Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1185-2023

for

PikeOS Separation Kernel v5.1.3 for the NXP LS 1023A/LS1043A Processor, Version 3.1.0

from

SYSGO 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-1185-2023 (*)

Operating System

PikeOS Separation Kernel v5.1.3 for the NXP LS 1023A/LS1043A Processor
Version 3.1.0

from	SYSGO SAS
sponsored by	SYSGO GmbH
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, AVA_VAN.5
valid until:	17 September 2028

SOGIS
Recognition Agreement
for components up to
EAL 4

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 and by advice of the Certification Body for components beyond EAL 5 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 September 2023

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Director-General

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 according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components ADV_FSP.5, ADV_IMP.2, ADV_INT.2, ADV_TDS.4, ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_FLR.3, ALC_TAT.2, ATE_DPT.3, AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

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.

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

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. 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 PikeOS Separation Kernel v5.1.3 for the NXP LS 1023A/LS1043A Processor, Version 3.1.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1146-2022. Specific results from the evaluation process BSI-DSZ-CC-1146-2022 were re-used.

The evaluation of the product PikeOS Separation Kernel v5.1.3 for the NXP LS 1023A/LS1043A Processor, Version 3.1.0 was conducted by atsec information security GmbH. The evaluation was completed on 1 September 2023. atsec information security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: SYSGO GmbH.

The product was developed by: SYSGO SAS.

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.

[5] Information Technology Security Evaluation Facility

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 September 2023 is valid until 17 September 2028. 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,
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 PikeOS Separation Kernel v5.1.3 for the NXP LS 1023A/LS1043A Processor, Version 3.1.0 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] SYSGO SAS
54 route de Sartrouville
78230 LE PECQ
France

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 PikeOS Separation Kernel v5.1.3 for the NXP LS1023A/LS1043A Processor. It consists of the PikeOS Kernel and System Software instantiated with an Armv8 ASP and extended with BSP components for the NXP LS1023A/LS1043A Processor hardware platform (featuring an Arm Cortex-A53 core processor with 4 cores for LS1043A, 2 cores for LS1023A): PSP, HWVIRT Hypervisor driver (as kernel device driver), CLKMGR driver (as kernel device driver), and e1000 driver (as external file provider in a normal partition).

The TOE is a Separation Kernel, which allows to effectively separate multiple applications running on the same platform from each other. Such applications can range from small bare-metal programs up to entire operating systems. Non-privileged applications may be malicious, and even in that case the TOE ensures that malicious applications are neither capable of harming other applications nor the TOE itself.

SYSGO defines separation as follows: The TOE separates partitions by managing their accesses to and usage of resources, such as memory, devices, processors, and communication channels, as defined by the configuration. Isolation of a partition is the absence of communication with other partitions, except partitions hosting the components implementing the system API, when no communication channels or shared resources between the partition and other partitions are configured. Isolation is a special case of separation. Additionally, the TOE has the characteristics of an embedded real time operating system. Thus, the partitioning is configured statically and the TOE does not include typical desktop operating system services (e.g. user login, printer drivers). The TOE will typically be installed and operated on a hardware platform suitable for embedded systems.

- Separation in space of applications hosted in different partitions from each other and from the PikeOS Operating System according to the configuration data,
- Separation in time of applications hosted in different partitions from each other and from the PikeOS Operating System according to the configuration data,
- Control of information flows between applications hosted in different partitions via assigning to the partitions communication objects and access rights to those,
- Management of the TOE (e.g. system partition API) and the TOE data (e.g. threads, tasks).

