP standard

When creating an OpenPGP key pair, the user can choose between RSA (3072 bit) and ECDSA / EdDSA with Brainpool curves (256 bit).

6. Receiving OpenPGP certificates Certificates / keys

When using keys in OpenPGP format, the user is responsible for the authenticity of the key. Before using an OpenPGP key certificate for the first time, the user must ensure the authenticity of the certificate, especially if he did not receive the certificate personally from the owner, but if he received it, for example, via a key server, in an email attachment or received by a third party. To check the authenticity of the certificate, the recipient of a certificate can contact the holder by telephone to compare the fingerprint of the key contained in the certificate. The fingerprint can be displayed in the Kleopatra certificate manager (see illustration).
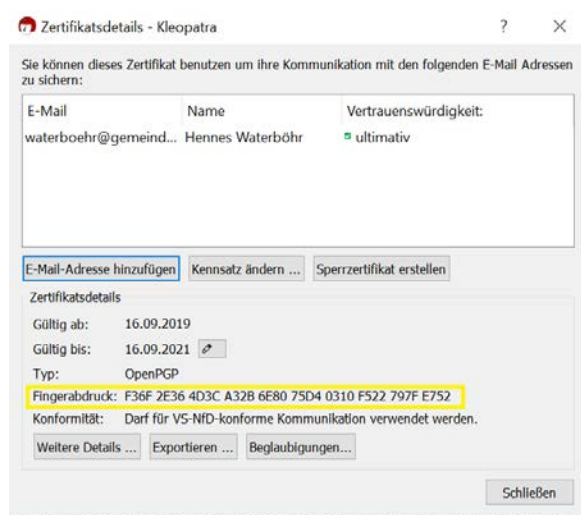

Figure 1 –Certificate details – Kleopatra

7. Selection of the cryptographic algorithms for the S/MIME standard

By means of the used PKI (such as the "Bundeswehr PKI" or the administration PKI) cryptographic algorithms are specified by the S/MIME standard. As regards GnuPG VS-Desktop these are preset by the manufacturer.

Options to choose must not be provided to the users and must be excluded by the IT administration by means of a pertinent product configuration.

8. Symmetrical encryption and decryption using passwords

Strong passwords should be used for symmetrical encryption and decryption using passwords. A password should consist of at least 20 randomly chosen characters. The components of the password must not be in any dictionary. (Note: It is legitimate to write down the password and keep it as safe as RESTREINT UE/EU RESTRICTED or NATO RESTRICTED.)

Passwords with which RESTREINT UE/EU RESTRICTED or NATO RESTRICTED data are encrypted must themselves be classified at least as VS-NfD.

The exchange of passwords must take place in a confidential way. Passwords with the classification RESTREINT UE/EU RESTRICTED or NATO RESTRICTED must be exchanged

- in a personal contact,

- via an encrypted connection approved at least for RESTREINT UE/EU RESTRICTED or NATO RESTRICTED (telephone, fax or data transmission),

- by post; mainly in a sealed envelope or as insured letter.

RESTREINT UE/EU RESTRICTED or NATO RESTRICTED classified passwords should not be exchanged over the phone.

Under no circumstances may a password be sent unencrypted over the Internet (e.g. as an e-mail). If a password is not given personally, the sender must telephone the recipient to inquire about the correct receipt of the password before using it for the first time for encryption.

9. Root certificates not changeable by the user

   Certificates of Root CAs have a special function as regards the verification of certificates. If the root certificate is accepted by the user, all other certificates that are arranged in the hierarchy below will indirectly be accepted as well. Thus to accept a root certificate constitutes a security-critical step as regards the use of products for electronic signature and encryption.

   Only the IT administration should be able to root and/or change these root certificates in the email client and/or in Kleopatra, i.e. they should be stored in an integrity-protected manner. The IT administration must decide whether the import of further root certificates will be allowed to the user on his own authority.

10. Unencrypted storage of emails on the server

    Unencrypted emails may only be stored in environments suitable for RESTREINT UE/EU RESTRICTED or NATO RESTRICTED.

11. Taking account of the selected email addresses

    In the address file of the email client the user usually stores, apart from the internal addresses of the respective organization also addresses of external communication partners. In case of congruences between synonyms under which the internal and external address is stored in the address file (e.g. if there is a "Ms Mueller" as an internal entry and as an external addressee – and both exist in the address file) there is a danger of confusion when choosing an addressee.

