Federal Office
for Information Security

# Certification Report

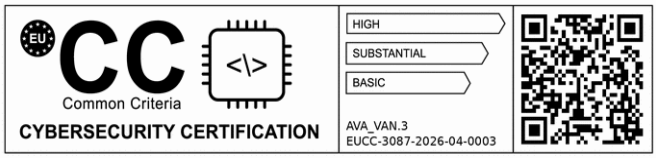
**EUCC-3087-2026-04-0003**
Administration ID
**BSI-DSZ-CC-1177-V2-2026**

for

**L4Re Secure Separation Kernel,** Version CC 1.0.2

from

**Kernkonzept GmbH**



BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-11

# Contents

A. Certification....4
1. Preliminary Remarks....4
2. Specifications of the Certification Procedure....4
3. Recognition Agreements....5
4. Performance of Evaluation and Certification....5
5. Publication....7
B. Certification Results....8
1. Executive Summary....9
2. Identification of the TOE....10
3. Security Policy....11
4. Assumptions and Clarification of Scope....11
5. Architectural Information....11
6. Supplementary Cybersecurity Information....12
7. IT Product Testing....12
8. Evaluated Configuration....13
9. Results of the Evaluation....13
10. Obligations and Notes for the Usage of the TOE....14
11. Security Target....14
12. Definitions....15
13. Bibliography....16
C. Annexes....18

# A. Certification

## 1. Preliminary Remarks

The Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 [EUCC-VO] establishes a Union-wide cybersecurity certification scheme for TOEs and Protection Profiles for conformity assessments using the requirements of Common Criteria.

By implementing the Cybersecurity Act[1], certification activities at assurance level 'high' and in duly justified cases at assurance level 'substantial' are reserved to the National Cybersecurity Certification Agency of a Member State.

In accordance to BSIG[2] Act, the Federal Office for Information Security (BSI) issues certificates for information technology products.

Certification of a product is carried out at the request of a developer, vendor or a distributor, hereinafter called the applicant.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria referenced in the above mentioned Implementing Regulation (EU) 2024/482 as well as relevant application notes and interpretations published by the certification body of the BSI.

Evaluation facilities notified by the German National Cybersecurity Certification Authority carry out the evaluation.

This Certification Report is the result of the certification activities carried out by the certification body of the BSI in conclusion of the technical evaluation. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

## 2. Specifications of the Certification Procedure

The certification body carries out its activities according to the criteria laid down in the following:

- Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [EUCC-VO]
- EUCC state-of-the-art documents of relevance to the TOE [EUCC_SOTA]
- Act on the Federal Office for Information Security[2]

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025 Nr. 301, S. 2

- BSI Certification and Approval Ordinance[3]
- BMI Regulations on Ex-parte Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 Common Criteria for IT Security Evaluation (CC), Version 3.1 R5 [CC]
- ISO/IEC 18045 Common Methodology for IT Security Evaluation (CEM), Version 3.1 R5 [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC_PROG]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [AIS]

# 3. Recognition Agreements

In order to avoid multiple certifications of the same product in different countries a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed

## 3.1. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 5 EAL 2 and ALC_FLR components.

# 4. Performance of Evaluation and Certification

- The certification body monitors each individual evaluation to ensure a uniform application and interpretation of the criteria as well as uniform ratings.
- The TOE L4Re Secure Separation Kernel, Version CC 1.0.2 has been certified by the certification body of the Federal Federal Office for Information Security (BSI) based on

[3] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 02 December 2025, Bundesgesetzblatt 2025, no. 301

[4] BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

administration ID BSI-DSZ-CC-1177-2025. Specific results from the evaluation process were re-used.

- The evaluation of the product L4Re Secure Separation Kernel, Version CC 1.0.2 was carried out by atsec information security GmbH, located at Ismaninger Str. 19 81675 München.
- The evaluation was completed on 25 March 2026. atsec information security GmbH is a notified evaluation facility (ITSEF) .
- This certification was applied for: Kernkonzept GmbH.
- The assessed TOE was developed by: Kernkonzept GmbH.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

This Certification Report applies only to the version of the TOE as identified in this document. The confirmed assurance package is valid on the condition that

- all statements and indications regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in an environment as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The issued Certificate confirms the assurance of the product claimed in the Security Target [ST] on certificate’s issuance day. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be reassessed. Therefore, the holder of the certificate should involve the assurance continuity program of the EUCC Certification Scheme (e.g. by a re-assessment or re-certification) in its obligations to monitor the certified product. Specifically, if certification results should be used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a reassessment on a regular e.g. annual basis.

