Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ver. 3.1 rel. 5

Certificato n. *(Certificate No.)*	12/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/06/2024/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	23 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5
Sviluppatore *(Developer)*	Guntermann & Drunck GmbH (G&D)
Tipo di Prodotto *(Type of Product)*	Altre categorie - KVM-over-IP
Livello di Garanzia *(Assurance Level)*	EAL2+ (ALC_FLR.2), conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto, conforme a CC Parte 2

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 23 febbraio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5

OCSI/CERT/CCL/06/2024/RC

Version 1.0

23 February 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	23/02/2026

2 Table of contents

1 Document revisions 3
2 Table of contents 4
3 Acronyms 6
3.1 National scheme 6
3.2 CC and CEM 6
3.3 Other acronyms 6
4 References 8
4.1 Normative references and national Scheme documents 8
4.2 Technical documents 9
5 Recognition of the certificate 10
5.1 European recognition of CC certificates (SOGIS-MRA) 10
5.2 International recognition of CC certificates (CCRA) 10
6 Statement of certification 11
7 Summary of the evaluation 12
7.1 Introduction 12
7.2 Executive summary 12
7.3 Evaluated product 13
7.3.1 TOE architecture 13
7.3.2 TOE security features 15
7.4 Documentation 15
7.5 Protection Profile conformance claims 16
7.6 Functional and assurance requirements 16
7.7 Evaluation conduct 16
7.8 General considerations about the certification validity 17
8 Evaluation outcome 18
8.1 Evaluation results 18
8.2 Recommendations 19
9 Annex A – Guidelines for the secure usage of the product 20
9.1 TOE delivery 20
9.2 Installation, configuration and secure usage of the TOE 21
10 Annex B – Evaluated configuration 22

10.1 TOE operational environment 22
11 Annex C – Test activity 23
11.1 Test configuration 23
11.2 Functional tests performed by the Developer 23
11.2.1 Testing approach 23
11.2.2 Test coverage 23
11.2.3 Test results 23
11.3 Functional and independent tests performed by the Evaluators 23
11.3.1 Test approach 23
11.3.2 Test results 24
11.4 Vulnerability analysis and penetration tests 24

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

CM	Configuration Management
CON	Console
CPU	Central Processing Unit
CS	Customer Support
GUI	Graphical User Interface
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IT	Information Technology

MMSH	Microsoft Media Server over http
NTP	Network Time Protocol
KVM	Keyboard, Video and Mouse
RTP/TCP	Real-time Transport Protocol over TCP
RTSP/TCP	Real Time Streaming Protocol over TCP
SHA	Secure Hash Algorithm
SSH	Secure Shell
UID	Unique Identifier
USB	Universal Serial Bus
VNC	Virtual Network Computing
SQL	Structured Query Language
TCP	Transmission Control Protocol
XS	Extra Small
XSS	Cross Site Scripting

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components", Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components", Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, "Common Methodology for Information Technology Security Evaluation – Evaluation methodology", Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[ETRv4] Evaluation Technical Report G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5, GUNTER_033_ETR_v4, CCLab Software Laboratory (Debrecen site), 11 February 2026

[GUIDE_CC] G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5 KVM-over-IP Matrix System Guidance Supplement, version: v0.17, date: February 6, 2026

[ST] G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5 Security Target - Evaluation Assurance Level (EAL): EAL2+ Document Version: 1.12, 6 February 2026

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT -Products. A higher recognition level for evaluations beyond EAL4 is provided for IT -Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all claimed assurance components up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5**", developed by Guntermann & Drunck GmbH (G&D).

The Target of Evaluation (TOE) is a product that provides a secure medium to connect one or more input peripherals to one or more computers. The TOE models support connectivity between two sets of peripheral devices (audio, keyboard/mouse, user authentication, USB devices, and one display) and one connected computer. The TOE consists of a family of devices that support different computers, different monitors, and different types of display protocols depending on the model.

The TOE provides a capability to dynamically change the switching configuration to connect a particular computer to a particular peripheral set. The TOE enforces secure separation of information flows corresponding to what actions a logged-in user is permitted to perform. The corresponding Information Flow Control Security Policy is the main security feature of the TOE. Users have no rights initially, but are assigned individual rights such as user rights, global device rights, individual device rights, and script rights. The TOE consists of several components: Vision-IP or VisionXS-IP, which act as KVM Extender Consoles; Vision-IP, VisionXS-IP, or RemoteAccess-IP, which serve as KVM Extender CPUs; and ControlCenter-IP (including the XS variant), which functions as the KVM matrix switch.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2 and NIS3]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should also review the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 Revision 5 for the assurance level EAL2, augmented with ALC_FLR.2, according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3] e [CC5]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product named "G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5
Security Target	G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5 Security Target - Evaluation Assurance Level (EAL): EAL2+ Document Version: 1.12, 6 February 2026 [ST]
Evaluation Assurance Level	EAL2, augmented with ALC_FLR.2
Developer	Guntermann & Drunck GmbH (G&D)
Sponsor	Corsec Security, Inc.
LVS	CCLab - The Agile Cybersecurity Laboratory (Debrecen site)
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	April 29, 2024
Evaluation ending date	February 11, 2026

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description refer to the Security Target [ST].