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

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 5 augmented by ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 8.1. 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
TSS_SSA	Separation in space of applications hosted in different partitions from each other and from the PikeOS Operating System according to the SSP by using the underlying hardware, as shown by the red lines in Figure 1 in the ST [6]. Applications can be hosted in different partitions. Partitions get assigned resources (i.e. space) according to the SSP, which comprise memory ranges and a set of CPUs. The TSF enforces the corresponding part of the SSP by the enforcement of access control on partition content, per-partition provision of physical memory space and allocated CPU time for each CPU. By confining non-privileged executables into partitions, the TSF enforces that these applications can affect neither applications in other partitions nor the PikeOS Operating System itself.
TSS_STA	Separation in time of applications hosted in different partitions from each other and from the PikeOS Operating System according to the SSP. Applications can be hosted in different partitions. Partitions get assigned CPU time (i.e. time windows) according to the SSP. The TSF enforces the corresponding part of the SSP by per-partition allocation of a predefined amount of CPU time for each CPU. On a partition switch CPUs will be reused.
TSS_COM	Provision and management of communication objects. Applications hosted in different partitions can get assigned a set of communication objects. A communication object is an object exposed to one or multiple partitions with access rights as defined in the configuration data, thus allowing communication between partitions.
TSS_MAN	Management of the TOE (e.g. system partition API) and the TOE data (e.g. threads, tasks). The TOE restricts a non-privileged application to only manage tasks and threads within its partition. The TOE provides an API to privileged applications to manage the TOE and the TOE data.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 9.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 5.1. 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], chapters 5.2, 5.3 and 5.4.

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:

PikeOS Separation Kernel v5.1.3 for the NXP LS 1023A/LS1043A Processor,
Version 3.1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	PikeOS Microkernel for Armv8	pikeos-kernel-cert-arm_v8hf-5.1-20592.x86_64.rpm SHA-256: a948e9b8fd09769e483e87d0409a36a2\ 75616ca3b8071c5bdaed1e5b47872195	from ISO
2	SW	PikeOS System Software for Armv8	pikeos-ssw-cert-arm_v8hf-5.1-4562.x86_64.rpm SHA-256: 2499e9fd8a57438ee38d4933c89d220a\ 7c4a82252745037806cdfc53603a395b	from ISO
3	SW	PikeOS Hardware Virtualization Hypervisor for Armv8	pikeos-hwvirt-hypervisor-arm_v8hf-5.1-817.x86_64.rpm SHA-256: fe169e669554c2e4faaaa11d9f4a5ebc\ 5bb50e64b335ca210f447804054e3dcb	from ISO
4	SW	18109 Platform Support Package	pikeos-p18109-psp-18109-arm_v8hf-5.1-89104.x86_64.rpm SHA-256: f8637fcb917bd0edf3a2ca83c2cdadeb\ 6eecb16f57a2bd360cc61f0a8f2d1dad pikeos-p18109-config-psp-18109-arm_v8hf-5.1-89104.x86_64.rpm SHA-256: 3838281ea93e1d85a074d127be9ee5df\ c7e2167f7a1d65705df5443a00ab2ee7	from ISO
5	SW	18109 Clock Manager	pikeos-p18109-hwvirt-eeh-clock-manager-arm_v8hf-5.1-131631.x86_64.rpm SHA-256: 454db2e4909ae88bf6c3769f28040249\ 41faf4da6b7c5c537975fc09e3eeaf81	from ISO
6	SW	18109 PikeOS e1000 driver	pikeos-p18109-e1000_fp-cert-210-arm_v8hf-5.1-36984.x86_64.rpm SHA-256: 4c97a5b03bad29d162b3f6fe2f0ca2db\ 176717349c5e632cd31f4121c18d1db9 pikeos-p18109-e1000_fp-cert-config-arm_v8hf-5.1-36984.x86_64.rpm SHA-256: 0b7b86f5ba831b2e58571b2d1c7b5b03\ 3c8a624d3efb487a716748a0dd9a948c	from ISO
7	DOC	PikeOS User Manual	pikeos-doc-fundamentals-5.1-1077.noarch.rpm SHA-256: c3bdd123fc0e3c6ac612062437f088a0\ 4a07a2707e6436c27ef41972f62ef077	from ISO
8	DOC	PikeOS Installation Guide	pikeos-doc-installationguide-5.1-112.noarch.rpm SHA-256: 13ad083d5ce7c1ab323dabfed8ae229d\ 24313f4385cb26ed2f288aff796245eb	from ISO
9	DOC	PikeOS Kernel Reference Manual	pikeos-doc-kernelref-5.1-297.noarch.rpm SHA-256: 261f060d456ec8a34d6dfd2de2c062c4\ 97b5449b58284ca66c0f0d2b655661dd	from ISO
10	DOC	PikeOS System Software Reference Manual	pikeos-doc-psswref-5.1-321.noarch.rpm SHA-256: 56ecd5bf36ded1cf53effefbb09b2b98\ b624dde5ad2ca309ff9cd905478e19bf	from ISO
11	DOC	PikeOS Device Driver Programming Reference Manual	pikeos-doc-drvref-5.1-305.noarch.rpm SHA-256: bd36e8b97ce4b5e8eb2cb458a8f261c4\ fde8b7376d050746559fd445e5c0ef20	from ISO

