Federal Office
for Information Security

GRP: Zulassungsstelle BSI

Digital unterschrieben von GRP: Zulassungsstelle BSI
Datum: 2023.01.18 14:26:02 +01'00'

Security Operating Procedures and Operational COMSEC Doctrine

SINA L2 Box S, Versions 3.3.2, 3.3.3

BSI-VSA-10722

Issued: 23.12.2022

Suitable for protecting: RESTREINT UE/EU RESTRICTED
NATO RESTRICTED

EU - NATO - Multi National Version

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: zulassung@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

Annexes

Annex A - Approval and Design Status

Annex B - Security Classification List

Figures

Tables

Blank Page

FOREWORD

This Doctrine and Information Publication - Operational COMSEC Doctrine and Security Operating Procedures (SecOPs) for the SINA L2 Box S 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 SINA L2 Box S and its associated security management and documentation.

This publication complements the User Manual of the SINA L2 Box S 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.

For reasons of better readability, the simultaneous use of female, male or other forms of language for the individual parties and instances is dispensed with and the generic masculine is used. All references to persons and roles apply equally to all genders.

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 the SINA L2 Box S 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.

The SINA L2 Box S 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 SINA L2 Box S, its security management, ancillaries, and documentation hereinafter referred to as SINA L2 Box S.

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 SINA L2 Box S 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 the SINA L2 Box S.

1.3 Prerequisite

A prerequisite for the purchase, lease, loan and use of the SINA L2 Box S 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 the SINA L2 Box S 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 the SINA L2 Box S is used to protect national classified information or the SINA L2 Box S is used by an EU- and/or NATO-Nation outside the EU- or NATO-context, the referenced EU-, resp. NATO-documents shall be applied mutatis mutandis.

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**	Crypto and Comsec Material Management (TECH-I-01) of 15 January 2007 (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**	AC/322-D/0048-REV3 - Technical and Implementation Directive on CIS Security (NATO UNCLASSIFIED)
N5	**AC/322-D(2012)0011**	AC/322-D(2012)0011 - INFOSEC Technical and Implementation Directive on Downgrading, Declassification and Destruction of System Equipment and Storage Media (NATO RESTRICTED)
N6	**AC/322-D(2012)0012**	AC/322-D(2012)0012 - INFOSEC Technical and Implementation Guidance on Downgrading, Declassification and Destruction of System Equipment and Storage Media (NATO RESTRICTED)
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-10722, dated 23.12.2022, incl. Annexes
A2	**EU-Approval**	Approval for the protection RESTREINT UE/EU RESTRICTED is granted by the national approval document (see Reference A1)
A3	**NATO-Approval**	Approval for the protection NATO RESTRICTED is granted by the national approval document (see Reference A1)
	Operating Manuals/Handbooks	
H1	**SINA L2 Box S, Versions 3.3.2, 3.3.3 Manual**	SINA L2 Box S, Versions 3.3.2, 3.3.3 installation- and configuration manual, Version 3.3.2/3.3.3

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 (EU terminology; in Germany the BSI)
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	
TFS	Traffic Flow Security, prevents the recognition of traffic patterns or traffic at all on the encrypted interface.
AAD	Additional Authenticated Data (signed but not encrypted parts of user data)
MTU	Maximum Transmit Unit (maximum allowed packet size of the network)
Crypt-Engine	A part of the atmedia firmware that controls the crypt functionality of the encryptors

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
    - defining the business and operational requirements, operating principles and concept of operation of a CIS, including the information exchange requirements;
    - 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;
    - formally accepting the residual risk, if applicable, resulting from the security risk assessment process and agreeing on a plan to manage the residual risk;
    - 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;
    - conducting operational evaluation of the CIS and validating/authorizing the CIS for operational use, once the security accreditation is granted by the SAA
    - 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
  - providing CIS Security advice to, and maintaining CIS Security awareness of, CIS administrators and users, including managers;
  - 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;
  - checking the implementation and maintenance of hardware, firmware and software modifications and enhancements to the CIS to ensure that security is maintained;
  - 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;
  - checking security related logs for event/process failure and unauthorised user and system activity;
  - conducting or coordinating the execution of periodic security risk and vulnerability assessment of CIS;
  - reporting to the SAA on any detected CIS security weaknesses and vulnerabilities;
  - 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.:
  - managing the cryptomaterial in his account to prevent loss or possible physical compromise;
  - 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;
  - maintaining COMSEC accounting;
  - conducting physical inventory checks;
  - 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.
  - performing routine and emergency destruction or disposition of cryptomaterial in accordance with approved methods;
  - ensuring that cryptomaterial is properly prepared and shipped;
  - verifying the contents of a shipment of cryptomaterial on initial receipt (completeness, physical integrity);
  - ensuring the integrity of cryptomaterial prior to use;
  - 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.
  - being familiar with current plans for the destruction, disposal, evacuation, or protection of cryptomaterial in the event of fire, disaster, or other emergency;

  - reporting immediately to the CIS Security Officer any known or suspected physical compromise, loss, or unauthorised destruction/disposal of cryptomaterial;
  - 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 atmedia GmbH of the approved CIS security product SINA L2 Box S 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:
  - providing advice and guidance on CIS Security policy and directives (and supporting security measures);
  - 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;
  - reviewing and approving security-related documentation;
  - performing a risk assessment and applying risk management for CIS being accredited;
  - providing a statement of security accreditation resp. re-accreditation for CIS and stating the conditions and activities which have to be applied for use;
  - performing periodic security inspections or reviews in accordance with the security accreditation process;
  - 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;
  - providing advice/recommendations on corrective measures to be implemented (or recommending sources for appropriate advice);
  - 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;
  - liaising with other SAAs in respect to interconnected CIS for such purposes as agreeing System Interconnection Security Requirement Statements (SISRS) or national equivalent;
  - providing advice on the interconnection of CIS handling classified information to any CIS;
  - 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
  - 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;
  - verifying the security accreditation statements for any CIS in use to ensure that they achieve and maintain an appropriate security accreditation status;

- 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

In addition to Layer 2 Ethernet networks, the SINA L2 Box S, Versions 3.3.2, 3.3.3 also secure connections over any MPLS, IPv4 or IPv6 networks from a few Mbit/s up to 100 Gbit/s transparently and at line speed.