The Target of Evaluation (TOE) is a KVM-over-IP matrix system composed of hardware and firmware components, designed to provide a secure medium for connecting one or more input peripherals to one or more computers. The TOE enables dynamic switching between computers and peripheral sets, enforcing secure separation of information flows according to user permissions. The main security feature is the Information Flow Control Security Policy, which ensures that only authorized actions and connections are permitted.

The TOE includes the guidance documentation for establishing the certified configuration [GUIDE_CC].

The TOE consists of the following hardware components:

- Vision-IP or VisionXS-IP (CON) – These devices act as KVM Extender Consoles, connecting monitors, keyboards, mice, audio, and USB peripherals.
- Vision-IP, VisionXS-IP, or RemoteAccess-IP (CPU) – These devices act as KVM Extender CPUs, connecting to physical computers or virtual machines. RemoteAccess-IP supports integration of virtual machines via SSH and streaming protocols (RTP/TCP, RTSP/TCP, MMSH).
- ControlCenter-IP (including XS variant) – This device functions as the KVM matrix switch, providing central administration, secure encrypted communication, and scalability to thousands of devices.

Firmware versions for the evaluated configuration are: ControlCenter-IP v1.7, ControlCenter-IP-XS v1.1, Vision-IP v2.4, VisionXS-IP v1.5, RemoteAccess-IP v1.3.

TOE users authenticate using a username and password, with optional two-factor authentication. Initially, users have no rights and are assigned specific permissions such as user rights, global device rights, individual device rights, and script rights.

Administrators manage the TOE through a Web GUI (Config Panel), which allows configuration of TOE settings, viewing audit messages, managing users and permissions, and modifying network filtering rules. All management actions generate audit logs that are sent to an internal syslog server.

The TOE provides the capability to dynamically change switching configurations, connecting a specific computer to a specific peripheral set. Switching actions are controlled by authorized mechanisms and indicated to the user to prevent unintended connections.

For a detailed description of the TOE, refer to sections 1.4 and 1.6 of the Security Target [ST].

7.3.1 TOE architecture

The TOE is a KVM-over-IP matrix system composed of hardware and firmware components listed in section 1.4 of the Security Target [ST]. The TOE includes Vision-IP and VisionXS-IP modules (console and computer), RemoteAccess-IP modules, and ControlCenter-IP (-XS) matrix switches. The TOE is installed on an internal IP-based network and provides secure connectivity between peripheral devices (audio, keyboard/mouse, USB, display) and one connected computer. The physical architecture and TOE boundary are depicted in Figure 1.