No	Type	Identifier	Release	Form of Delivery
12	DOC	PikeOS PSP and KDEVDeveloper's Guide	pikeos-doc-pspdevguide-5.1-281.noarch.rpm SHA-256: beb01adac2c23d44ecb0a9cf45e33251\ 4ce93b9fd6dfdcd6390c35a069581897	from ISO
13	DOC	P4EXT PikeOS Native Personality Extensions	pikeos-doc-p4ext-5.1-87.noarch.rpm SHA-256: a35ac8a76908f4f82bb0df9a443fd338\ 5c916208c40276cf35dc1f9dbd1cc056	from ISO
14	DOC	CENV C Language Programming Environment	pikeos-doc-cenv-5.1-41.noarch.rpm SHA-256: b7cc316394bacb72f912b53872aafee5\ b6e3c481f370247dbed9fa6c63963158	from ISO
15	DOC	PikeOS Platform Manual for ARM v8-A 64-bit Boards	pikeos-doc-platarm64-5.1-597.noarch.rpm SHA-256: c61258d7b610df4f6de655b7931686cd\ 8401aa1968816f5e562c78e6993c8924	from ISO
16	DOC	PikeOS Armv8 Generic Certification Kit	PikeOS Armv8 Generic Certification Kit pikeos-certkit-gen-asp-arm_v8hf-5.1-353.noarch.rpm SHA-256: 754f275945bf46792bc0e3842060766\ 1c75375c85305f4d5fc3471f36cc589dc pikeos-certkit-gen-conf-arm_v8hf-5.1-353.noarch.rpm SHA-256: 82c7e5b0ce760b908ed5a8f\ 5985fe997738b1098f137441832de0c213a62aa6a pikeos-certkit-gen-libs-arm_v8hf-5.1-353.noarch.rpm SHA-256: d70127908687dbe3b0e82bc\ a01b195e2c18e2c2f10e5f4146986abdcc6da8f74 pikeos-certkit-gen-kern-arm_v8hf-5.1-353.noarch.rpm SHA-256: 248778905d2fab83a93e80e\ 5925b6fe4570748c41106bee83270ae634a0666b1 pikeos-certkit-gen-pgen-arm_v8hf-5.1-353.noarch.rpm SHA-256: c76ed7f3555f790c6c82b44\ 6d8dd6df405365d7405009b692ae80117acf484d6 pikeos-certkit-gen-pssw-arm_v8hf-5.1-353.noarch.rpm SHA-256: 8176e79590077c76f2df2eb\ 0dee6a9b11b063264d3a68aabee274c941509fb4d pikeos-certkit-gen-sm-arm_v8hf-5.1-353.noarch.rpm SHA-256: 3e11eaf2874a5fed4ffadaf\ 561412dfa249824a340663fa9e9db0570d2edc201 pikeos-certkit-gen-usermanual-arm_v8hf-5.1-92.noarch.rpm SHA-256: 613f83524ef082a7f296246\ 7dbdbdcdfc43368e0a1b52f9061cceb9de1a526bd	from ISO