Application scenarios are site couplings and data center connections in the LAN, MAN and WAN area.

In combination with Traffic Flow Security mode (TFS), the connection can be additionally protected against traffic analysis and unwanted data leakage. In all transmission modes, data is protected against eavesdropping, manipulation and replay using AES-256 GCM.

The network and encryption functionality is realized by programmable FPGA hardware and completely designed and implemented in Germany.

2.2 System Components and Function

As a standard, the manufacturer will deliver the SINA L2 Box S to the end-user with the following system, components and ancillary equipment (see also Manual (reference H1)):

> **NOTE:**
>
> The end-user shall check the completeness and integrity of the delivered system components and ancillary equipment immediately upon receipt of the SINA L2 Box S.
>
> Especially the completeness and integrity of TAMPER Detection Stickers (MEPs) shall be checked, if applicable. In case of any damage of a component or a security seal, the procedures in chapter 10 shall be followed.

Accessories:

- 2 AC power cords (inlet connector for non-heating apparatus) or external power supplies with AC and DC cables.
- 1 crossover serial cable (null modem cable)
- Rack mount kit incl. manual for rack mounting (19“ devices only)
- Optional: SFP/SFP+/QSFP+/QSFP28 interface modules
- CE Declaration of Conformity

Integration into the network

Line modes

The SINA L2 Box S, Versions 3.3.2, 3.3.3 offers two different classes of line modes. On the one hand, private networks can be transparently coupled via any public Layer-2 or IP networks at Layer-2 level. Here, the private Ethernet frames are embedded in a Layer-2 or IP transport frame and thus tunneled over the public network without revealing any private information (such as MAC addresses, IP addresses and packet sizes). This routing mode is called "GCM tunnel" for Layer 2 transport frames and

"GCM-IP tunnel" for IP transport frames, and can only be used for point-to-point connections. It also provides the option of nearly offsetting the overhead due to encryption by aggregating Ethernet frames to achieve maximum encrypted line throughput.

The second class of line modes makes parts of the private Ethernet header, such as the MAC or IP addresses, VLAN tags or MPLS stacks, visible on the public network, allowing network components on the public network to make routing decisions or maintain a desired quality-of-service through prioritization. These modes are suitable for both point-to-point and multipoint applications. Depending on whether Layer 2 or IP header information is to be visible, the "GCM" or "GCM-IP" routing mode can be used. In multipoint networks with client separation, the "GCM-VLAN" and "GCM-IP-VLAN" modes are available accordingly. In all cases, the publicly visible header information can be secured against manipulation (AAD).

All line modes always encrypt data at Layer-2, although exception rules from encryption can evaluate information from Layer-2 and Layer-3. Section 2.5 explains in detail how the different modes work and how they behave on the line.

Processing of Ethernet and IP packets

Line mode gcm

The line mode "gcm" is the standard line mode for Layer-2 networks and encrypts the payload of the Ethernet frame and leaves the Ethernet header partially or completely unencrypted.

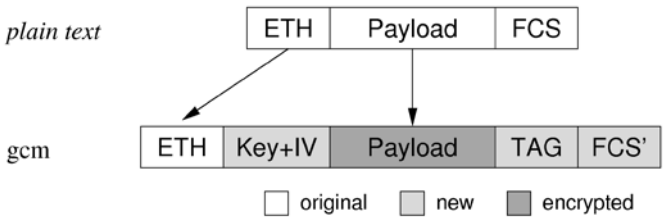

Figure 1: Processing of data packets (mode gcm)

Line mode gcm-ip

The "gcm_ip" mode handles non-IP frames like the "gcm" mode, but for IP packets it makes parts of the IP header visible by inserting a new IP header in the public network. Only selected fields such as the IP version and IP addresses of the private header are included in the new IP header. This allows routing based on IP addresses in the public network without revealing the full header information and at the same time secures the full IP header against tampering.

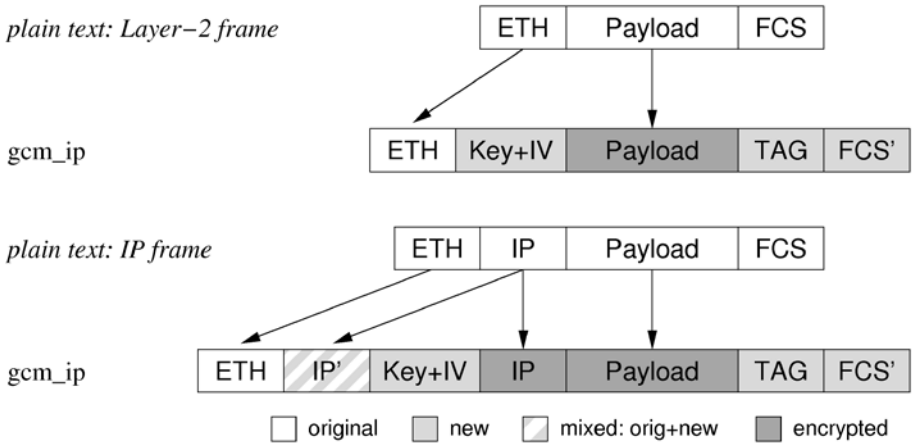

Figure 2: Processing of data packets (mode gcm_tunnel)

Line modes gcm_tunnel and gcm_ip_tunnel

The line modes "gcm_tunnel" and "gcm_ip_tunnel" offer a direct and transparent layer 2 coupling over any Ethernet respectively IP network. All data of the Ethernet frame including the header are encrypted and then packed into a new Ethernet transport frame.