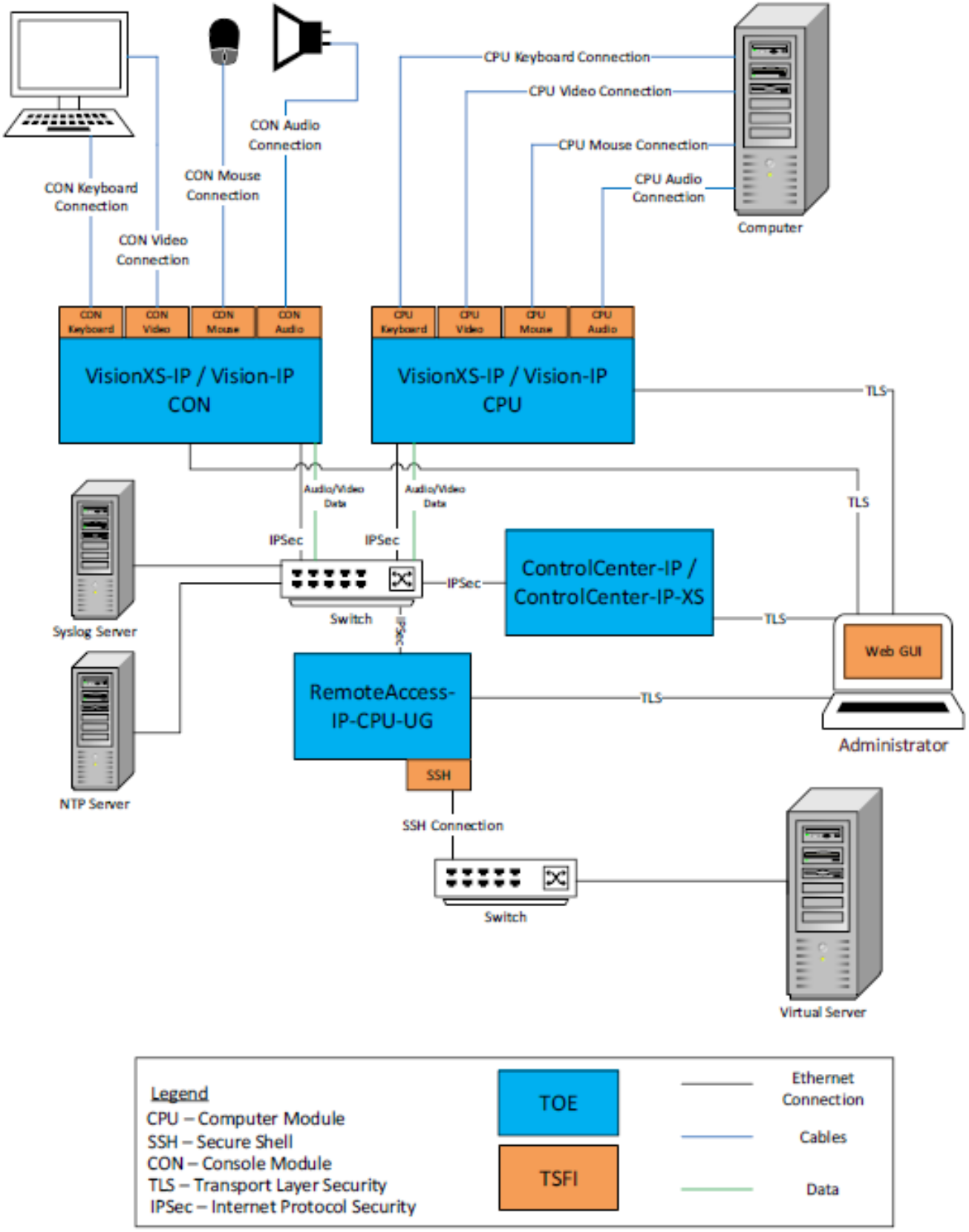

Figure 1 - Physical TOE Boundary

7.3.2 TOE security features

Assumptions, threats, and security objectives are defined in sections 3 and 4 of the Security Target [ST].

The major security features of the TOE are summarised in the following:

1) **Security Audit**

   The TOE's components generate audit messages for startup and shutdown of the audit function, user authentication, and configuration changes. These audit records include the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure). Audit messages are sent to an internal syslog server via the syslog protocol and are protected from unauthorized deletion or modification.

2) **User Data Protection**

   The TOE enforces information flow control using device UIDs and user permissions. Video and audio data flow unidirectionally, while USB, keyboard, and mouse data flow bidirectionally between UID-locked peripheral devices and TOE components. Unauthorized devices or users are rejected, and user data is purged prior to switching connections. Non-volatile memory is not used for user data.

3) **Identification and Authentication**

   Administrators authenticate to the TOE using a username and password before any TSF-mediated actions. Two-factor authentication can also be configured. Identification and authentication are required prior to any other actions within the TOE.

4) **Security Management**

   The TOE provides a Web GUI for administrators to configure and manage TOE settings, view audit messages, and manage users. Management functions include creating and deleting administrators, modifying user permissions, and configuring KVM system components. Only authorized administrators can modify security attributes.

5) **Protection of the TSF**

   The TOE automatically runs a suite of self-tests at startup or reset to verify the integrity of its firmware. Each component can connect to an NTP server to provide synchronized date and time for reliable timestamps. Firmware integrity can be verified by authorized users.

For a detailed description of the security features of the TOE, please refer to sections 1.6.2 and 7 of the Security Target [ST].

7.4 Documentation

The Guidance Supplement [GUIDE_CC] provides clarifications and changes to the G&D documentation and should be used as the guiding document for the installation and administration of the TOE in the Common Criteria-evaluated configuration. The official G&D documentation should be referred to and followed only as directed within this document.

The Common Criteria Guide can also be downloaded from the G&D website at https://www.gdsys.com/en/securecert. In order to check the integrity of the document, you can execute the command "sha256sum file_name".