No	Type	Identifier	Release	Form of Delivery
17	DOC	PikeOS Armv8 Generic Certification Kit	pikeos-certkit-gen-asp-arm_v8hf-5.1-353.noarch.rpm SHA-256: 754f275945bf46792bc0e3842060766\ 1c75375c85305f4d5fc3471f36cc589dc pikeos-certkit-gen-conf-arm_v8hf-5.1-353.noarch.rpm SHA-256: 82c7e5b0ce760b908ed5a8f\ 5985fe997738b1098f137441832de0c213a62aa6a pikeos-certkit-gen-libs-arm_v8hf-5.1-353.noarch.rpm SHA-256: d70127908687dbe3b0e82bc\ a01b195e2c18e2c2f10e5f4146986abdcc6da8f74 pikeos-certkit-gen-kern-arm_v8hf-5.1-353.noarch.rpm SHA-256: 248778905d2fab83a93e80e\ 5925b6fe4570748c41106bee83270ae634a0666b1 pikeos-certkit-gen-pgen-arm_v8hf-5.1-353.noarch.rpm SHA-256: c76ed7f3555f790c6c82b44\ 6d8dd6df405365d7405009b692ae80117acf484d6 pikeos-certkit-gen-pssw-arm_v8hf-5.1-353.noarch.rpm SHA-256: 8176e79590077c76f2df2eb\ 0dee6a9b11b063264d3a68aabee274c941509fb4d pikeos-certkit-gen-sm-arm_v8hf-5.1-353.noarch.rpm SHA-256: 3e11eaf2874a5fed4ffadaf\ 561412dfa249824a340663fa9e9db0570d2edc201 pikeos-certkit-gen-usermanual-arm_v8hf-5.1-92.noarch.rpm SHA-256: 613f83524ef082a7f296246\ 7dbdbdcdfc43368e0a1b52f9061cceb9de1a526bd	from ISO
18	DOC	PikeOS HWVIRT Generic Certification Kit	pikeos-certkit-hwvirt-gen-analysis-arm_v8hf-5.1-36.noarch.rpm SHA-256: 8443b999306fefac8bf04f8ef7d6c1b\ c1f73944c0d2c86a8c5f60826aa98dc55 pikeos-certkit-hwvirt-gen-artefacts-arm_v8hf-5.1-123.noarch.rpm SHA-256: 89daf06b0a90765becdb8e9b4590244\ e43a844fc9e2f8ce0372424907ccde515 pikeos-certkit-hwvirt-gen-usermanual-arm_v8hf-5.1-41.noarch.rpm SHA-256: 04d52c2a9fe46aac294f669a60edbbb\ 7d07e1f313c278a1ae118c13ee434080f	from ISO
19	DOC	18109 PikeOS BSP Genric Certification Kit	pikeos-certkit-generic-18109-arm_v8hf-5.1-279.noarch.rpm SHA-256: 5916183aa735c6c20ec04080accc55f\ 8b98cbfa96dbd3d26502ddc5efeb263dc	from ISO
20	DOC	Security Bulletin 18109 PikeOS BSP	pikeos-p18109-certkit-cc-secbul-5.1-287.noarch.rpm SHA-256: fabed1a44677566e69c9a36639f9dc4\ 847917338486ef53cd7d5b0261843b49c	from ISO

Table 2: Deliverables of the TOE

The RPMs listed with their checksum in the sections of the table for each architecture become locally available on the user's development computer upon installation of the

corresponding main PikeOS distribution ISO images (see below). In addition, the user installs the listed CERTKIT ISO images also used to deliver the current PikeOS security bulletin.

2.1. Overview of Delivery Procedure

The TOE is delivered to the customer (human TOE user) by means of RPMs. These are contained in ISO images, in turn made available for download from an FTP-server. These ISO images are not explicitly listed in the ST. They can additionally contain non-TOE components. The customer receives the download link to the ISOs as part of a delivery mail sent by the developer. The TOE and all guidance documents are extracted from the RPMs by the PikeOS installer. The PikeOS 5.1 Installation Guide is additionally available for download and contains the instructions to run the installer.

2.2. Identification of the TOE by the User

The integrator (human TOE user) identifies the TOE by inspecting the file names of the downloaded ISO-images and comparing the SHA-256 hash of each of these with the ones quoted in the corresponding signed SHA-256-files. The integrity of latter files is verified with the help of GPG. This process is described in the delivery mail. The integrity of the installation is verified by running a script that computes the checksums of the packaged RPMs. This process is described in the CERTKIT manuals. The CERTKIT ISO-images which include the relevant guidance and the verification scripts are themselves verified by comparing their checksums with those from the Security Target [6].