In order to prevent an indefinite certificate usage where evolving attack methods justify a recent reassessment of the product’s resistance, the maximum validity period of the certificate is limited. The certificate issued on 16 April 2026 is valid until 15 April 2031 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged:

1. to meet the obligations from the Implementing Regulation (EU) 2024/482, in particular but not exclusively to respect the rules for certificate usage, to monitor the conformity of the certified TOE, to inform the certification body about subsequently detected vulnerabilities or irregularities with relevance to the security of the TOE and to maintain vulnerability management and disclosure procedures.

Should changes be introduced into the certified version of the TOE, the validity period of its related certificate can be extended in order to cover the changed TOE, provided the holder of the certificate applies for measures under EUCC scheme’s assurance continuity (i.e. recertification or maintenance) and the changed TOE then meets the assurance requirements.

# 5. Publication

The TOE L4Re Secure Separation Kernel, Version CC 1.0.2 has been notified to ENISA for publication on the website on European cybersecurity certification schemes and has also been included in BSI's list of certified products, which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate[5] has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

[5] Kernkonzept GmbH
Buchenstraße 16 b
01097 Dresden
Deutschland

# B. Certification Results

The following chapters summarise the assessment results of the

- the applicant’s Security Target specified for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes, statements and indications from the certification body.

# 1. Executive Summary

The Target of Evaluation is the L4Re Secure Separation Kernel CC 1.0.2 (L4Re SSK). L4Re SSK is a distribution of the open-source L4Re Operating System Framework. As such it is based on the L4Re Microkernel. The L4Re Microkernel is a 3rd-generation microkernel with a state-of-the-art capability-based mandatory access control security model. It allows the separation of applications into different security domains, information flow control, and, subject to access control, dynamic assignment of resources and communication channels. Further the L4Re Microkernel supports static workloads alongside dynamic workloads, which allows to start, restart and shutdown applications during runtime.

L4Re SSK is configured to act as a separation kernel, to provide the security features claimed by the ST. The TOE supports native applications as well as virtual machines (VMs). Access to every resource including but not limited to memory, hardware devices and CPU cores is protected by capabilities. Applications and VMs can only access a resource if they possess a capability with suitable permissions for that resource.

The product L4Re Secure Separation Kernel, Version CC 1.0.2 has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. This is a re-certification based on the BSI administration ID BSI-DSZ-CC-1177-2025. Specific results from the evaluation process BSI-DSZ-CC-1177-2025 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product L4Re Secure Separation Kernel, Version CC 1.0.2 was conducted by atsec information security GmbH. The evaluation was completed on 25 March 2026. atsec information security GmbH is a notified evaluation facility (ITSEF).

The Evaluation Technical Report (ETR) [ETR] was provided by the ITSEF according to the Common Criteria [CC], the Methodology [CEM], the requirements of the Scheme [EUCC-VO],[EUCC_PROG].

The evaluation has confirmed:

- CC Version and Release: see [CC] and [CEM]
- PP Conformance: None
- Assurance Level: EUCC High with component AVA_VAN.3
- Assurance Package: EAL 4+
- Augmentation: ALC_FLR.3

The Security Target [ST] is the basis for this certification.

A detailed description of the security functionality, addressed threats, organisational security policies and the operational environment can be found in the Security Target [ST].

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results stated in this certificate do not express an appraisal of the strength and suitability of the cryptographic algorithms implemented in the TOE (see BSIG Section 52, Para. 4, Clause 2).

The certification results apply only to the version of the product indicated in the certificate and on the condition that all the statements and indications are kept as detailed in this

Certification Report. Neither the BSI nor any other organisation that recognises or gives effect to this certificate implicitly or explicitly guarantee or endorse the certified TOE.

# 2. Identification of the TOE

The Information and communications technology product is identified as follows:

**L4Re Secure Separation Kernel,** Version CC 1.0.2

Holder of the certificate: Kernkonzept GmbH
Buchenstraße 16 b
01097 Dresden
Deutschland
https://www.kernkonzept.com/cybersecurity-information/

