Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1041-2018

for

PikeOS Separation Kernel 4.2.2

from

SYSGO AG

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-1041-2018 (*)

Operating System

PikeOS Separation Kernel
4.2.2

from	SYSGO AG
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ALC_FLR.3

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 4

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, 10 December 2018

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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 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]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- 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 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- 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.sogisportal.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.

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+ ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern 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 PikeOS Separation Kernel, 4.2.2 has undergone the certification procedure at BSI.

The evaluation of the product PikeOS Separation Kernel, 4.2.2 was conducted by atsec information security GmbH. The evaluation was completed on 22 November 2018. 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 AG.

The product was developed by: SYSGO AG.

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 product’s resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 10 December 2018 is valid until 9 December 2023. Validity can be renewed 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 PikeOS Separation Kernel, 4.2.2 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 AG

Am Pfaffenstein 14
55270 Klein-Winternheim

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 version 4.2.2 running on the microprocessor family (x86 64-bit, ARMv7, or ARMv8) hosting different applications.

The TOE is a separation kernel, which is a special kind of microkernel that allows to effectively separate different applications running on the same platform from each other. Applications are hosted in partitions, which can be separated from each other. Such non-privileged applications can also be operating systems. Non-privileged applications may be malicious, and even in that case the TOE ensures that the malicious applications are harming neither the TOE nor other applications in other partitions. The TOE will be installed and run on a hardware platform (e.g. embedded system). SYSGO defines separation as follows:

The TOE separates partitions by managing their access 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. The TOE is a real time separation kernel; thus, the partitioning is configured statically and the TOE does not include typical desktop operating system services (e.g. user login, printer drivers).

The major security services provided by the TOE are summarized in table 1.

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 3 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7.1. 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. 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

TOE Security Functionality	Addressed issue
	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 PikeOS Separation Kernel restricts a non-privileged application to only manage tasks and threads within its partition. The PikeOS Separation Kernel 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 8.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 4.1. 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 4.2 – 4.4.

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, 4.2.2

The following table outlines the TOE deliverables:

#	Type	Identifier	Release	Form of Delivery[7]
PikeOS 4.2.2 x86 64-bit				
1	SW	PikeOS 4.2.2 build S5400 for x86 64-bit architecture	R4p2_PIKEOS_MT_CMB_X86_S5400.iso hash: 505683ba8288ca44da70acfd3350ca7c\ 4ab74c9f6a10b3b291e0fe253a9f11ed	DL
2	SW	PikeOS 4.2.2 certification documentation for x86	R4p2_PIKEOS_DK_CMB_X86_AMD64_CERTKIT_S5400.iso hash: 6eb5b2f4202672c599e88502225e274\ 15df1101b7cbe3f101178f57ebee6c093	DL
PikeOS 4.2.2 ARM v7				
3	SW	PikeOS 4.2.2 build S5400 for ARM v7 architecture	R4p2_PIKEOS_MT_CMB_ARM_V7HF_S5400.iso hash: ec4818bb2d4cf9f96d912c46f07684d3\ a31f2daafaf67c8f1b93787c4863c322	DL
4	SW	PikeOS 4.2.2 certification documentation for ARM v7	R4p2_PIKEOS_DK_CMB_ARM_V7HF_CERTKIT_S5400.iso hash: 8313b13cd52d1cec9ee9662dfde44a0\ 501c7a0720805f6d7d407584db04ce713	DL
PikeOS 4.2.2 ARM v8				
5	SW	PikeOS 4.2.2 build S5400 for ARM v8 architecture	R4p2_PIKEOS_MT_CMB_ARM_V8HF_S5400.iso hash: 832bd69a8b715f9b2b236ff14a3645e4\ 38b4dc8c5716eaacbff74a61d43bc20d	DL
6	SW	PikeOS 4.2.2 certification documentation for ARM v8	R4p2_PIKEOS_DK_CMB_ARM_V8HF_CERTKIT_S5400.iso hash: cb3748f3ef4d9a8c42820050041b4ae7\ 3e3be52be0741b769c9e11c54a0ce20d	DL
TOE guidance documents (delivered mostly by means of the ISO images listed above)				
1	DOC	PikeOS Safety and Security Manual	20.16	from ISO
2	DOC	PikeOS Safety and Security Manual (x86 AMD64 Supplement)	20.13	from ISO
3	DOC	PikeOS Safety and Security Manual (ARM7 Supplement)	20.14	from ISO
4	DOC	PikeOS Safety and Security Manual (ARM8 Supplement)	20.15	from ISO