The TOE is only one element of the product PikeOS delivered by means of the ISO-images and needs to be combined with other components by the integrator in order to execute it on the target platform. The required steps are described in PikeOS User Manual (see item 7 in table 2) with details contained in further documents listed above.

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:

- memory access control policy
- file access control policy
- communication port access control policy
- interrupt access control policy
- PSP-specific services access control policy
- CPU core access policy
- IPC and event communication policy

Specific details can be found in chapter 8 of the Security Target [6].

The detailed implementation of the specified security policy is defined by the integrator who performs the static configuration of the TOE and referred to as the System Security Policy (SSP).

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.PRIVILEGED_EXECUTABLES All privileged executables are approved by the integrator. The integrator thereby takes responsibility that the privileged executables have been developed according to the TOE User Manuals and do not violate the SSP.

OE.HARDWARE The underlying hardware, firmware and bootloader needed by PikeOS to guarantee secure operation provide the necessary properties, are working correctly and have no undocumented security critical side effect on the functions of the TOE. The hardware must fulfil the following requirements, as explained in the TOE User Manuals:

- Provide CPU(s) with at least two privilege modes (“user” and “supervisor” mode). Only the TOE itself and privileged executables may run in the “supervisor” mode. Non-privileged executables always run in “user mode”. In “user mode”, only a limited set of instructions is available; in “supervisor mode”, all instructions are available.
- The hardware shall have a MMU, which is capable of restricting accesses (e.g. destinations of load and store CPU instructions) of non-privileged executables to certain memory regions. The MMU shall only be configurable from a privileged CPU mode, thus, it can only be configurable through the TOE to configure the policies specifying these access restrictions. These policies are part of the SSP. During TOE run time, these policies are represented as page tables used by the MMU.
- The hardware (CPU or CPUs) shall provide instructions to switch between privilege modes and to use the memory management to set up different segments of memory.
- The hardware (CPU or CPUs) shall allow the TOE to reuse CPU(s) for different non-privileged executables, in a way that there is no residual information flow through CPU registers across a partition boundary.
- The hardware shall provide default values for security-relevant settings at power-on (e.g. program counter, detailed instructions shall be included in the hardware reference manual). This supports the TOE reaching the initial safe and secure state.
- If the hardware possesses any other active components beside CPUs or CPUs have operating mode(s) not under control of PikeOS, then the hardware shall provide support either to turn these components completely off or to control them as described in the TOE User Manuals. For example, if a device accessible by non-privileged executables can execute DMA, then all DMA shall be switched off or, in order to control DMA, the hardware shall provide an I/O MMU, with an I/O MMU driver protected by the PikeOS Operating System.

Specific requirements to the ARMv8 architecture (Cortex-A53) are:

- The processors are operated in 64-bit mode.
- Memory Management Unit (MMU) with Virtual Memory System Architecture.
- Vector Floating Point (VFP) / Advanced SIMD (Neon) extension.

The timer facilities provided by the hardware shall be sufficient for the timing requirements (e.g., timer resolution) of the product based on PikeOS. The CPU-specific requirements

are met by all ARMv8 CPUs specified in the TOE User Manuals for the selected CPU architecture.

OE.EXCLUSIVE_RESOURCES All resources required by the PikeOS Operating System, its privileged executables, and its non-privileged executables are exclusively controlled by the TOE.

OE.PHYSICAL The IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

OE.TRUSTWORTHY_PERSONNEL The personnel configuring and integrating the TOE (integrator) and those installing and operating the TOE (system operator) are trustworthy, act according to the TOE User Manuals, and are sufficiently qualified for this task.

5. Architectural Information

The elements that form the TSF for this evaluation are the PikeOS System Software "PSSW" (without any System Extension) and the PikeOS microkernel "KERN" (including the PikeOS ASP, the PikeOS PSP), as well as the HWVIRT Hypervisor driver to add hardware virtualization support and CLKMGR as a Clock Manager. Both are implemented as Kernel Level Device Driver. Included in the TOE scope, but not the TSF, is also a e1000 driver implemented as a PikeOS External File Provider running in a normal partition.

