Certification Report

PKE4 Core version 4.1

Sponsor and developer:	***Rambus Inc.*** **4453 North First Street, Suite 100** **San Jose, CA 95134** **USA**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0503107-CR**
Report version:	**1**
Project number:	**0503107**
Author(s):	**Wim Ton and Jordi Mujal**
Date:	**11 December 2023**
Number of pages:	**12**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the PKE4 Core version 4.1. The developer of the PKE4 Core version 4.1 is Rambus Inc. located in San Jose, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a Soft-IP cryptographic hardware block designed to perform public-key cryptographic operations. The TOE is delivered to the integrator as synthesizable Verilog RTL description together with other supporting SW files and guidance. The integrator is responsible for integrating the TOE into their system, which is referred to as the Security IC throughout this document.

The TOE is not in itself a Security IC, it supports development of Security IC.

The evaluation and certification of this TOE was performed to enable re-use of the PKE4 Core IP into an EAL4+ Security IC, hence to fulfil the composition requirements *[COMP]* assurance up to and including EAL4 augmented (EAL4(+)) is needed.

Due to the form of the TOE (Verilog), only a limited amount of attacks is directly applicable and countered by the TOE. For example, physical attacks are not countered by this TOE. **Users of the TOE, developers of a Security IC, must strictly follow the guidance and must successfully pass a composite evaluation against *[PP_0084]* to claim full EAL4+ and/or AVA_VAN.5 resistance.**

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in guidance documents. As such it is vital that meticulous adherence to the user guidance of the TOE is maintained. During composition into a full Security IC, significant vulnerability analysis and testing must be performed. However, the *[ETRfR]* and the guidance enable efficient re-use.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 11 December 2023 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the PKE4 Core version 4.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the PKE4 Core version 4.1 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures), ATE_DPT.2 (Testing: Security Enforcing Modules) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the PKE4 Core version 4.1 from Rambus Inc. located in San Jose, USA.

The TOE is comprised of the following main components:

Package	Name	Version
Hardware Package (source code and test bench)[2]	Synthesizable Verilog RTL description of PKE Engine	Part Number 950-029004-410
	Test bench C files and SystemVerilog files	
	Test bench scripts and file lists	
	Simulation vectors with self-checks	
Software package (source code and documentation)	Software library source code in C	Part Number 951-029004-410
	Software reference manual	
	Software unit tests	

To ensure secure usage a set of guidance documents is provided, together with the PKE4 Core version 4.1. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 2.5.

2.2 *Security Policy*

The TOE provides the following features:

- ECDH calculation using NIST P-192, NIST P-224, NIST P-256, NIST P-384, NIST P-521, Brainpool-224, Brainpool 256, Brainpool 320, Brainpool 384, Brainpool 512 and ANSSI frp256v1;
- ECDH calculation using the Montgomery X-coordinates X25519 and X448 based on Curve25519 and Curve448;
- ECDSA key generation, signature generation and signature verification using NIST P-192, NIST P-224, NIST P-256, NIST P-384, NIST P-521, Brainpool-224, Brainpool 256, Brainpool 320, Brainpool 384, Brainpool 512, ANSSI frp256v1;
- EdDSA key generation, signature generation and signature verification using Ed448 and Ed25519;
- SM2DSA key generation, signature generation and signature verification using SM2(256);
- Auxiliary elliptic-curve functionality e.g. verification of the curve equation,
- RSA public-key and private key operations for non-CRT implementations;
- Modular exponentiation.

2.3 *Assumptions and Clarification of Scope*

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 of the *[ST]*.

[2] This TOE comprises the design of a crypto-processor. As such, no physical hardware is delivered, but the synthesisable Verilog is intended to be integrated into a hardware solution.

2.3.2 Clarification of scope

The TOE is the set of functionalities, encoded in Verilog, for a crypto-processor in a Security IC. The intended environment for the TOE is the Security IC for smart card applications or similar services as identified and described in *[PP_0084].*

The TOE is not in itself a Security IC, it supports development of Security IC.

The evaluation and certification of this TOE was performed to enable re-use of the PKE4 Core IP into an EAL4+ Security IC, hence to fulfil the composition requirements *[COMP]* assurance up to and including EAL4 augmented (EAL4(+)) is needed.

Due to the form of the TOE (Verilog), only a limited amount of attacks is directly applicable and countered by the TOE. For example, physical attacks are not countered by this TOE. **Users of the TOE, developers of a Security IC, must strictly follow the guidance and must successfully pass an evaluation against *[PP_0084]* to claim full EAL4+ and/or AVA_VAN.5 resistance**