[7]"DL" signifies delivery by direct download from a server. "from ISO" means that the TOE component is contained in an ISO image (available for direct download) that needs to be extracted or be brought on a suitable media to access the respective component.

#	Type	Identifier	Release	Form of Delivery
5	DOC	PikeOS Platform Manual for x86-amd64 Boards	4.2-225	from ISO
6	DOC	PikeOS Platform Manual for ARM v7 Boards	4.2-182	from ISO
7	DOC	PikeOS Platform Manual for ARM v8-A 64-bit Boards	4.2.182	from ISO
8	DOC	User Manual PikeOS Certification Kit (X86_AMD64)	20.6	from ISO
9	DOC	User Manual PikeOS Certification Kit (ARM_V7HF)	20.6	from ISO
10	DOC	User Manual PikeOS Certification Kit (ARM_V8HF)	20.6	from ISO
11	DOC	PikeOS 4.2 Installation Guide	20.04.2018	from ISO / DL
12	DOC	PikeOS User Manual	4.2-330	from ISO
13	DOC	PikeOS Kernel Reference Manual	4.2-107	from ISO
14	DOC	PikeOS System Software Reference Manual	4.2-132	from ISO
15	DOC	PikeOS PSP Developer’s Guide	4.2-104	from ISO
16	DOC	PikeOS Device Driver Programming Reference Manual	4.2-151	from ISO
17	DOC	P4EXT PikeOS Native Personality Extensions	4.2-40	from ISO
18	DOC	CENV C Language Programming Environment	4.2-22	from ISO

Table 2: Deliverables of the TOE

2.1. Overview of Delivery Procedure

The TOE is delivered to the customer by means of ISO-images. These images are made available for download from an FTP-server (indicated by "DL" in table 2). The customer receives the corresponding download links as part of a delivery mail sent by the developer. The guidance documents are contained in the ISO-images. The PikeOS 4.2 Installation Guide is additionally available for download and contains the instructions to extract the ISO-images.

2.2. Identification of the TOE by the customer

The customer identifies the TOE by inspecting the file names of the ISO-images downloaded and comparing the sha256 hash of each of those with the ones quoted in the corresponding signed sha256-files and table 2 above. The integrity of the latter files is verified with the help of GPG. This process is described in the PikeOS 4.2 Installation Guide, see table 2. 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 the PikeOS 4.2 Installation Guide and details thereof 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. The TOE implements policies pertaining to the security functional classes User Data Protection and Security Management. They are named in the instantiated SFRs, according to the protected resources, as follows

- 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 section 7 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), see also chapter 10 for further integrator aspects.

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 (cf. table 2):

1) Provide CPU(s) with at least two privilege modes (“user” and “supervisor” mode). Only the PikeOS separation kernel 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.
2) 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.
3) 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.
4) 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.
5) 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 PikeOS.

Specific requirements to the x86 64-bit architecture are:

- The processors are operated in 64-bit mode.
- AMD64 instruction set architecture.
- Non-Execute bit (NX bit) support enabled in the BIOS.

Specific requirements to the ARMv7 architecture (Cortex-A7, Cortex-A9, Cortex-A15 ...) are:

- The processors are operated in 32bit mode.
- Memory Management Unit (MMU) with Virtual Memory System Architecture.
- Vector Floating Point (VFP) / Advanced SIMD (Neon) extension.