The PSP, KERN and PSSW may be thought of as three layers living on top of a hardware platform featuring the supported CPU architecture ARMv8, Cortex-A53. On top of the PSSW sits a configurable number of "partitions" that can contain different types of applications (including adapted versions of whole operating systems). The TOE itself has a limited set of features, compared to what would be expected from a general-purpose operating system, but ensures that the applications in different partitions cannot interfere in unwanted ways, within the description provided by the Security Target [6].

The TOE is a microkernel-based operating system and, therefore, exposes a security architecture that – at a generic level – is quite similar to the one that almost every operating system has. The specifics of the TOE are the limited complexity of the kernel (i.e. the parts of the TOE that execute with highest privileges) and the real-time capabilities. Also specific is the aspect that the TOE itself does not have the abstraction of a "human user" directly interacting with the TOE.

Another specific of the TOE is the static nature of the applications running on an instance of the TOE. Those are defined when the instance of the TOE is built by the system integrator. This reflects the main usage area of the TOE as an operating system for embedded systems.

The TOE is designed as a separation kernel that separates individual partitions from each other. A static number of partitions is defined when a product based on PikeOS is built. Partitions may communicate with each other using communication ports provided by the TOE. Such communication capabilities between partitions are also defined at build time.

The PikeOS microkernel (also kernel or KERN subsystem) takes many of the responsibilities kernels have in other operating systems, including hardware abstraction, the management of threads and tasks or exception handling. With respect to the security features of the TOE, it is in charge of performing the partitioning of resources (memory and time). The KERN subsystem runs with highest privileges.

The PSSW resides in user space. It takes care of the partitioning and inter-partition communication according to the configuration. After initialization, it acts as a server

providing services to applications inside the various partitions. The PSSW can also be viewed as a partition with the full set of abilities. This important property distinguishes it from normal partitions whose separation PikeOS guarantees.

The KERN and the PSSW implement the security functionality of the TOE, but PSP, HWVIRT and CLKMGR execute in the same security domain (in contrast to the e1000 driver which executes in a normal partition).

To define the precise behaviour of the TOE (including its detailed SFPs), its integrator needs to make a number of configuration choices. Most importantly, PikeOS has some elements that are statically defined in a table called the "Virtual Machine Initialization Table" (VMIT). Among those are:

- Resource Partitions:

A Resource Partition defines a sort of "container" for applications to run in. It consists of memory, I/O resources, predefined processes, file services, and communication ports assigned to each partition. It also gets a set of "abilities" (privileges to call specific system services) assigned.

- Process or Task:

A task or process is represented by an address space within a resource partition. The task is the abstraction that KERN knows while the PSSW adds some semantics to a task, which makes it a "process" for the PSSW.

Tasks build a hierarchy within a resource partition. A child task can inherit the abilities of its parent task, but the parent task can also decide to restrict the abilities of a child further when it creates the child.

The configured processes are the "root" tasks of a resource partition. They inherit all the abilities that are assigned to its resource partition.

- Thread:

Threads are the active entities within a task. A thread inherits the security attributes of its task, including the abilities assigned to the task the thread belongs to.

- Abilities:

Abilities are specific privileges that can be assigned to a resource partition. The abilities determine which "privileged" system calls can be invoked. As described above, tasks within a resource partition may have less abilities than are assigned to the partition they belong to, but they can never have more abilities than are assigned to the partition itself.

Note that the Security Target [6] does not explicitly mention abilities, although they are an important PikeOS concept. The reason is that there is a relationship between abilities and "normal partitions"/"system partitions". System partitions possess one or more abilities from a set of abilities given in the PikeOS User Manual (see item 7 in table 2). Except for two abilities that are common to all partitions, normal partitions do not possess any of these. A number of abilities are reserved for the PSSW and not available to others.

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 test setup differed between the ITSEF and the developer site with respect to the deployment of the integrated TOE to the target platform. While the ITSEF executed the tests on a single target platform, the developer maintains a sophisticated test setup to execute tests on a larger variety of systems in a fully automated fashion. However, the developer and evaluator testing were based on the same test framework. Details of both approaches, as well as the penetration testing, are described in dedicated sub-sections below. At the end of each, a short summary of the test results is given.

7.2. Developer Testing

Testing Effort

The developer uses an automated test framework to cover most of the functionality.