    Thus the user must carefully check both the recipient address and the associated keys and make sure that no confusion has occurred.

12. Signing automatically

    In the email client the setting"sign messages automatically" should always be active.

13. Avoiding HTML contents

    HTML contents should, as a matter of principle, not be displayed in the email clients Outlook and/or Kontact. The feature of reloading external contents must be turned off.

14. Use as backend in automated solutions (command line)

    When used as a backend in automated solutions, it must be ensured that the necessary passphrase for decryption, signature or symmetric encryption is passed securely. For this purpose, the use of the "--passphrase" option is explicitly excluded. Only the "--passphrase-fd" and "--passhrase-file" options may be used. Alternatively, a dedicated pinentry module may be used.

15. when decrypting data via the command line interface, it must be ensured that the corresponding status messages are output and evaluated via the "--status-fd" option. It must be ensured that plaintext is accepted only if its output is evaluated by the status messages

    [GNUPG:] BEGIN_DECRYPTION

[GNUPG:] END_DECRYPTION

is framed. Furthermore, it must be checked whether between the above status messages also the messages

[GNUPG:] DECRYPTION_OKAY

and

[GNUPG:] DECRYPTION_COMPLIANCE_MODE 23

occur. The DECRYPTION_COMPLIANCE_MODE 23 indicates the VS-NfD compliant state. Other status messages can be ignored. These requirements can be conveniently ensured by using the GPGME library. After successful decryption, the "is_de_vs" field of the gpgme_decrypt_result_t data object must also be evaluated. This field only has the logical value "True" if the message was encrypted in a VS-NfD compliant manner. When checking signatures, the "is_de_vs" field of the gpgme_signature_t data object must be considered accordingly. These requirements can also be met by using the auxiliary application "gpgme-json". This application provides a JSON based interface to GPGME.
To ensure VS-NfD compliance and secure implementation of such an automation solution, the creator is recommended to have the integration assessed by the GnuPG VS-Desktop vendor.

16. Observation of the instructions given in the user documentation and the release notes

    The user manual ("Gpg4win compendium") and the release notes contain important instructions on how to deal with the product as well as on how to interpret warning and error messages. In particular the instructions on the configuration and secure use of the GnuPG VS-Desktop product for the protection against attacks known under the term "Efail" under CVE-2017-17689 are to be observed.

2.8   TEMPEST/EMSEC

2.8.1   Protection of Classified National Information

There are no special TEMPEST/EMSEC requirements for the protection of national information classified VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) or corresponding national classification levels (RESTRICTED) with GnuPG VS-Desktop.

2.8.2   Protection of Classified EU Information

There are no special TEMPEST/EMSEC requirements for the protection of information classified RESTREINT UE/EU RESTRICTED with GnuPG VS-Desktop.

All other applications which require a risk assessment of the intended application and usage scenario in accordance with the EU requirements model, which is explained in reference E5 (considering threat and impact level), do also require a verification of the compliance to EU TEMPEST/EMSEC requirements (references TE1, TE2, TE3, TE4).
As already stated in section 1.1, the verification shall be done by the CAA together with the responsible SAA. Depending on the application and the usage scenario additional TEMPEST/EMSEC measures may be required.

2.8.3   Protection of Classified NATO Information

There are no special TEMPEST/EMSEC requirements for the protection of information classified NATO RESTRICTED with GnuPG VS-Desktop.

All other applications which require a risk assessment of the intended application and usage scenario in accordance with the NATO requirements model which is explained in reference N3 (considering threat and impact level), do also require a verification of the compliance to NATO TEMPEST/EMSEC requirements (references TN1, TN2, TN3, TN4).

As already stated in section 1.1, the verification shall be done by the NCSA together with the responsible SAA. Depending on the application and the usage scenario additional TEMPEST/EMSEC measures may be required.

3   SECURITY MANAGEMENT

3.1   Responsibilities

The CIS Security Officer, the System Administrator, as well as the Crypto Custodian are responsible for the implementation of the requirements in their area of responsibility. The SAA shall include these requirements appropriately into the accreditation documentation und check the correct implementation in the course of the system accreditation.

3.2   Description of the Security/Key Management

The Security/Key Management for GnuPG VS-Desktop is described in the Operating/User Manual (Reference H1).