Specific requirements to the ARMv8 architecture (Cortex-A35, Cortex-A53, Cortex-A57 and Cortex-A72) 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 x86 64-bit, ARMv7 or ARMv8 CPUs specified in the TOE User Manuals for the selected CPU architecture.

OE.EXCLUSIVE_RESOURCES: All resources required by PikeOS, 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.

Details can also be found in the Security Target [6], chapter 4.4.

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 (including the PikeOS ASP, but excluding the PikeOS PSP and any Kernel Level Device Driver), see Security Target [6], Figure 1.

These two layers live on top of a hardware platform featuring one of the three supported CPU architectures (x86 64-bit, ARMv7 or ARMv8). On top of the PSSW sit 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 the TOE instance 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.

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 the kernel 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.

A resource partition always has a "root" task which inherits 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 fewer abilities than are assigned to the partition they belong to, but they can never have more abilities than are assigned to the partition itself.

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 all 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.

At the level of detail of the provided design description, the security features of the TOE are agnostic of the precise CPU within the subsets of processors from the three CPU architectures specified in the ST [6] and the security manuals (see table 2). Therefore, the execution of the tests on one representative of each of these classes has been determined to be sufficient.

Details of both approaches, as well as the penetration testing, are described in dedicated sub-sections below. At the end of each these contain a short summary of the test results.

7.2. Developer Testing

Testing Effort

The developer uses an automated test framework to cover most of the functionality. The executed test suites contain around 648 tests depending on the tested architecture.

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 it 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 (and the including test application) as network-bootable image. Finally, it returns the test results to the developer system.

Some of the tests require a manual check of 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 evaluator uses a document system that allows specifying high-level requirements identified by a specific ID, which is then referred to in 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 the interface function behaviours. Usually, all possible error codes of a function are covered. These return codes are used in test code as expected results following the tested functionality.

The test framework uses various supportive libraries in the test framework to facilitate tests that would otherwise be awkward if only external interfaces would be used. Examples are:

- addromfp: adds a ROM image or other files to the final installation image

- psplib: PSP level device to be able to trigger interrupts that would not be triggerable through normal external interfaces

In addition, the developer created a special test setup and tools for showing interaction between subsystems. This test setup allowed to trace the IPC communication between the subsystems when a user partition sends a request to the PSSW.

Configuration

The TOE was tested based on the CDK ISO S5400 and the related kernel build 4.2-1709 for these architectures:

- ARMv7 (board: SABRE Lite, CPU: Freescale i.MX6Q rev1.2 996 MHz running at 792 MHz)
- ARMv8 (board: LS1043A RDB Board, CPU: A53, 1600 MHz)
- x86-amd64 (board: x86-64, CPU: Intel Core i5 7400 4x3.00GHz So.1151 BOX)

Test results

All relevant tests were successful.

7.3. Evaluator Testing Effort

Testing effort

The evaluator performed a preliminary testing at the developer's site. This provided a first understanding of the test framework and how the result is structured.

The evaluator ran official tests on the final TOE version using a developer-provided test system in the ITSEF lab. Using the developer test suite he reran 55 developer tests. In addition, he devised and conducted 7 additional independent evaluator tests.

Test approach

In combination, the testing did cover all types of interfaces with the focus lying on the interfaces at the attack surface: Kernel Service Interface and PikeOS System Software Service interface.

The re-run of the developer tests includes functions related to the following security function aspects:

- memory access control
- file access control
- communication port access control
- interrupts access control
- access control to PSP-specific services
- CPU access
- IPC handling
- event access control
- thread handling
- memory usage
- CPU time usage

The additional evaluator tests were designed to extend the developer tests for a few specific functions and untested wrapper calls. They related to memory access control, invalid file/volume initialization, VMIT configuration errors, and IPC restrictions.

Test depth

The evaluator tested the externally accessible interfaces. Based on how the TOE is designed, this approach also directly tests all subsystems.