The test suites also contain manual tests which prompt the tester for confirming assertions, e.g. that a certain statement is included in the guidance or interface specification.

Test Approach

Most of the tests are executed automatically. The testing involves the compilation of the test code and the TOE on a developer system and uploading the result to the target test system. The developer uses an intermediary between the developer system and the TOE, which receives the test request, determines which of the attached test targets (i.e. platform) it is aimed for, restarts that test target and provides the TOE instance (including the test application) as network-bootable image. Finally, it returns the test results to the developer system.

Some of the tests require a manual check by the tester. This check is integrated into the test run such that it waits for a developer response on a specific item and, depending on the answer, it marks the test as "pass" or "fail" and integrates it into the test result log together with all other tests.

The testing is done very systematically. For this, the developer uses a document system that allows specifying functional/design requirements identified by a specific ID (Req. ID) to which statements in the respective evidence documents are linked and which are then systematically covered by test cases. In that way, also for very detailed behaviour requirements, it is always clear whether and where it has been tested.

Test Depth

The developer tests are very detailed in testing of functional interface behaviour. Usually, all possible error codes of a function are covered. These return codes are used in test code as expected results for the tested functionality. The developer focuses on testing all behaviour by stimulating the external interfaces. In some cases a source code or guidance inspection is used as alternative test method.

In addition, to better verify internal functions, the test framework uses libraries allowing the replacement of symbols to inject code which can log to the test host documenting interactions between for example the PSP and kernel.

The tested TOE is complete with regard to the evaluated components with the exception of the E1000 driver and its partition. This partition is only configured and active as part of the E1000 tests.

Configuration

All tests are performed on the official TOE version. The used installation images were the following:

- R5p1_PIKEOS_ARM_V8HF_S6510.amd64.iso
- R5p1_PIKEOS_ARM_V8HF_HWVIRT_S7000.amd64.iso
- R5p1_PIKEOS_18109_PIKEOS_BSP_S7010.amd64.iso

Test results

The developer tests showed a number of failures for which the evaluator could verify that these do not affect the evaluated functionality.

All relevant tests were successful.

7.3. Evaluator Testing Effort

Testing Effort

Beginning with September 2022, until March 2023, the evaluator ran the developer tests on the test machine. During the evaluation the test suites as well as the TOE received updates. The tests on the final TOE version in February/March showed all relevant tests running successfully.

The evaluator rerun relevant developer test sets. Many test sets perform a number of tests, and each test can check several requirements.

Test Approach

Given that the TOE is unchanged with regard to the core components that implement security functions and because ATE_COV and ATE_DPT analysis showed a systematic coverage of the TOE functionality by vendor, the evaluator reran the majority of the developer test suites focusing on suites covering the new TOE components. One test suite (HLRQ), which verifies a broad range of security-functions, was also executed.

Test Depth

While the component-specific test suites test the HWVIRT, PSP, CLKMGR, and E1000 TOE parts, the HLRQ test suite covers a broad range of high-level requirements. It basically touches all SFRs from the ST.

Test Configuration

The test setup was based on the images R5p1_PIKEOS_ARM_V8HF_S6510.amd64.iso, R5p1_PIKEOS_ARM_V8HF_HWVIRT_S7000.amd64.iso and R5p1_PIKEOS_18109_PIKEOS_BSP_S7010.amd64.iso and was run on an ARMv8 64bit platform (LS1043A RDB reference board using the rev 1.1 SoC). The target system was connected to the development system (where the TOE image is build together with the applications within the resource partitions) via network for TFTP boot and also connected via serial line to receive the test output. The evaluator received the test framework of the developer, which

allowed the automation of all test phases, including test and TOE instance compilation, linking, upload to the target platform, execution, and result observation.

The tested TOE is complete with regard to the evaluated components with the exception of the E1000 driver and its partition. This partition is only configured and active as part of the E1000 tests.

Test results

All tests passed and did not indicate any relevant deviation from the expected TOE behaviour.

7.4. Evaluator Penetration Testing

Overview

The penetration testing was performed using the test environment of the ITSEF.

The tests were developed by the evaluators and executed on the NXP LS1043A ARM platform described in the ST. The second supported platform, with LS1023A processor, has an almost identical SoC with the main difference being a smaller number of cores (2 instead of 4). This difference is deemed irrelevant for the design and results of the penetration tests.