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | SW | l4re_ssk_cc_lx2160a.zip (Hashwert: 6bceb5f05015819cb9d70e2ce9391d17dfc83dde) | 1.0.2 | Compressed zip archive for LX2160A with SMMU |
| 2 | SW | l4re_ssk_cc_x86_virt.zip (Hashwert: 2de780b0d6b09db6b24008cc54a30265ee50e191) | 1.0.2 | Compressed zip archive for x86 with VT-x enabled |
| 3 | SW | l4re_ssk_cc_x86_novirt.zip (Hashwert: 05d20a993ba6166f228884b33c2715cc42abf57d) | 1.0.2 | Compressed zip archive for x86 with VT-x disabled |
| 4 | DOC | l4re_ssk_cc_customer_doc.zip (Hashwert: be2390ec82decb6d7be4df4adcf2cdfd94150459) | 1.0.2 | Compressed zip archive of TOE documentation (see #6 and #7) |
| 5 | DOC | l4re_ssk_cc_interface_and_usage_documentation.zip (Hashwert: 3ffa6276da70dce7a1287ee32b1812c18599e7f8) | 1.0.2 | Compressed zip archive containing the L4Re Interface and Usage Documentation; separately available |
| 6 | DOC | L4Re Configuration Guidance | 15 | PDF contained in #4 |
| 7 | DOC | Development Guidance for a Compartment Communication Proxy based on L4Re | 8 | PDF contained in #4 |

Table 1: Deliverables of the TOE

## 2.1. Overview of Delivery Procedure

As the TOE consists only of Software and Documentation components but no hardware components, delivery of physical items is not applicable. The TOE is delivered to the customer either via remote access to the respective directory or as download, in a way preserving authenticity, confidentiality and integrity. Note that the TOE is usually not delivered to end users. It is rather made available to integrators responsible for integration of the TOE as underlying platform into their products. That integration task is not a part of the evaluation.

## 2.2. Identification of the TOE by the User

The TOE is delivered in several signed archives, one archive for each configuration and an additional archive with documentation and configuration-independent code. Each archive contains a VERSION file. The configuration-specific archives contain the compiled TOE components for one particular configuration and hardware architecture. Before using any

of the archives, the integrator must check the signature of the archive with the gpg key provided by Kernkonzept, and check that the version matches the latest version announced by Kernkonzept.

# 3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

The TOE implements a capability-based access control policy to control resource access by applications and virtual machines. The capability-based access control is also the basis for an information flow control between the mentioned applications / VMs. Specific details concerning the mentioned security policies can be found in sections 7.1 and 7.2 of the [ST].

A general description of the flaw remediation processes at Kernkonzept can be found in [FLR] and [FLRGuide]. For vulnerability handling, information can be found on the following website: https://www.kernkonzept.com/cybersecurity-information/

# 4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These uncovered aspects need to be provided for by specific security objectives that have to be met by the TOE environment. They are in particular:

| | |
|---|---|
| OE.HARDWARE | The underlying hardware, firmware and bootloader needed by the TOE to guarantee secure operations fulfil the requirements, as explained in the TOE User Manuals and stated in section 1.3.5 of [ST]. They are working correctly and have no undocumented or unintended security critical side effect on the functions of the TOE. |
| OE.PHYSICAL | The IT environment provides the TOE with appropriate physical security that is commensurate with the value of the IT assets protected by the TOE. |
| OE.NOEVIL | The integrators are trustworthy, act according to the guidance documentation, and are sufficiently qualified for this task. |

Table 2: Security objectives for the operational environment

Details can be found in the Security Target [ST].

# 5. Architectural Information

L4Re Secure Separation Kernel CC 1.0.2 is a microkernel-based operating system, where the functionality is split among the operating system kernel and multiple user land applications and that is configured to work as a separation kernel. Only the L4Re Microkernel runs in the most privileged CPU mode, where it provides the basic services needed to implement use-case-specific services and policies in isolated user land applications. This system architecture combined with the state-of- the-art, capability-based mandatory access control allows L4Re SSK to efficiently implement the Principle of Least Authority (POLA), which enables Zero Trust.

The L4Re Secure Separation Kernel CC consists of 7 components, 2 of which are optional. The core is the L4Re Microkernel, which provides capability-based access control, scheduling, secure memory management and inter-process communication (IPC), and which separates user-level components by employing hardware features for spatial and temporal isolation. The non-optional user-level components Sigma0, Moe, Ned, and Io provide core system features and are implemented in an unprivileged CPU mode on the basis of the L4Re Microkernel. These features include user-space memory management, secure device access, and scriptable application workload booting. The two optional components are the compartment communication proxies virtio-net-switch and NVMe server. The virtio-net-switch provides a virtual network for those compartments that may communicate but must not exchange capabilities. The NVMe server can provide persistent storage to several compartments that are completely separated and can and must not communicate with each other. The certification additionally includes a development guidance for compartment communication proxies that enables users of the L4Re Secure Separation Kernel CC to implement their own specialized compartment communication proxies to securely connect compartments.