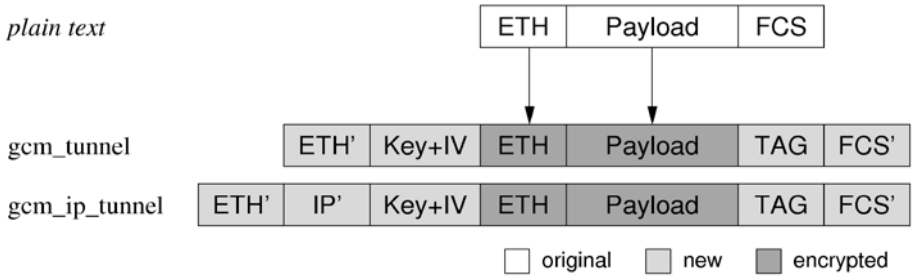

Figure 3: Processing of data packets (mode gcm_ip_tunnel)

The connections of the approved hardware are described in the user manual (reference H1).

2.3 Approval and Approved Design Status

The type of the approval and the currently approved design status of the SINA L2 Box S 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

The SINA L2 Box S are fully interoperable across approved hardware platforms in the multipoint operating modes. Since proprietary crypto technology and key management is used, they are not interoperable to IPSec or MACSEC solutions.

2.5 Operating Modes

Line operating modes

The crypt devices offer two different classes of line modes. On the one hand private networks can be transparently connected via arbitrary public Layer 2 or IP networks. In this case the private Ethernet frame is embedded into a Layer 2 or IP transport frame and is tunnelled via the public network without any visible private information like MAC addresses, IP addresses or packets sizes. If Layer 2 transport frames are used, this line mode is called “gcm-tunnel”. If IP transport frames are used, this line mode is called “gcm-ip-tunnel”. Both line modes can be used for point-to-point connections. This line mode offers an option for combining Ethernet frames, nearly eliminating the encryption overhead in most cases. As a result data private networks can be connected via arbitrary networks and in most cases with nearly the same throughput like without encryption.

On the other hand there is the second class of line modes that keeps parts of the private Ethernet header visible in the public network, like for example the MAC or IP addresses, VLAN tags or MPLS stacks, enabling network components in the public network to take routing decisions or fulfil quality of service requirements by prioritizing the traffic. These modes can be used for point-to-point scenarios and for multipoint scenarios as well. Depending on whether there should be Layer 2 or IP header information be visible, either the “gcm” line mode or the “gcm-ip” line mode can be used. In

multipoint scenarios with multi tenant support the line modes “gcm-vlan” and “gcm-ip-vlan” can be used. In all cases public visible header information can be secured against manipulation.

Point-to-point mode

The point-to-point mode can be used for all those scenarios, where the private LAN networks of two different sites are connected via a public link. This can be either a connection via a dark fibre link (or a wave length link of a WDM system) or any public layer 2 or IP standard network. According to the security requirements and the operation mode of the public network one of the following four modes can be used: “gcm”, “gcm_ip”, “gcm-tunnel” or “gcm-ip-tunnel”. The tunnel modes reveal absolutely no information about the encrypted Ethernet frame, whereas in the other two modes parts of the private header are transferred in plain over the public link, in order to allow routing or prioritizing in the public network. Apart from higher confidentiality the tunnel modes offer an option for being compliant with an MTU in the public network. In addition this mode offers the possibility to combine Ethernet frames before the transport, which results in a transparent coupling of the private network on layer 2 level without having a negative impact on throughput based on the encryption in most cases.

Figure 4: Mode point-to-point

Multipoint mode

In multipoint mode, different network topologies can be secured. The classic deployment scenario is the coupling of the private LAN networks of several sites via any public Ethernet or IP network. This coupling can be done on an equal or prioritized basis using VLAN networks and MPLS routing. Depending on the bandwidth requirements, Fast Ethernet, Gigabit Ethernet or 10/40/100 Gigabit Ethernet, also mixed as desired, can be used at the individual locations.

Data is encrypted in "GCM" or "GCM-IP" mode, which ensures that the MAC, IP or MPLS headers required for switching or routing the data packets in the transport network are retained in plain text. Within a multipoint group, devices use a common line key to encrypt and decrypt data, allowing any-to-any communication for unicast as well as multicast and broadcast frames. The line keys are generated and negotiated by specially configured encryption devices (keyservers), which distribute the key material to all members of the group.