The obtained value must match the SHA-256 hash value:

30A7B64C43184D501C1B570977A1AF4EC236FD66E1817CF54E2A88389C84262C.

G&D KVM-over-IP matrix system documentation includes additional relevant guidance for the secure operation of the TOE that are listed in section 1.6.1.2 of [ST].

In order to check the integrity of each document, users can execute the command “sha256sum file_name” to verify that the obtained value matches the SHA-256 hash value available in section 1.6.1.2 of [ST].

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL 2 assurance package, augmented with the CC part 3 components ALC_FLR.2.

All the SFRs have been selected from CC Part 2 [CC2].

It is possible to refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and [NIS5] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab - The Agile Cybersecurity Laboratory (Debrecen site).

Technical Report v4 [ETRv4], which was approved by the Certification Body on 17th February, 2026. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in "Annex B – Evaluated configuration".

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The Certification Body recommends reviewing the assumptions in the [ST], section 3.3, which are necessary conditions to be implemented for the TOE security:

- *A.PHYSICAL - The TOE is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the device's physical interconnections and correct operation.*
- *A.TRUSTED_ADMIN - Administrators are trusted to follow and apply all guidance in a trusted manner.*
- *A.NETWORK - Access to the TOE's ConfigPanel can be restricted to individual IP networks and individual devices.*

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate.

This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETRv4] issued by the LVS CCLab - The Agile Cybersecurity Laboratory (Debrecen site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2 augmented with ALC_FLR.2, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2 augmented with ALC_FLR.2 (augmentation *in italics* in Table 1).

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	*Pass*

Assurance classes and components		Verdict
Test	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product "G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "Security Objectives for the Operational Environment" specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.3 of the Security Target [ST] shall be satisfied.

As mentioned in section 7.8, the Certification Body recommends reviewing the assumptions in the [ST], section 3.3, which are necessary conditions to be implemented for the TOE security:

- *A.PHYSICAL - The TOE is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the device's physical interconnections and correct operation.*
- *A.TRUSTED_ADMIN - Administrators are trusted to follow and apply all guidance in a trusted manner.*
- *A.NETWORK - Access to the TOE's ConfigPanel can be restricted to individual IP networks and individual devices.*

This Certification Report is valid for the TOE in its evaluated configuration; in particular, "Annex A – Guidelines for the secure usage of the product" includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE (Guidance Supplement [GUIDE_CC]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The G&D KVM-over-IP matrix system TOE is delivered as hardware/firmware and includes the following component families within the evaluated configuration:

- ControlCenter-IP
- ControlCenter-IP-XS
- RemoteAccess-IP
- Vision-IP
- VisionXS-IP

Trusted couriers are used to deliver TOE hardware. Parcels are collected from the production site in Siegen by parcel service or freight forwarder; G&D products are transported by land, air, or sea by a trusted courier. Couriers use signature proof of delivery to confirm receipt, and tracking services are offered by parcel service providers and freight forwarders. The processing status is communicated to notify customers of any changes or updates to the TOE during distribution.

Upon receipt, customers verify the integrity of the TOE by comparing the delivered parcels with the shipping papers. Delivery verification relies on the carriers' standard security measures, including signature proof of delivery, and requires that the receiver witness the delivery and verify the delivery contents. Customers report any suspicions or issues related to the security of the delivered product by first contacting the service department. The TOE performs an initial self-test for device integrity at power-up or reset.

Each component contains a label on the bottom of the device for identification purpose. New firmware updates are not publicly available, a download link can be provided to customers upon request through G&D support. Table 2 can be used to verify the firmware reference file for the evaluated TOE version. Customers may reach out to G&D support for access to these files. Customers may verify their firmware files by taking the SHA-256 hash of their files and comparing them those reported in Table 2.

TOE Firmware Files	SHA-256 Hash
ControlCenter-IP firmware 1.7	36A484B4B858AD73F057A6ACF1E0B45105F58485E4FEC7FB07F2EEF2E4CE4CAC
ControlCenter-IP-XS firmware 1.1	1EF006F26B1A8DE4B61A0F8055D09AB1BF2951C614A6BFEECAE239F3DE78B2AE
RemoteAccess-IP firmware 1.3	0DE6F69D7EE1CDE8819DF4CE4C1A1DAFCDD4143796C96C6A46B2FD435517E7C9
Vision-IP firmware 2.4	50756FA90F33C7040E9C1E16DDEC8F218D575DBB94EEA2A158D6DF5823A6997C
VisionXS-IP firmware 1.5	C9413794415890900578 4CA5549FBAABDF861920EDEB5A42F0DCEA5330FD7D68

Table 2 TOE firmware references

In addition, once the customer is logged into the Web GUI for each component, they will be able to verify the firmware version by navigating to Configuration > Information > Hardware Information and checking the version in the Firmware rev. field.

