Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1177-2025

for

L4Re Secure Separation Kernel CC Version 1.0.1

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 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1177-2025 (*)

Operating System

L4Re Secure Separation Kernel CC, Version 1.0.1

from	Kernkonzept GmbH
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3
valid until:	17 February 2030

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) 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 the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 18 February 2025
For the Federal Office for Information Security

Sandro Amendola
Director-General

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. 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 conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 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

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification 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. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it 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 under SOGIS-MRA for all assurance components selected.

3.2. 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 3 EAL 2 and ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product L4Re Secure Separation Kernel CC, Version 1.0.1 has undergone the certification procedure at BSI.

The evaluation of the product L4Re Secure Separation Kernel CC, Version 1.0.1 was conducted by atsec information security GmbH. The evaluation was completed on 11 February 2025. atsec information security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: Kernkonzept GmbH.

The product was developed by: Kernkonzept GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, 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 Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are 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 re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 18 February 2025 is valid until 17 February 2030. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product L4Re Secure Separation Kernel CC, Version 1.0.1 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Kernkonzept GmbH
Buchenstraße 16 b
01097 Dresden
Deutschland

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the L4Re Secure Separation Kernel CC, Version 1.0.1 (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 Security Target [6] is the basis for this certification.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
Separation of Compartments	Compartments can only access those devices that are assigned to them in the initial configuration. Unauthorized memory accesses via DMA as well as device to device communications are prevented by utilizing appropriate hardware features (IOMMUs and PCI-ACS).
Information Flow Control	The communication channels present in the initial configuration determine the possible information flow between compartments for the entire runtime. Compartments can be configured to be isolated from each other (strong separation), to exchange data but no capabilities (capability separation), or to exchange data and capabilities (address space separation). Special purpose information flow properties can be achieved by connecting two compartments only via a compartment communication proxy.
System Management	The TOE configuration is defined with Lua scripts which allows the definition of objects and subjects (i.e. compartments) and to assign objects to subjects. The TOE does not provide management interfaces that allow system configuration at runtime.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions,

Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

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

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

L4Re Secure Separation Kernel CC, Version 1.0.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	l4re_ssk_cc_lx2160a.zip (Hashwert: f2b9256e72b2317acc51cd72e8743edb42c75f37)	1.0.1	Compressed zip archive for LX2160A with SMMU
2	SW	l4re_ssk_cc_x86_virt.zip (Hashwert: 057aff5ed3a4a4ba8f642e47298f28e9997c9464)	1.0.1	Compressed zip archive for x86 with VT-x enabled
3	SW	l4re_ssk_cc_x86_novirt.zip (Hashwert: 433edf0f54fd869d515ec8f6524de48060583657)	1.0.1	Compressed zip archive for with VT-x disabled
4	Doc	l4re_ssk_cc_customer_doc.zip	1.0.1	Compressed zip archive of TOE documentation (see #6 and #7)
5	Doc	l4re_ssk_cc_interface_and_usage_documentation.zip	1.0.1	Compressed zip archive L4Re Interface and Usage Documentation; separately available
6	Doc	L4Re Configuration Guidance.pdf	14	Guidance included in #4
7	Doc	Development Guidance for a Compartment Communication Proxy based on L4Re.pdf	7	Guidance included in #4

Table 2: Deliverables of the TOE

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.

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 enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. 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 [6].

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 aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

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 3: Security objectives for the operational environment

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

L4Re Secure Separation Kernel CC, Version 1.0.1 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, Version 1.0.1 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) 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 which can not 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, Version 1.0.1 to implement their own specialized compartment communication proxies to securely connect compartments.

6. Documentation

The evaluated documentation as outlined in table 2 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.

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

7.1. Test Configuration

The evaluator tests were executed together with the developer tests using the same test harness employed by the developer.

The following test environment was used for conducting testing:

- Test system hardware: The evaluator verified that a hardware platform consistent to the hardware stated in [6] was provided. Specifically, the following hardware was made available to the evaluator:
  - Intel: Shuttle DS10U7 with Intel Intel Core i7-8565U CPU (Broadwell architecture) offering support for VT-x with EPT and Intel IOMMU. The evaluator verified that VT-x, EPT and IOMMU were activated by the BIOS.
  - ARM: R-Car-M3
  - ARM: LX2160A with support for SMMU
- Test system software: The evaluator verified that the TOE binaries version 1.0.1 were provided along with the associated source code.
- Test case software: The evaluator verified that the TOE test cases were provided with the TOE source code. The evaluator concluded that the test case version is therefore inherently consistent with the TOE software version.