Test configuration

The test setup was based on the image R4p2_PIKEOS_MT_CMB_X86_S5400.iso and was run on an Intel x86-64 platform. The target system was connected to the development system via network for TFTP boot, and via serial line to receive the test output. The evaluator was provided the test framework of the developer, which allowed the automation of nearly all test phases, including test and TOE instance compilation, linking, upload to the target system, execution, and result observation.

Test results

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

7.4. Evaluator Penetration Testing

Overview

The penetration testing was partially performed using the developer’s testing environment, partially using the test environment of the ITSEF.

All configurations of the TOE intended to be covered by the current evaluation were tested.

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

Testing effort

The evaluator devised 6 tests. He did so in collaboration with the developer, who provided support in implementing a test that required ARM-specific assembler code.

Penetration testing approach

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

For the PSSW fuzz testing, the evaluator used an exploitative approach as well as information from the provided source code[8], in order to:

- craft IPC messages that meet the required format and content
- gradually change the messages to exercise the message size checks of the TOE, as well as "inject" incorrect message payloads that pass the general message format checks, and then reach inner processing routines that might not be prepared to be faced with invalid message content

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

[8]During the evaluation activities, the ITSEF had access to the full source code of the PikeOS Separation Kernel under evaluation. The evaluators used source code to verify certain TOE functions in cases where such an analysis was deemed more efficient than performing tests.

The tests, with the exception of one test, were not platform-specific. Therefore, the evaluator only used one test architecture setup (x86_64) at the ITSEF lab, while relying on the developer to execute the tests on the ARM platform. The evaluator provided the devised test code to the developer who in turn provided the execution logs for the ARM platforms.

Test configurations

The penetration testing was performed on the TOE version 4.2 (ISO suffix S5205) for the full set of defined penetration tests and TOE version 4.2.2 (ISO suffix S5400) for tests that could touch areas that were changed between versions 4.2 and 4.2.2. Each test run on one of these versions was executed on all three underlying platforms: x86_64, ARMv7, and ARMv8. The test equipment for x86_64 resided within the ITSEF lab, while the ARM7 and ARM8 test setup resided at the developer site. Note that, 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.

Test depth

The tests covered all TOE subsystems.

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

The PSSW fuzzing revealed that an attacker could crash his own partition (on x86_64 and ARM). But it also showed that this crash had no impact on the TOE itself, nor on any other partition running within the TOE.

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[9] 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 (see table 2 for details) on the development host and configuring and integrating the TOE according to the TOE guidance.

[9]See [6], chapter 7.2

The TOE in the evaluated configuration provides the following security features (See [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, describes limitations within which these features have been evaluated. In particular, the evaluation results apply only for hardware platforms based on a subset of the x86 64-bit, ARMv7 and ARMv8 architectures

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 3 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 3 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.

In addition, the following aspects need to be fulfilled when using the TOE:

The TOE needs to be combined with other components (such as a platform support package PSP) and, usually, one or more applications to create an image which can be booted on the target device. This combination is performed by “integrators” as described in the ST [6], see especially chapter 2.4.4.2 “System Integration”. They are the target audience of guidance documents including the security manuals, see table 2. The evaluation assumes that they are sufficiently trained to understand the security implementation of configuration choices made during the integration process.

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

Please refer to ST [6] chapter 1.3. for TOE-specific Abbreviations and Acronyms and chapter 1.4. for TOE-specific Terms and Definitions.

12.1. Acronyms

AIS Application Notes and Interpretations of the Scheme

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

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
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

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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012

Part 3: Security assurance components, Revision 4, September 2012
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, 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[10] 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-1041-2018, Version 20.6, 10.10.2018, PikeOS Separation Kernel v4.2.2, SYSGO AG

[7] Evaluation Technical Report, Version 3, 21.11.2018, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] Configuration list for the TOE, 03.09.2018, Master Document List, 16162-9101-MDL.xlsx (confidential document)

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

[10] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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