3.3   Quantum Computer Resistance

Please note that the product in the approved configuration uses cryptographic mechanisms that are not quantum computer resistant.

4   SECURITY CLASSIFICATIONS

4.1   Security Classification List

The classification levels for control and safeguarding GnuPG VS-Desktop and ancillaries are defined by the security classification list included as Annex B.

If Annex B lists items which can optionally be handled as CCI (COMSEC Controlled Item/Controlled Cryptographic Item) the requirements given for CCI in Reference E4, resp. N2, shall be applied. Nations or organisations not able to accommodate CCI control requirements shall not choose this option.

5   ACCOUNTABILITY AND CONTROL

5.1   Sale, Loan and Export

There are no restrictions for sale, loan and export of GnuPG VS-Desktop.

5.2   Declaration of Compliance (DoC)

GnuPG VS-Desktop only uses Type B-Algorithms. For that reason, it is not required to sign a Declaration of Compliance (DoC) for GnuPG VS-Desktop.

5.3   Accountability and Control

Accounting is not required for GnuPG VS-Desktop.

6   PHYSICAL SECURITY

6.1   Responsibilities

This section describes the security relevant aspects regarding the use of GnuPG VS-Desktop. The strict adherence to the instructions given in this document is required to permanently ensure security of the classified information, which is protected with GnuPG VS-Desktop. The Security Officer and the Crypto Custodian, as well as the CIS Security Officer are responsible for the implementation of the requirements in their area of responsibility. The SAA shall include these requirements appropriately into the accreditation documentation und check the correct implementation in the course of the system accreditation.

6.2   Requirements

If EU- and/or NATO classified information will be protected with GnuPG VS-Desktop, the respective provisions of references E1-E4 and N1-N2 apply. In addition, the security regulations listed hereinafter shall be applied.

6.2.1 General

Security protection for GnuPG VS-Desktop shall be afforded according to the classification levels and markings given in Annex B.

- GnuPG VS-Desktop shall only be used and operated by authorised personnel, who hold a user chip card and the appropriate User Access Code (UAC).
- During operation GnuPG VS-Desktop shall be protected against unauthorized access, to avoid any misuse which could cause a disclosure of the confidentiality or a violation of the integrity or authenticity of the protected information and to avoid any violation of the integrity of GnuPG VS-Desktop.
- GnuPG VS-Desktop shall be inspected by the Security Officer (or a competent body authorized by him) visually at regular intervals, not exceeding one year.
- Each apparent manipulation or external damage to the hardware shall be reported to the Security Officer immediately (see Chapter 10).

6.2.2 Installed Product

The security classifications and handling requirements given in the Security Classification List in Annex B shall be met.

6.2.3 Storage and Transport

There are no special requirements for storage and transport of GnuPG VS-Desktop.

6.2.4 Handling of Key Material

The following requirements shall particularly be noted by the Crypto Custodian and the End User.

The requirements for the handling of key material for the protection of classified EU- and NATO-information are given in References E4 and N2.

6.3 Product Protection Mechanisms

GnuPG VS-Desktop does not have any special protection mechanisms.

6.3.1 Reporting and Measures

Recommendations for reporting of any COMSEC incidents or suspected COMSEC incidents and measures to be taken, when the product is tampered or MEPs are missing, damaged or broken, are given in Chapter 10.

6.4 Routine Destruction

The instructions listed below are mainly tasks of the Crypto Custodian and the CIS Security Officer.

6.4.1 Deletion/Destruction of stored Keys/Certificates

Smartcards that are no longer in use can still be used in similar application scenarios by the same user. Prior to this, old key material must be actively overwritten by new initialization.

6.4.2 Product Disposal and Destruction

There are no special requirements for the disposal or destruction of GnuPG VS-Desktop.

Smartcards definitely no longer used or defect smartcards are to be securely destroyed (e.g. by cutting up the smartcard chip crosswise).

After the decision has been taken to no longer use a smartcard, it is to be ensured that this card cannot be used until its final destruction. This can be effected by technical and/or organizational measures.

7 PERSONNEL SECURITY

In addition to the requirements described in references E1-E4 and N1-N2, the following security requirements apply for GnuPG VS-Desktop.

7.1 Responsibilities

The requirements concerning personnel security and authorisation shall be considered and implemented by the Security Officer and the CIS Security Officer.