To support the evaluator, the developer provided access to a build environment that allows creation of the test case binaries from the developer's test case sources as well as the evaluator independent test case sources.

Based on the conducted analyses, the evaluator concluded that the test hardware, software and test cases, and thus the test configuration was consistent with the configuration under evaluation as specified in [6].

7.2. Developer Testing

The developer runs a test suite of more than 200 automated tests.

Testing Approach

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.

Test Configuration

The automated tests are performed for each supported platform defined in the ST:

- x86_64 Intel CPU with Broadwell microarchitecture or later, support for VT-x with EPT, Intel IOMMU, the latest microcode applied by the BIOS
- ARMv8 CPU: NXP LX2160A with support for ARM virtualization

Not all tests do apply for all platforms as some do verify platform-specific functions.

Verdict

All test results for the relevant test cases show a 'PASS' verdict.

7.3. Evaluator Testing

The evaluator conducted the independent 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.

Test Approach

The evaluator developed fully automated test cases. These test cases were written such that they can be embedded into the developer's test harness which implies that the test cases establish all required test conditions, execute the test operation and validate the expected result. The user is returned only an indicator whether the test succeeded or failed.

Test Configuration

The evaluator configured the TOE compliant to the guidance specifying the evaluated configuration. For well-defined tests intending to validate the behaviour of TOE components that are not configurable, the evaluator decided to have a configuration that is not fully compliant to the evaluated configuration - the deviations have been reviewed to not affect the tested functionality. In addition, all hardware systems outlined in the ST were used during the testing. Each evaluator test case contained its own Ned LUA configuration to specify its initial environment.

Verdict

All tests showed the expected results. Thus, the evaluator concluded that the TOE behaves as expected with respect to the tested functionality.

7.4. Penetration Testing

The evaluator conducted the penetration testing by conducting the developer testing jointly with the developer as well as executing independent tests.

Test Approach

The evaluator used the same test setup as for independent testing.

Test Configuration

The evaluator configured the TOE compliant to the guidance specifying the evaluated configuration. For most of the test cases, however, the evaluator only instantiated the TOE components that are intended to be tested to ensure that other TOE components cannot interfere. This is considered appropriate, because the evaluated configuration does not change the behaviour of the TOE components, but only ensures that compartments have a disjoint set of resources. Yet, one test case complies with the evaluated configuration by using the designated LUA service functions to establish separated compartments. In addition, all hardware systems outlined in the ST were used during the testing. Each evaluator test case contained its own Ned LUA configuration to specify its initial environment.

Verdict

All tests showed the expected results. Thus, the evaluator concluded that the TOE behaves as expected with respect to the tested functionality.

8. Evaluated Configuration

This certification covers the following configurations of the TOE: The Target of Evaluation is the Kernkonzept L4Re Secure Separation Kernel CC, Version 1.0.1 (L4Re SSK). The TOE is software only and is accompanied by guidance documentation. The items listed in table 2 of this report represent the TOE.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant

- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.3

The results of the evaluation are only applicable to the TOE as defined in chapter 2 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

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

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. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage 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 [6] of the Target of Evaluation (TOE) 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
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
L4Re SSK	L4Re Secure Separation Kernel CC 1.0.1
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

[1] 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

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

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1177-2025, Version 2.14, 2025-02-10, Security Target for L4Re Secure Separation Kernel CC, Version 1.0.1, Kernkonzept GmbH

[7] Final Evaluation Technical Report, Version 2, 2025-02-04, atsec information security GmbH, (confidential document)

[7] specifically

- AIS 1 Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC
- AIS 14 Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC
- AIS 19 Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 23 Zusammentragen von Nachweisen der Entwickler (Collection of Developer Evidence)
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[8] L4Re Secure Separation Kernel CC, Version 1.0.1 Konfigurationsliste, Version 1.0, 2024-11-18, Kernkonzept GmbH (confidential document)

[9] L4Re Secure Boot Guidance, 2022-10-07, Kernkonzept GmbH

[10] L4Re Configuration Guidance, Version 13, 2024-08-19, Kernkonzept GmbH

[11] Development Guidance for a Compartment Communication Proxy based on L4Re, Version 7, Date 2024-10-21, Kernkonzept GmbH

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report