# 6. Supplementary Cybersecurity Information

The evaluated documentation as outlined in table 1 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

The developers website as stated in chapter 2 provides the following supplementary information:

- the period during which support is offered (esp. security related updates)
- contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers: https://www.kernkonzept.com/cybersecurity-information/
- Vulnerabilities are listed on ENISA's European Vulnerability Database (EUVD): https://euvd.enisa.europa.eu/

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

# 7. IT Product Testing

All tests have been carried out by ITSEF: atsec information security GmbH,
Ismaninger Str. 19
81675 München
under the responsibility of certification Body

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87
Postfach 20 03 63
D-53175 Bonn

Please refer to chapter 1 for details on assurance levels or packages involved into testing.

The developer runs a test suite of more than 4500 automated tests, of which 288 tests check security critical functionality and were closely assessed during the evaluation.

The automated tests are API tests which test the TOE using its external interfaces, usually a specific TOE subsystem or object functions. The tests usually only involve the Sigma0,

the kernel, and Moe. There are special scenario tests which involve a more complex setup including proxy components like the NVMe server or virtio-net-switch.

All developer tests showed the expected results.

The evaluator conducted the independent and penetration testing by conducting the developer testing jointly with the developer as well as executing independent tests. These independent tests are fully automated test cases which -apart from compiling and execution- do not require specific pre- or post-conditions. The evaluator focused his testing on proper error handling and input sanitization considering the nature of the TOE being a separation kernel. All resources available to a third-party software stack have been subject to test. As these resources are partially provided by the TOE kernel, the Moe subsystem and the Ned subsystem, the evaluator concludes that the key subsystems of the TOE were covered by the evaluator testing.

All evaluator tests showed the expected results.

Please refer to chapter 8 for complete and precise information on settings and configuration of the TOE during the evaluation, including relevant operational notes and observations.

# 8. Evaluated Configuration

This certificate covers the following configurations of the TOE: The Target of Evaluation is the Kernkonzept L4Re Secure Separation Kernel CC, Version 1.0.2 (L4Re SSK). The TOE is software only and is accompanied by guidance documentation. The items listed in table 1 of this report represent the TOE.

The TOE requires hardware systems with the following components – additional hardware is considered a form factor which does not affect the security functionality of the TOE:

- x86_64 Intel CPU with any microarchitecture starting from Broadwell up to and including Meteor Lake and, additionally, with support for VT-x with EPT, and Intel IOMMU. If available, the latest microcode update must be applied by the BIOS.
- ARMv8 CPU: NXP LX2160A with support for ARM virtualization.

The hardware, which is also stated in section 1.3.5 of [ST], is not part of the TOE.

# 9. Results of the Evaluation

## 9.1. CC specific results

The ITSEF produced and provided the Evaluation Technical Reports (ETR) [ETR] according to the requirements of the Scheme [EUCC-VO],[EUCC_PROG], the Common Criteria [CC], the Common Evaluation Methodology [CEM], and all relevant interpretations and guidelines of the Scheme (AIS) [AIS].

On advise by the Certification Body and consent by the certificate holder the following guidance further specific for the technology of the product [AIS] were applied:

*(i) AIS 1 Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC*

*(ii) AIS 14 Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC*

*(iii) AIS 19 Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)*

*(iv) AIS 23 Zusammentragen von Nachweisen der Entwickler (Collection of Developer Evidence)*

*(v) AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema*

*(vi) AIS 38, Version 2, Reuse of evaluation results*

As a result of the evaluation, the verdict PASS is confirmed for the assurance components that are identified in chapter 1 of this report and claimed by the Security Target [ST] for the corresponding TOE. The corresponding TOE is identified in chapter 2 of this report.

The certificate

- is uniquely identified by: EUCC-3087-2026-04-0003, administration ID BSI-DSZ-CC-1177-V2-2026
- was issued on: 16 April 2026
- is valid until: 15 April 2031

The results of the evaluation are only applicable to the TOE as defined in chapter 1 and the configuration as outlined in chapter 8 above.

### 9.2. Results of cryptographic assessment

The TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

## 10. Obligations and Notes for the Usage of the TOE

Table 1: Deliverables of the TOE outlines the documents that contain necessary information on the intended use of the TOE including all security related information, conditions and instructions to be taken into account by the user. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target and not covered by the TOE itself need to be met by the operational environment of the TOE.

The customer or user of the TOE shall take the statements of this certificate into account in its system risk management process. The user should define measures in its risk management that respond to emerging and new attack methods and techniques to the TOE until the TOE has been reassessed.