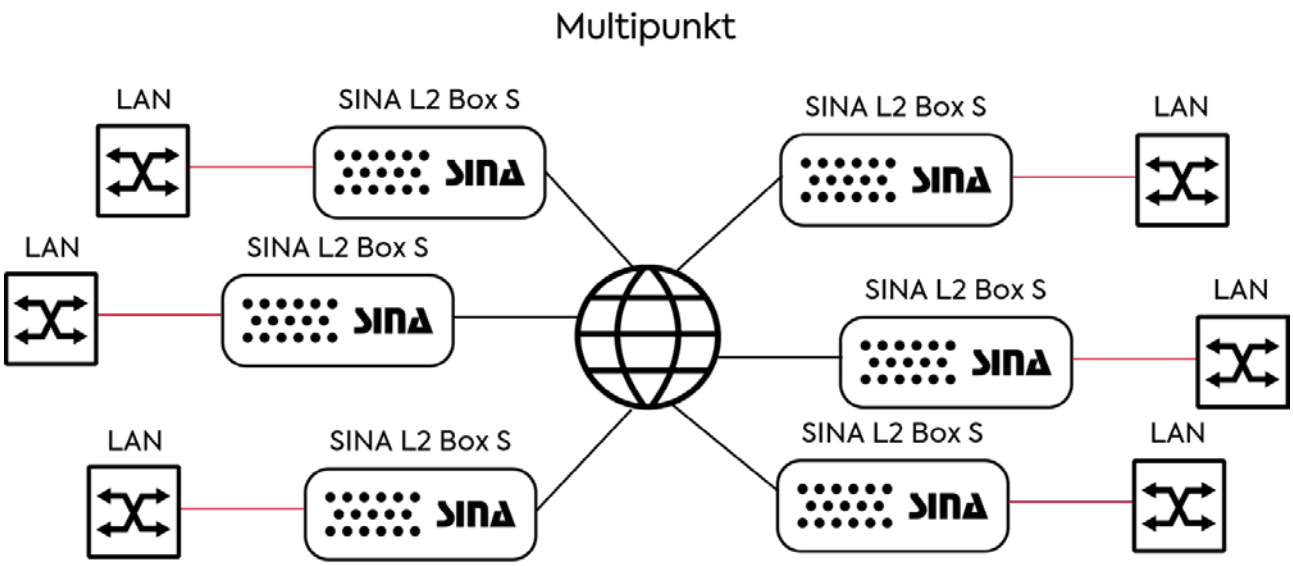

Figure 5: Mode multipoint

Operating conditions

The SINA L2 Box S, Versions 3.3.2, 3.3.3 can operate in these operating modes:

stop

Stops the Crypt engine and blocks transmission of data.

plain

Starts the Crypt engine and activates the plaintext mode (all data lead through without encryption).

crypt (only in point-to-point mode)

Starts the Crypt engine in point-to-point mode and activates the crypt mode. No authentication with the opposite site is performed, but manually chosen master keys are used. This mode can only be used in expert-mode.

auth (only in point-to-point mode)

Performs an authentication with the opposite site in point-to-point mode and exchanges the master key and session key. Starts the Crypt engine and activates the crypt mode.

pasv (only in point-to-point mode)

Starts the Crypt engine in the passive mode in point-to-point mode and waits for an authentication from the opposite site. Therefore it is not allowed to configure both devices of a connection to passive mode.

crypt_mp (only in multipoint mode)

Starts the Crypt engine in multipoint mode and activates the crypt mode. If valid registration data is available a client will try to logon at one or more configured servers. A server will start the key generation and key distribution (if properly configured).

plain_mp (only in multipoint mode)

Starts the Crypt engine in multipoint mode but activates the plaintext mode. If valid registration data is available a client will try to logon at one or more configured servers. A server will start the key generation and key distribution.

All data received from the private network will be sent in plaintext into the public network. In this mode a client will be able to decrypt received encrypted data from the public network, after receiving the key material from the server. All plaintext data received from the public network is sent into the private network.

crypt_mp_bypass (only in multipoint mode)

Starts the Crypt engine in multipoint mode and activates the crypt mode. If valid registration data is available a client will try to logon at one or more configured servers. A server will start the key generation and key distribution.

All data received from the private network will be encrypted and sent into the public network. In this mode a client will be able to decrypt received encrypted data from the public network, after receiving the key material from the server. All plaintext data received from the public network is sent into the private network.

This operation mode should only be used temporary during the setup of a multipoint network. For security reasons this mode should be immediately replaced by the “crypt_mp” mode after the setup has been properly finished!

Further information can be obtained from the user manual (chapter 5).

2.6 Installation, System Integration and Configuration

Requirements for the installation and the integration of the SINA L2 Box S in a system and for the system-specific configuration are given in the manual (reference H1). The SAA and the CISOA (or the IA Operational Authority, resp.) are responsible to verify the implementation of these requirements during the installation, configuration and accreditation.

- The initial installation and configuration of the crypt system must be done in secure environment by qualified and authorized personnel.
- The integrity of Tamper Detection Sticker (MEP) attached by the manufacturer must be checked before the device is deployed. The device must not be used if the MEP is damaged.

2.7 Operation

Requirements for the operation of the SINA L2 Box S are given in the Operating/User Manual (reference H1).

- The integrity of the MEP must checked on a regular basis. The device must be put out of operation if the MEP is damaged.
- The parameter „mode2“ configures if a „Run“-smartcard is needed for the operation of the device (set mode2 off|on|start). If not set to „off“, the mode Setting must not be set to „off“ either. If a device is NOT operated in a secure environment, mode2 must be set to „on“.