7.2 Clearance and Authorisation

Only personnel authorised and cleared to handle classified and crypto material according to the respective security classifications and markings given in Annex B, shall be permitted to install, operate (use) and store GnuPG VS-Desktop.

7.3 Need-To-Know

The access to GnuPG VS-Desktop shall be limited according to the need-to-know principle.

8   MAINTENANCE AND REPAIR

The following requirements shall be met for the maintenance and repair of GnuPG VS-Desktop.

8.1   Responsibilities

Normally the CIS Operational Authority (assisted by the Crypto Custodian, the CIS Security Officer and the CIS Administrator) and the manufacturer are responsible for the implementation of these requirements in their area of responsibility.

8.2   Requirements and Measures

The administrator should inform himself about updated versions of the product at regular intervals and install them where appropriate.

Prior to updating a software it is to be examined whether there is a BSI security statement available for it.

Maintenance of the computers and software updates may only be carried out by authorized and trained personal.

9   EMERGENCY PROCEDURES

9.1   Responsibilities

Normally the CIS Operational Authority, the Crypto Custodian, the CIS Security Officer, the CIS Administrator and the End User are responsible for the implementation of these requirements in their area of responsibility.

9.2   Emergency Action Plan

Safeguarding of GnuPG VS-Desktop and associated cryptomaterial under emergency conditions shall be addressed in an Emergency Action Plan, which describes the measures to be taken in the case of an emergency condition.
EU and NATO requirements for an Emergency Action Plan are mandated by references E4 and N2.

9.3   Zeroization

GnuPG VS-Desktop does not impose any special requirements with regard to this work item.

10 COMSEC INCIDENTS

10.1 Contact person of the operator

The CIS Operational Authority or End User ofGnuPG VS-Desktop shall communicate to the manufacturer the name and further details a point of contact (e.g. the CIS security officer/security officer) for receiving security related information. This data shall be kept up to date. The manufacturer will use this point of contact only for forwarding information on possible security incidents, necessary security measures, security relevant product updates, and approval updates.

10.2 Reporting obligation and responsibilities

The CIS Operational Authority and the SAA (assisted by the CIS Security Officer) are responsible for the investigation and reporting of COMSEC insecurities and incidents.

10.3 COMSEC Insecurities and Incidents

A general listing of reportable COMSEC insecurities and incidents and the standards for reporting them are contained in references E4 and N2. In the EU context, the BSI acts as the CAA and in the NATO context as the NCSA.

10.4 Measures in case of BSI warning

In the case of discovered vulnerabilities of the product or discovered security problems in its operational environment, the BSI communicates warnings and notices, usually associated with measures to be implemented (e.g. immediate update obligation, exchange of certificates, change in the configuration of the product, change in the conditions of use and operation, etc.).

These warnings and instructions are sent by the manufacturer to the contact person of the operator named in 10.1.

These instructions must be followed.

10.5 Reporting and Compromise Recovery

The Requirements for Reporting COMSEC Incidents, given in references E4 and N2, shall be applied.

11 POINTS OF CONTACT

11.1   Manufacturer

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

Intevation GmbH
Neuer Graben 17
49074 Osnabrück
Germany
https://intevation.de
Email: intevation@intevation.de

Inquiries and support: vsnfd@gpg4win.org

11.2   BSI Crypto-Support

When a manipulation of GnuPG VS-Desktop is detected or suspected the BSI shall be contacted immediately, giving only the name of the product and a point of contact.

Further information about the nature of the insecurity or incident shall be exchanged by secure means.

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

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

11.3   Approval Related Questions

For questions concerning the approval of GnuPG VS-Desktop we would like to refer to the FAQ list on our webpage (only available in German language):
https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/FAQ-Evaluierung-und-Zulassung/faq-evaluierung-und-zulassung_node.html

Questions (not classified and not sensitive) can also be raised to the BSI sending a message to the following E-Mail address:

E-Mail: zulassung@bsi.bund.de

ANNEX A
APPROVAL AND DESIGN STATUS
GnuPG VS-Desktop, Version 3.x
Approval-ID BSI-VSA-10584

1 Approval

GnuPG VS-Desktop, 3.x is nationally approved by the Bundesamt für Sicherheit in der Informationstechnik (BSI) with the Approval-ID BSI-VSA-10584, dated 01.06.2021, for the protection of information classified VS - NUR FÜR DEN DIENSTGEBRAUCH.