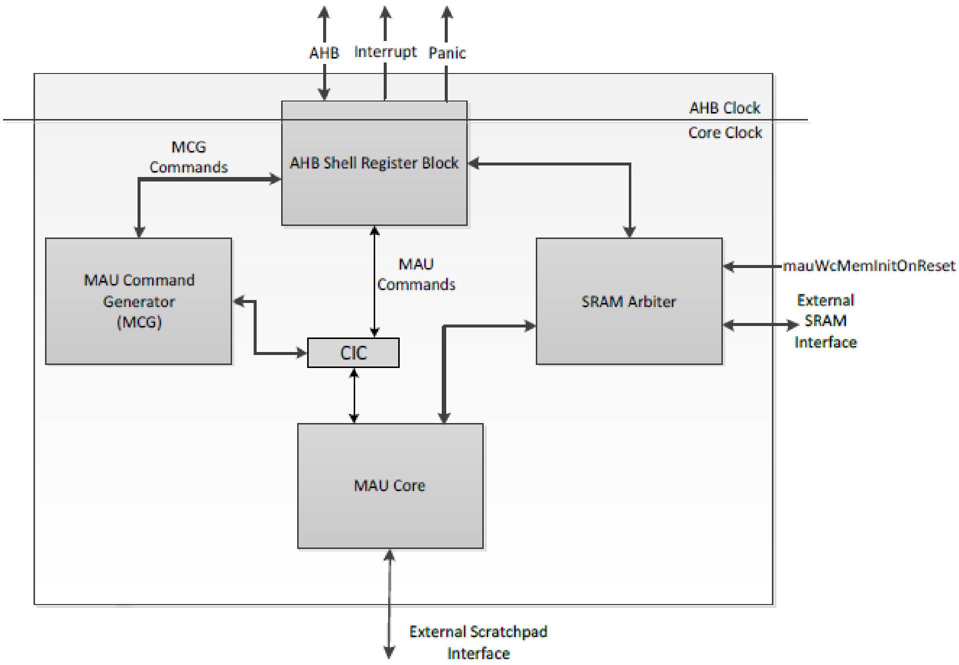
During integration and re-use into a full Security IC, significant vulnerability analysis and testing must be performed. However, the *[ETRfR]* and the guidance enable efficient re-use.

See [ST-lite] chapters 4.3 and 4.4 for details regarding policies and assumptions that are countered by the environment.

Please note that the TOE contains a SW Library providing access to the TOE functionality and adding additional functionality (without security claims). The functionality and security of these features have not explicitly been addressed in this certification (see *[ST]* section 7 for exact security functionality claimed by the TOE). Therefore, if these features are required by the integrated product the developer/evaluator should do their own security analysis and/or testing. In order to support this analysis, the Vendor asked the Lab to carry out additional analysis/testing that is included in the *[ETRfR]*.

2.4 Architectural Information

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version	Date
PKE v4.1 Integration and Testing Guide, Document Number: 007-029410-228	Rev. A	2021-01-12
Security IP, PKE v4.1, User Security Guidance, Document Number: 007-029410-424	Rev, G	2023-01-13
PKE v4.1 External Reference Specification, Document Number: 007-029410-222	Rev. A	2021-01-12
DPA Resistant Software Libraries	Version 2.0	2022-08-09
Secure Data Handling Requirements for Intellectual Property and Information, Spec No 000425,	Version D	2021-08-16

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The testing of the TOE takes place during development and during the integration. Both were considered during ATE_FUN analysis.

The overall completeness is being monitored using code coverage tools during the TOE development phase. The evaluator analysed the output and asked the developer for a rationale for all cases where an interface (TSFI and module interface) was not 100% covered.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The independent vulnerability analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack-oriented analysis the protection of the TOE is analysed using the knowledge gained from all evaluation classes. This results in the identification of (additional) potential vulnerabilities. This analysis used the attack methods in *[JIL-AM]* and *[JIL-AAPS]*.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities were not exploitable. The potential vulnerabilities were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 118 days. During that test campaign, 98% of the total time was spent on side-channel testing and 2% on Perturbation attacks.

2.6.3 Test configuration

The penetration testing has not been performed on a final product (as the TOE is not a final product), but on a FPGA that implements the TOE in the environment (i.e. representative of a final product) or using simulations. Configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the [ST].

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

For re-use evaluations, please consult the *[ETRfR]* for details.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the site involved in the development and production of the TOE, by use of Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number PKE4 Core version 4.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support re-use evaluations based on *[COMP]* a derived document *[ETRfR]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a re-use evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the PKE4 Core version 4.1, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 4 augmented with ATE_DPT.2, AVA_VAN.5 and ALC_DVS.2** . This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target is based on *[PP_0084]* but does **not** claim conformance to the Protection Profile *[PP_0084].* Nevertheless, re-use evaluations based on this TOE can claim *[PP_0084]* conformance*.*

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in guidance documentation. Therefore, it is vital to maintain meticulous adherence to the user guidance of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must 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. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

The re-use evaluator should note the following regarding the rating of required knowledge of this TOE (i.e., the PKE4 core design). The TOE comprises the implementation representation which is available under a licensing agreement with the developer. Hence, any required knowledge of the implementation representation of the TOE shall not be rated higher than Sensitive in an attack potential calculation.

3 Security Target

The Rambus PKE4 Core version 4.1 Security Target, Revision 0.1o, 04 December 2023 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

DFA	Differential Fault Analysis
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
FIA	Fault Injection Attack
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
RTL	Register Transfer Level
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[ETR] Evaluation Technical Report “PKE4 Core version 4.1” – EAL4+, 22-RPT-508, version 4.0, 08 December 2023.

[ETRfR] Evaluation Technical Report for Reuse “PKE4 Core version 4.1” – EAL4+, 23-RPT-816, version 4.0, 08 December 2023.

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019

[PP_0084] Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014

[ST] Rambus PKE4 Core version 4.1 Security Target, Revision 0.1o, 04 December 2023

[ST-lite] Rambus PKE4 Core version 4.1 Security Target Lite, Revision D, 08 December 2023

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)