- The crypt mode aes256-gcm must be used.
- The AES crypto engine must be used with standard AES S-boxes.
- The setting for the ECC curve parameters for the ECDH key agreement have to be:
  - set ecc_curve = brainpoolP256t1|brainpoolP320t1|brainpoolP384t1|brainpoolP512t1 or
  - set ecc_curve = custom
  - if „set ecc_curve = custom“ is used, a curve parameter setting provided by the BSI must be used
- For point-to-point connections, the modes „GCM Tunnel“ or „GCM-IP-Tunnel“ shall be used when possible.
- It is advised to use tunnel modes and no transport modes in order to mitigate the risk of leakage of sensitive information of the private network. The sensitive information can be e.g. knowledge about infrastructure data obtained from unencrypted Ethernet headers. For technical reasons, the multipoint modes cannot use tunnel-mode but GCM or GCM-IP only. In this case, the operator is responsible for the risk remains described above.
- Enabling a container mode (mtu or tfs, if licensed) is recommended to reduce overhead and additionally if required to activate Traffic Flow Security (TFS) in order to complicate to analyze network traffic.
- For the AES-GCM block mode these settings must be used:
  - The GCM tag length must be at least 64 bit.
  - The Ethernet Payload must be integrity protected by the GCM tag and packets must be forwarded to the local (red) side after full verification of the integrity (<set delete = on>) only.
  - If possible in the network scenario used, the header data shall be protected with the AAD settings „dest+source“ or „on“. If this is not possible, the operator is responsible for the risk remains (spoofing of header data).
- The setting for the replay protection must be „3s”, „10s“ or „on“.
- The internal Firewall of the device has to be configured to allow access from authorized SINA Management stations only. Optionally, a closed SINA management network can also be released in the firewall.
- The configurable filter rules for passing unencrypted (plain) user data packets identified by a network source addresses or certain network services must be used only after consultation of the BSI or the manufacturer in order to prevent unintended bypasses of the crypt device.
- If SNMP is used for network monitoring, the IP addresses of authorised SINA Management stations have to be configured (SNMP Client). If possible, SNMP version 3 shall be used since SNMP versions 1 und 2 could leak sensitive information about the crypt system. The operator is responsible for the risk remains described above.
- The administration must analyse the logfiles at regular intervals (at least once a week). Attention has to be paid for security relevant events.
- The parameter „set l2sec“ hat to be set to „on“ or „ip“. During rollout and network deployment of the systems, the setting „mixed“ can be used.
- The administration of the crypt system must always be performed in a trusted environment by authorised and trained personnel.
- If all components (SINA L2 Box S, Versions 3.3.2, 3.3.3 und management) are installed in one trusted environment, the mode “secure” can be used for the network administration of the crypt system via the Ethernet management port.

- If the SINA L2 Box S, Versions 3.3.2, 3.3.3 and the SINA Management are connected via an open network, an administration in “secure” mode is allowed only if an VS-NfD approved encryption is used for the management connection.
- In all other cases, the administration is allowed in read only mode only.
- For each administrator user role, an individual password must be configured, known by the authorised user only.
- Personalised user roles have to be configured for all users which shall access the system in order to tie user actions logged in the system log to individual persons.
- The password based authentication must be disabled by setting „set pw_auth“ to „off“ and public key based authentication must by used only for management access.
- For the privileged modes (crypt, admin, mp, update ...), passwords must be configured.
- Only a SINA management or another management system approved by the BSI for use with SINA L2 Box S, Versions 3.3.2, 3.3.3 devices may be used for configuration by means of a smartcard. Only smartcards that have been explicitly created for a system may be used. Mandatory passwords for smartcards must be specified here, and these must be assigned accordingly when they are created. As value for the parameter <set password> the appropriate password must be set.
- In multipoint mode these settings must be used:
  - The parameter „mp set broadcast“ shall be set „off“ (round-robin distribution of individual master keys) for small networks with less than 16 clients. For larger networks, the more efficient distribution of keys via broadcasts can be used („mp set broadcast on“).
  - The <watchdog> monitoring of key exchanges („set watchdog on“) must be activated.
  - The parameters „add server <mp-id> l2sec“ resp. „add client <mp-id> l2sec“ have to be set.

2.8 TEMPEST/EMSEC

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 the SINA L2 Box S.

Protection of Classified EU Information

There are no special TEMPEST/EMSEC requirements for the protection of information classified RESTREINT UE/EU RESTRICTED with the SINA L2 Box S.

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.

Protection of Classified NATO Information

There are no special TEMPEST/EMSEC requirements for the protection of information classified NATO RESTRICTED with the SINA L2 Box S.

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

Requirements for the Security Management, resp. Key Management of the SINA L2 Box S, which are not already described in the Manual (reference H1), are described in the following.

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 management for the SINA L2 Box S is described in the Manual (reference H1). Additional descriptions and requirements are listed below:

- Key Management:
  - The lifetime of the Session Keys is limited to a maximum of 120 seconds.
  - The lifetime of the Master Keys is limited to a maximum of 12 hours.
  - The parameter for the key length of the (ECDH) Diffie–Hellman key agreement has to be at least 32 (256 bit) to guarantee a sufficient EC key length.
  - The Host Key must not be used for the inband management (setting <system>). A dedicated inband management key must be used and this key must be changed at least once a year, depending on key utilisation.
  - The lifetime of the Host Keys is limited to 1 month if (ECDH) Diffie–Hellman is not used. If (ECDH) Diffie–Hellman is used, the lifetime is limited to 4 months.
  - It is recommended to use Host Keys with an expiration date for point-to-point operation.
  - The Host Keys and the Inband Management Keys must be generated either by the BSI, with a SINA management station or with another management system approved by the BSI for use with the SINA L2 Box S, Versions 3.3.2, 3.3.3 only.
  - The Host Keys, the Device Keys and the Inband Management Keys must be zeroised if the device leaves the secure operating environment (repair, relocation).
- Emergency(Adhoc)-Authentication:
  - The Emergency-Authentication must only be used if there is no authorised administrator available for the configuration of Host Keys in case of a device replacement due to failure and a loss of the network connection cannot be accepted.
  - In point-to-point mode, the Emergency-Authentication (adhoc) must be done as follows:
    - Both parties simultaneously start the Emergency-Authentication after the replacement of the defective device.
    - The local <crypt>-admin of the new device tells the remote <crypt>-admin the first part of the hash <local adhoc id> by telephone. The remote admin compares this hash with his <peer adhoc id>. A second person present at the remote site confirms the readings.
    - The same procedure will now be repeated into the other direction, where the remote admin tells the local admin his part of the hash and the local admin acknowledges the hash. Again a second person locally present confirms the readings.