The overall outcome is that no deviations were found between the expected and the actual test results. Moreover, no attack scenario with the attack potential High was actually successful.

Testing effort

The evaluators devised penetration tests that require execution on the actual hardware.

Penetration testing approach

The designed penetration tests use only external interfaces of the TOE, which was sufficient to verify the flaw hypotheses defined during the vulnerability analysis.

The penetration testing leveraged the use of the developer's test framework, which was also used for the ATE_IND testing.

For the re-certification new tests were devised to target the HWVIRT subsystem which was considered a major addition to the new TOE.

Test configurations

The penetration testing was performed on the TOE version 5.1.3. To unambiguously identify the TOE, the checksums of the installed RPMs were also checked against those from the current ST [6]. Apart from the TOE version and supported platforms, no further restrictions or configurations were defined for the evaluated configuration that would have to be applied to the test setup.

Testing depth

The tests directly covered three of the TOE subsystems, others are covered indirectly. The focus has been on critical subsystems at the attack surface.

As stated earlier, for some tests the evaluator did not use the libraries provided by the developer to use the TOE interfaces, but accessed the TSFI directly to have greater control over the interface parameters. One such case was the test of the PSSW daemon fuzzing, where IPC communication messages were crafted by hand (which would otherwise be constructed by the VM API library when calling a certain VM function) and

were then sent to the PSSW daemon via IPC messages. The other case was the test of the system call number checks , where the system calls were not executing using the kernel P4 API, but executing the system call assembler instruction provided by the respective TOE platform.

Test results

In summary, the tests did not show any deviation from the expected behaviour that would violate the security policies of the TOE.

Verdict for the sub-activity

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE's operational environment as defined in [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE: The evaluated configuration of the TOE is obtained by installing the Certification Kit ISO-images that are part of the TOE delivery on the development host and configuring and integrating the TOE according to the TOE guidance.

The TOE in the evaluated configuration provides the following security features (See the Security Tagregt [6] for all details):

- TSS_SSA: Separation in space of applications hosted in different partitions from each other and from the PikeOS Operating System according to the SSP by using the underlying hardware.
- TSS_STA: Separation in time of applications hosted in different partitions from each other and from the PikeOS Operating System according to the SSP.
- TSS_COM: Provision and management of communication objects.
- TSS_MAN: Management of the TOE (e.g. system partition API) and the TOE data (e.g. threads, tasks).

The TOE guidance, foremost the security manuals, describe limitations within which these features have been evaluated. In particular, the evaluation results apply only for the NXP LS1023A/LS1043A hardware platform (with more details provided in the Security Target [6]).

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 for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 [4] (AIS 34).

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

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1146-2022, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on

- added evidence for the new TOE portions had to be reviewed for the first time
- site-visits performed for previous sites had to be repeated
- an additional development site had to be taken into account
- testing activities and vulnerability assessment were repeated taking into account the specifics of the new, partially integrated TOE

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant / extended
  EAL 5 augmented by ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, AVA_VAN.5

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. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
ASP	Architecture Support Package
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
CLKMGR	Clock Manager
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GPG	Gnu Privacy Guard
HWVIRT	Hardware Virtualization
IPC	Inter-Process Communication
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MMU	Memory Management Unit
PP	Protection Profile
PSP	Platform Support Package
PSSW	PikeOS System Software
RPM	Red Hat Package Manager
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SoC	System on a Chip
SSP	System Security Policy

ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Security Service
VMIT	Virtual Machine Initialization Table

13.2. 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.

14. 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-1185-2023, Version 41.19, 2023-07-27, Security Target for the PikeOS Separation Kernel v5.1.3 for the NXP LS1023A/LS1043A Processor, Sysgo GmbH

[7] Evaluation Technical Report, Version 4, 2023-08-30, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] Configuration list for the TOE (Master Document List), 2023-07-27, 20069-0000-MDL.xlsx, Sysgo SAS (confidential document)

[9] Guidance documentation for the TOE, see table 2 in chapter 2

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 38, Version 2, Reuse of evaluation results

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