Customers shall obtain and verify the integrity of the Guidance Supplement [GUIDE_CC] following the steps defined in section 7.4 Documentation.

9.2 Installation, configuration and secure usage of the TOE

TOE installation, configuration and secure usage must be performed following the instructions contained in the relevant sections of the official guidance provided with the product to the customer.

In particular, the Guidance Supplement [GUIDE_CC] contains detailed information for the secure initialization of the TOE, the preparation of its operational environment, and the secure usage of the TOE in accordance with the security objectives specified in the Security Target [ST].

Customers shall obtain and verify the integrity of the Guidance Supplement [GUIDE_CC] following the steps defined in section 7.4 Documentation.

10 Annex B – Evaluated configuration

The Evaluators followed the preparation steps defined in the Guidance Supplement [GUIDE_CC] for the TOE being in the evaluated configuration.

The TOE consists of the following hardware components:

- Vision-IP or VisionXS-IP (CON) – These devices act as KVM Extender Consoles, connecting monitors, keyboards, mice, audio, and USB peripherals.
- Vision-IP, VisionXS-IP, or RemoteAccess-IP (CPU) – These devices act as KVM Extender CPUs, connecting to physical computers or virtual machines. RemoteAccess-IP supports integration of virtual machines via SSH and streaming protocols (RTP/TCP, RTSP/TCP, MMSH).
- ControlCenter-IP (including XS variant) – This device functions as the KVM matrix switch, providing central administration, secure encrypted communication, and scalability to thousands of devices.

Firmware versions for the evaluated configuration are: ControlCenter-IP v1.7, ControlCenter-IP-XS v1.1, Vision-IP v2.4, VisionXS-IP v1.5, RemoteAccess-IP v1.3.

The items described in section 10.1 “TOE operational environment” must be available before performing the installation.

10.1 TOE operational environment

The operational environment required for the correct functioning of the TOE includes several non-TOE infrastructure components and configuration requirements necessary to maintain the evaluated Common Criteria configuration. All TOE components must have the SecureCert feature to ensure CC compliance, and each device must be able to connect to a trusted NTP server to obtain NTP-synchronized time for reliable and consistent timestamp generation.

In order to ensure the TOE works properly, the network infrastructure must be configured with Layer-2 managed switch with Gigabit Ethernet capabilities, required to provide additional control and monitoring capabilities beyond basic switching. The following must be configured on the network switches:

- Multicast;
- IGMP;
- IGMP Snooping;
- IGMP Snooping Querier.

In addition, ports 18244, 18245 and 18246 must be open.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

The Evaluators for the evaluated configuration have followed the preparation steps for the TOE defined in the Guidance Supplement [GUIDE_CC]. The evaluator conducted the tests locally.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The developer performed extensive tests to verify the functionality of the TOE. The tests cover all Subsystems, Modules and TSFIs of the TOE

The Developer provided six manual test cases:

- Test Case 01 – Test Setup
- Test Case 02 – Identification and Authentication
- Test Case 03 – Security Audit
- Test Case 04 – Security Management
- Test Case 05 – User Data Protection
- Test Case 06 – Protection of the TSFs

The evaluator tested all the test cases to produce the best coverage of the testing.

11.2.2 Test coverage

The Evaluators verified the complete coverage between the test cases in the test documentation provided by Developer and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behaviour and properties of the TSF.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

All Developer's tests were repeated by the Evaluators to confirm the validity of expected results. Moreover, during the independent testing phase, the Evaluator created five additional tests to cover the TOE features more in depth:

- Test Case 07 – User Group settings
- Test Case 08 – Server Data Protection
- Test Case 09 – Network port misconfiguration

- Test Case 10 – Self-test and time validation
- Test Case 11 – Server Data Protection

11.3.2 Test results

All Developer's tests were run successfully, and the Evaluators verified the correct behaviour of the TSFIs and TSFs and the correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators were passed successfully and all the test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked with the TOE already used for the functional test activities and verified that the TOE and the test environment were properly configured.

The Evaluators designed the following attack scenarios:

- Sensitive data harvesting (network sniffing)
- Client-side attack with malicious SSH/VNC server
- SQL injection
- Cross-Site Scripting (XSS)
- Log injection
- Command injection
- Username enumeration (error-based)
- Hidden endpoints / information leakage

The Evaluators have concluded that the TOE is resistant to basic attack potential in its intended operational environment.