    - If both verifications are successful, the Emergency-Authentication can be accepted by entering <yes>.
    - The operation with an Emergency-Authentication must be terminated within 72 hours by an authorised administrator.
    - In order to move from Emergency-Authentication to ordinary operation, a new Host Key must be configured by an authorised administrator. A key management system approved by the BSI for use with the SINA L2 Box S, Versions 3.3.2, 3.3.3 must be used to generate the Host Key (see above).
  - In multipoint mode, the Emergency-Authentication (register) must be done as follows:
    - The passphrase previously configured for the Emergency-Authentication has to be kept safe and accessible for authorised personnel only.
    - The time window (register timeout) for the Emergency-Authentication must be less or equal 5 minutes.
    - The entry of the passphrase necessary for the Emergency-Authentication must happen in the presence of 2 persons to assure a correct execution.
    - The operation with an Emergency-Authentication must be terminated within 7 days by an authorised administrator.
    - In order to move from Emergency-Authentication to ordinary operation, a new Host Key must be configured by an authorised administrator. A key management system approved by the BSI for use with the SINA L2 Box S, Versions 3.3.2, 3.3.3 must be used to generate the Host Key (see above).
    - After an Emergency-Authentication, a passphrase must be configured for the Emergency-Authentication and has to be kept safe and accessible for authorised personnel only.
- Passwords:
  - General requirements for the use of passwords:
    - minimum length: 10 characters
    - different characters: 3 characters
    - lower case letters: 1 character
    - upper case letters: 1 character
    - Numbers/Special Characters: 1 character
  - All other passphrases (monitor, register, l2sec) must not be shorter than 20 characters and must comply to the password requirements above.

3.3 Quantum Computer Resistance

The SINA L2 Box S uses a hybrid crypto approach of Quantum Computer resistant symmetric cryptography (AES-256) and not Quantum Computer resistant asymmetric cryptography (ECDH) under BSI approved operation.

An attack with a Quantum Computer would result in a loss of Perfect-Forward Secrecy provided by the EC Diffie-Hellman only.

It is planned to complement the current hybrid approach by another, Quantum Computer resistant, algorithm by firmware upgrades.

4 SECURITY CLASSIFICATIONS

4.1 Security Classification List

The classification levels for control and safeguarding the SINA L2 Box S 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

The **SINA L2 Box S** is subject to sales restrictions. The export is subject to the German export legislation. Generally, the manufacturer requires the agreement of the appropriate bodies. The same restrictions apply to the manufacturer and end user to any loan or lease.

5.2 Declaration of Compliance (DoC)

The SINA L2 Box S only uses Type B-Algorithms. For that reason, it is not required to sign a Declaration of Compliance (DoC) for the SINA L2 Box S.

5.3 Accountability and Control

Accounting is not required for the SINA L2 Box S.

6 PHYSICAL SECURITY

6.1 Responsibilities

This section describes the security relevant aspects regarding the use of the SINA L2 Box S. The strict adherence to the instructions given in this document is required to permanently ensure security of the classified information, which is protected with the SINA L2 Box S. 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 of physical security

The secrecy regulations for material security applicable to the respective operator and end user must be observed

If EU- and/or NATO classified information will be protected with the SINA L2 Box S, 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 the SINA L2 Box S shall be afforded according to the classification levels and markings given in Annex B.

- The SINA L2 Box S shall only be used and operated by authorised and enabled personnel.
- For storage and during transport and shipment, the SINA L2 Box S shall be protected against unauthorised access to avoid any possible violation of the integrity of the SINA L2 Box S.
- During operation, the SINA L2 Box S shall be protected against unauthorised 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 the SINA L2 Box S.
- The SINA L2 Box S shall be inspected by the Security Officer (or a competent body authorised 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

For storage and transportation of the SINA L2 Box S, the requirements given in Annex B apply. The requirements set up therein shall particularly be noted by the Crypto Custodian and the manufacturer.

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

6.3.1 Tamper Protection

The device must not be opened by unauthorised personnel under any circumstances. If a device is opened at any time, an anti tamper mechanism prevents further operation of the device. Only the manufacturer at the factory can reset the tamper status in this case.

In a tamper condition, the emergency erase function of the device erased all keys and the security relevant configuration. The emergency erase function zeroises all key independent of operating condition of the device. The configuration will be erased during operation only. Logfiles must be erased manually.

If there are any assumptions or hints that the SINA L2 Box S has been tampered or manipulated, appropriate actions shall be taken as described in chapter 10.

6.3.2 Tamper Detection Sticker (MEP)

MEPs are a special kind of label which are affixed to the housing of a secure product in such a manner, that it cannot be opened without destroying the MEP. Every MEP carries an individual serial number. If a MEP is missing, has been removed for maintenance or repair, was unintentionally damaged or tampered by an unauthorised manipulation, it cannot be used anymore and has to be replaced by a new one.

The SINA L2 Box S is protected by 1 MEP.

The MEP (SEAL) is attached to this place at the device:

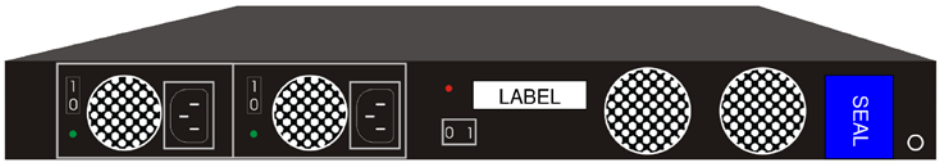

Figure 6: Position of MEPs

The MEP is attached around the edge (rear/bottom) of the device in order to prevent moving the lid backwards and opening the device.