The user also has to consider in its risk management the limited validity for the usage of cryptographic algorithms as outlined in chapter 9.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. Until the TOE has been re-certified, the user should examine the use of not yet certified updates and patches or take additional measures in order to maintain system security.

## 11. Security Target

For the purpose of publishing, the Security Target [ST] of the TOE / Information and communications technology (ICT) product is provided within a separate document as Annex A of this report.

# 12. Definitions

## 12.1. Acronyms

| | |
|---|---|
| **ACS** | Access Control Services |
| **AIS** | Application Notes and Interpretations of the Scheme |
| **API** | Application Programming Interface |
| **BIOS** | Basic Input/Output System |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **BSIG** | BSI-Gesetz / Act on the Federal Office for Information Security |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CC** | Common Criteria for IT Security Evaluation |
| **CEM** | Common Methodology for Information Technology Security Evaluation |
| **cPP** | Collaborative Protection Profile |
| **DMA** | Direct Memory Access |
| **EAL** | Evaluation Assurance Level |
| **EPT** | Extended Page Tables |
| **ETR** | Evaluation Technical Report |
| **ICT** | Information and communications technology |
| **IOMMU** | Input/Output Memory Management Unit |
| **IPC** | Inter Process Communication |
| **IRQ** | Interrupt Request |
| **ITAS** | In-Task Service |
| **IT** | Information Technology |
| **ITSEF** | Information Technology Security Evaluation Facility |
| **L4Re** | L4 Runtime-Environment |
| **L4ReSSK** | L4Re Secure Separation Kernel CC 1.0.2 |
| **MMU** | Memory Management Unit |
| **MMIO** | Memory-mapped I/O |
| **NVMe** | Non-Volatile Memory (NVM) Express |
| **PCI** | Peripheral Component Interconnect |
| **PCIe** | PCI Express |
| **PP** | Protection Profile |
| **SAR** | Security Assurance Requirement |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **ST** | Security Target |

| | |
|---|---|
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |
| **VT-x** | Intel® Virtualization Technology for x86 processors |

## 12.2. Glossary

**Augmentation** - The addition of one or more requirement(s) to a package.

**Collaborative Protection Profile -** A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

**Extension** - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

**Formal** - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

**Informal** - Expressed in natural language.

**Object** - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

**Package** - named set of either security functional or security assurance requirements

**Protection Profile** - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

**Security Target** - An implementation-dependent statement of security needs for a specific identified TOE.

**Semiformal** - Expressed in a restricted syntax language with defined semantics.

**Subject** - An active entity in the TOE that performs operations on objects.

**Target of Evaluation** - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

**TOE Security Functionality** - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

# 13. Bibliography

[EUCC-VO] Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
and
Implementation Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art document

[CC] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017

https://www.commoncriteriaportal.org

[CEM] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[EUCC_SOTA] EUCC state-of-the-art documents: https://certification.enisa.europa.eu/publications/eucc-state-art-documents_en

[EUCC_PROG] EUCC program of the BSI: Scheme documentation describing the certification process (EUCC), https://www.bsi.bund.de/zertifizierung

[EUCC_CERT] EUCC Certificates, periodically updated list published on ENISA's website on European cybersecurity certification schemes (https://certification.enisa.europa.eu/) but also on BSI's website (https://www.bsi.bund.de/zertifizierungsreporte)

[AIS] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[6] https://www.bsi.bund.de/AIS

[ST] Security Target for L4Re Secure Separation Kernel CC 1.0.2 BSI-DSZ-CC-1177-V2-2026, Version 2.1700, 2026-01-26, Kernkonzept GmbH

[ETR] Final Evaluation Technical Report, Version 1.1, 24.03.2026, atsec information security GmbH, (confidential document)

[ConfList] L4Re Secure Separation Kernel CC 1.0.2 Konfigurationsliste, Version 1.2, 2026-01-26, Kernkonzept GmbH (confidential document)

[ConfGuide] L4Re Configuration Guidance, Version 15, 2025-11-28, Kernkonzept GmbH

[DevGuide] Development Guidance for a Compartment Communication Proxy based on L4Re, Version 8, 2025-11-20, Kernkonzept GmbH

[FLR] Flaw remediation and incidence response at Kernkonzept, Version 9, 2024-10-21, Kernkonzept GmbH

[FLRGuide] L4Re problem reporting guide, Version 3, 2024-10-21, Kernkonzept GmbH

[6]See section 9.1 for detailed list of used AIS

# C. Annexes

## List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report