The approval includes an approval for the protection of EU information classified RESTREINT UE/EU RESTRICTED/requiring protection with an (EU) SoM level STANDARD and which is handled or transmitted in national CIS.

The approval includes an approval for the protection of NATO information classified NATO RESTRICTED requiring protection with a (NATO) Strength of Mechanism (SoM) level STANDARD.

The requirements of the Security Operating Procedures (SecOPs) shall be met.

In the following the current design status of the approved version of GnuPG VS-Desktop is listed. The design status is recorded for each approved version of a product and is an integral part of the approval documentation.

2 Verification of the Design Status

The manufacturer is responsible for the delivery of GnuPG VS-Desktop with the approved design status, and the correct version and configuration. Prior to installation and operation of the delivered GnuPG VS-Desktop the design status shall be checked and verified by the CIS Operating Authority, to ensure it is compliant with the approved design status listed below. In any case, prior to initial operation, the CIS Operating Authority shall ensure that the product to be installed is approved and has got an "Approval to Operate (ATO)" by the SAA for the type of classified information (e.g. NATO, EU, national) and the classification levels to be protected.

3 Design Status Deviations

If any deviations are found between the design status listed here and the one delivered, the Points of Contact listed in Section 11 of the main part of this document shall be consulted in order to clarify the situation.

4 Design Status

The approved design status of GnuPG VS-Desktop is listed below. The design status is recorded for every approved product version and is an integral part of the approval documentation.

The approval relates to the following version:

No.	Software
1	Version 3.x, starting with subversion 3.1.15 and the following

Usually, Gpg4NfD NfD is delivered from the manufacturer to the end user with the following system and accessory components:

1. Gpg4win 3.1.15 (gpg4win-3.1.15.exe)
   SHA256: 58b4de192ce0f3a7f25766e96ec379a8f125e3a1e2bdb2519c185a03a0a4ed4c

   Gpg4win 3.1.16 (gpg4win-3.1.16.exe)
   SHA256: c499213ff3e14e93c3b245546994cc0e654ec267b40a188788665ae8f4e9f5ad

2. The software packages of the Gpg4win and Gpg4KDE products are signed by the public OpenPGP key of the GnuPG project which can be obtained under the URL
   https://gnupg.org/signature_key.html

ANNEX B
SECURITY CLASSIFICATION LIST
GnuPG VS-Desktop, Version 3.x
Approval-ID BSI-VSA-10584

		Security Classification[12]		No Security Classification[1]	Remarks
		VS-V/NC/ C-UE/EU-C	VS-NfD/NR/ R-UE/EU-R		
1	GnuPG VS-Desktop SW installation medium			X	1)
2	GnuPG VS-Desktop, installed, ready for operation		X		
3	GnuPG VS-Desktop, "off" mode, key loaded		X		2)
4	GnuPG VS-Desktop, "off" mode, key deleted		X		2)

1)   The installation medium is not classified, but its integrity is to be protected.

2)   A person-related maintenance of records is not required.

Abbreviations of Classifications/Markings:

Germany	NATO	EU
VS-V (VS-VERTRAULICH)	**NC** (NATO CONFIDENTIAL)	**C-UE/EU-C** (CONFIDENTIEL UE/EU CONFIDENTIAL)
VS-NfD (VS-NUR FÜR DEN DIENSTBEGRAUCH)	**NR** (NATO RESTRICTED)	**R-UE/EU-R** (RESTREINT UE/EU RESTRICTED)
-	**CCI** (Controlled Cryptographic (COMSEC) Item)	**CCI** (Controlled Cryptographic (COMSEC) Item)

When national classified information is protected, the national security classification corresponding to the German security classification, as agreed in the nation's general security agreement with Germany shall be applied.

---

1 National crypto material according to §59, Sec. 1 VSA are products, devices, and respective documents as well as key material for the decryption, encryption, and transmission of information defined as such by the BSI.
Sec. IX, VSA defines that Crypto material shall be handled by the Crypto Custodian.
§59, Sec. 2 VSA states classified crypto material shall be labeled as "CRYPTO"/"KRYPTO", or – lacking a classification - as "CCI". The warning "CCI" shall be entered instead of "X" in the column **No Security Classification** and the warning "CRYPTO"/"KRYPTO" in the other columns.
2 When using the product for the protection of NATO / EU classified information the corresponding international classification levels and markings are valid.