Figure 7: Old MEP

Figure 8: New MEP

Example original MEP

Example of tampered MEP
(possible manipulation)

Figure 9: MEP conditions

Every time the SINA L2 Box S is comissioned, the End User shall check that MEPs have not been removed and that they are unharmed. In addition the CIS Security Officer (or authorised service staff) shall do periodic visual inspections to check that all MEPs are still in existence and that they are unharmed. It is recommended that the CIS Security Officer notes the serial numbers of the MEPs when the SINA L2 Box S is unpacked for the first use and archives these numbers for future inspections. The CIS Security Officer may decide on the frequency of the periodic checks.
For security reasons, the SINA L2 Box S shall not be operated with a damaged MEPs. Damages occurred at MEPs or other detected abnormalities shall be reported immediately to the CIS Security Officer for further action (see chapter 10 of the main document).

In case of observing a missing or damaged MEP, implying that an unauthorised opening of the crypto device could not be excluded, the device shall be checked by authorised service staff (e.g. the manufacturer).

If there are any assumptions or hints that the SINA L2 Box S has been tampered or manipulated, appropriate actions shall be taken as described in chapter 10. New MEPs will be applied by authorised personnel (e.g. the manufacturer) after performing and passing the technical inspection.

Being placed into operation again, it shall be checked whether the SINA L2 Box S operates properly, no tamper alert is signalled and the new Tamper Detection Stickers are unharmed.

6.3.3 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

6.4.1 Destroying/deleting keys/certificates

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

If a device is decommissioned, the emergency erase button at the rear side of the device must be pressed.

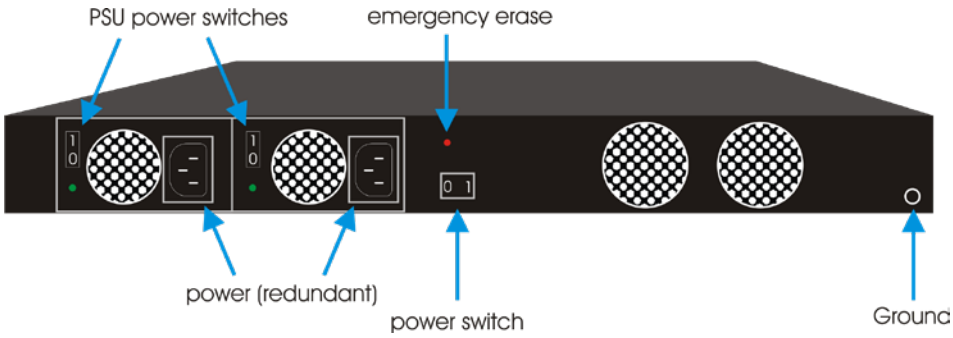

Figure 10: Emergency Erase 19“ devices

The emergency erase function of the device erases all keys and the security relevant configuration. The emergency erase function zeroises all key independent of operating condition of the device. The configuration will be erased during operation only. Logfiles must be erased manually.

It is recommended to press the emergency erase button when the device is switched off and to switch on the device afterwards. After 2 automatic boot cycles, the device is in its factory condition. Logfiles must be erased manually.

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

The SINA L2 Box S shall be destroyed at the end of its life cycle in a secure manner. The conditions and procedures relating to the destruction are described hereinafter:

- Internally stored key material or similar security critical parameters must be zeroised by emergency erase (see above).
- The internal flash storage with the firmware has to be removed and securely delete or destroyed.
- 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.

- If all internally stored keys and parameters are zeroised and the flash storage removed, the system hardware can be recycled. Care must be taken to assure that the systems are really being destroyed or recycled and are not coming into the market again.

7 PERSONNEL SECURITY

In addition to the requirements described in references E1-E4 and N1-N2, the following security requirements apply for the SINA L2 Box S.

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 the SINA L2 Box S.

7.3 Need-To-Know

The access to the SINA L2 Box S 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 the SINA L2 Box S.

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 following requirements shall be met for the maintenance and repair of the SINA L2 Box S.

- The **SINA L2 Box S** must not be opened by the customer or End User. Maintenance and repair requiring an opening of the housing as well as software or firmware upgrades have to be performed by authorized personnel of the manufacturer.
- For other maintenance works or firmware upgrades, authorized and reliable personnel must be used (see 7.2).
- It is not allowed to do maintenance or repair on the SINA L2 Box S, Versions 3.3.2, 3.3.3 during operation. Attention has to be paid to § 41 VSA. An exception is the replacement of a hot-swap power supply module.
- If a device leaves the secure operation area for maintenance or repair, all security relevant data (keys and other parameters) must be zeroised (see 6.4.1).
- The MEPs must be checked before recommissioning.
- The firmware of the device must be kept at the latest version recommended by the manufacturer.

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 the SINA L2 Box S 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

The emergency erase function of the device erases all keys and the security relevant configuration. The emergency erase function zeroises all key independent of operating condition of the device. The configuration will be erased during operation only. Logfiles must be erased manually.

It is recommended to press the emergency erase button when the device is switched off and to switch on the device afterwards. After 2 automatic boot cycles, the device is in its factory condition. Logfiles must be erased manually.

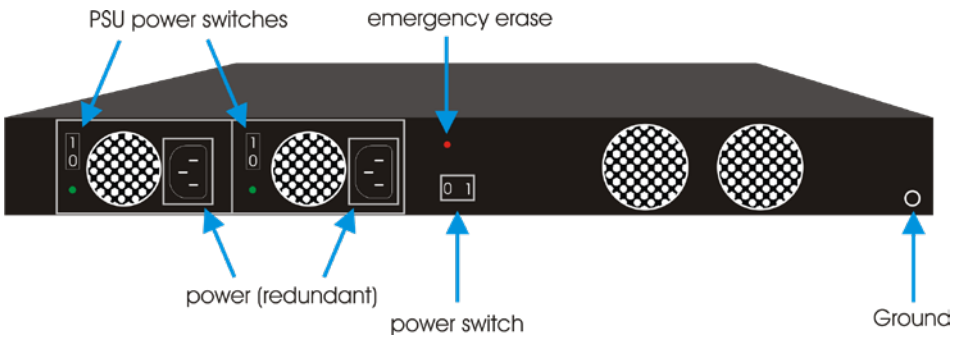

Figure 11: Zeroisation by Emergency Erase

10 COMSEC INCIDENTS

10.1 Contact person of the operator

The CIS Operational Authority or End User of the SINA L2 Box S 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 following measures shall be applied by the CIS Administrator, the CIS Security Officer, resp. the Security officer when the Tamper-Mechanism is activated:

- For security reasons, the SINA L2 Box S shall not be operated anymore when the Tamper-Mechanism is activated.

The following measures shall be applied by the CIS Administrator, the CIS Security Officer, resp. the Security officer when MEPs are destroyed or missing:

- For security reasons, the SINA L2 Box S shall not be operated anymore when MEPs are destroyed or missing.
- The device shall be sent to the manufacturer for further investigation and solving the problem. It shall be subjected to a security-related inspection by the manufacturer (manipulation, TEMPEST/EMSEC, ...). Prior to this, all classified data and key material shall be securely deleted by initiating the Zeroisation (Figure 11).
- New MEPs shall be fitted on the device by authorised personnel (e.g. from the manufacturer) when the security-related inspection showed a positive result.

The device must not be opened by unauthorised personnel under any circumstances. If a device is opened at any time, an anti tamper mechanism prevents further operation of the device. Only the manufacturer at the factory can reset the tamper status in this case.

11 POINTS OF CONTACT

11.1 Manufacturer

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Deutschland

E-Mail: support@secunet.com
Tel.: +49 201 5454-1520

11.2 BSI Crypto-Support

When a manipulation of the SINA L2 Box S 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 the SINA L2 Box S 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

SINA L2 Box S, Versions 3.3.2, 3.3.3

Approval-ID BSI-VSA-10722

1 Approval

SINA L2 Box S, versions 3.3.2, 3.3.3 is nationally approved by the Bundesamt für Sicherheit in der Informationstechnik (BSI) with the Approval-ID BSI-VSA-10722, dated 23.12.2022, for the protection of information classified VS-NUR FÜR DEN DIENSTGEBRAUCH.

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

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

SINA L2 Box S, 3.3. is approved by the EU Council with the approval document for RESTREINT UE/EU RESTRICTED: 11704/15, from 14.09.2015.

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

In the following the current design status of the approved version of SINA L2 Box S 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 SINA L2 Box S with the approved design status, and the correct version and configuration. Prior to installation and operation of the delivered SINA L2 Box S 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 SINA L2 Box S is listed below. The design status is recorded for every approved product version and is an integral part of the approval documentation.

The SINA L2 Box S, releases 3.3.2, 3.3.3 software may only be operated on the hardware platforms (variants) listed below.

4.1 Approved Software Versions

A detailed list of software and hardware components, which are part of the approved version of SINA L2 Box S, releases 3.3.2 including the relevant patch status can be found in the document titled "Konstruktionsstand_332.pdf" from 28.10.2019. The document is maintained by BSI.

A detailed list of software and hardware components, which are part of the approved version of SINA L2 Box S, releases 3.3.3 including the relevant patch status can be found in the document titled "Konstruktionsstand_333.pdf" from 28.10.2019. The document is maintained by BSI.

The version 3.3.4 shall be approved shortly. The next version 3.4 shall be evaluated this year and it is planned to make the approval at the beginning in 2024.
An update to the new versions shall be made shortly.
The update to the version 3.4 over 31.12.2025 is necessary to ensure an approved operation.

4.2 Approved Smartcards for Releases 3.3.2, 3.3.3

The smartcards are used for the transport of key material and configuration only.

Chip Manufacturer	**Chip Type**	**Operating System**
Infineon	SLE78CLX1280P	STARCOS 3.5
Infineon	SLE66CX322P	CardOS v4.3b

4.3 Hardware versions of the SINA L2 Box S

The approval is valid for the following hardware versions of releases 3.3.2, 3.3.3 of the SINA L2 Box S:

hardware platform	**platform ID**
SINA L2 Box S 50M-2/100M-2/1G-3	1004
SINA L2 Box S 40G	1094
SINA L2 Box S 1G-2/10G-2/10G-3	1254
SINA L2 Box S 100G	1104 (version 3.3.3 only)

ANNEX B

Security Classification List

SINA L2 Box S, Versions 3.3.2, 3.3.3

Approval-ID BSI-VSA-10722

		Security Classification[1]		No Security Classification[1]	Remarks
		VS-V/NC/ C-UE/EU-C	VS-NfD/NR/ R-UE/EU-R		
1	SINA L2 Box S (factory condition)			X	4)
2	SINA L2 Box S installed, ready for operation		X		5)
3	SINA L2 Box S, switched off, keys loaded		X		5)
4	SINA L2 Box S, switched off, keys zeroised		X		4)
5	SINA L2 Box S, switched off, keys zeroised, configuration deleted			X	4)
6	SINA L2 Box S, defective		X		4)
7	Smartcards		X		2) 3)
8	Other data storage or key material		X		2) 6)
9	Update Files			X	1) 6)

1) The Update File is not classified but its integrity shall be protected.

2) The Smartcard is classified RESTRICTED and shall be protected against unauthorized access anytime. If key material with a classification higher than RESTRICTED is used, the Smartcard has to be classified respectively.

3) The Smartcards and PINs shall be stored and shipped separately.

4) The SINA L2 Box S shall be protected against unauthorized access during storage, and transportation.

5) The SINA L2 Box S shall be protected against unauthorized access anytime.

6) The data shall be protected against unauthorized access.

1 When using the product for the protection of NATO / EU classified information the corresponding international classification levels and markings are valid.

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)
-		

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.