Certification Report

Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300

Sponsor and developer: ***Thales***
La Vigie, Avenue du Jujubier ZI Athelia IV,
13705 La Ciotat
France

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-230855-CR**

Report version: **1**

Project number: **230855**

Author(s): **Denise Cater**

Date: **24 December 2019**

Number of pages: **11**

Number of appendices: **0**

Headoffice:
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 Dutch Chamber of Commerce 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 license 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, in order 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.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300. The developer of the Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300 is Thales located in La Ciotat, France 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 mobile SDK library called AWPKI SDK. The AWPKI SDK is intended to be integrated by a customer in a mobile application (named here after Customer APP). This application is developed by a customer using AWPKI SDK development tools according rules defined in TOE development guidance and in line with Thales application example provided as AWPKI SDK APP. An AWPKI SDK APP is delivered also to help with customer integration and for evaluation purposes because AWPKI SDK cannot be run alone in the mobile environment.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 23 December 2019 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 Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300, 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 Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300 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 provides sufficient evidence that the TOE meets the EAL3 augmented (EAL3(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ADV_FSP.4 (Complete functional specification), ADV_TDS.3 (Basic modular design), ADV_IMP.1 (Implementation representation of the TSF) ALC_TAT.1 (Well-defined development tools) and AVA_VAN.3 (Focused 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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300 from Thales located in La Ciotat, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Gemalto Advanced Whitebox PKI SDK for Android	v1.0.1.300

To ensure secure usage a set of guidance documents is provided together with the Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300. Details can be found in section “Documentation” of this report.

2.2 Security Policy

The TOE has the following logical features:

- VAD derivation.
- Mobile binding.
- Customer Binding (Whitebox AES cryptography).
- Cryptographic operation access control
- Whitebox ECDSA signature
- Operation protection with obfuscation, anti-rooting, ant-hooking and anti-debugging.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 3.4 of the *[ST]*.

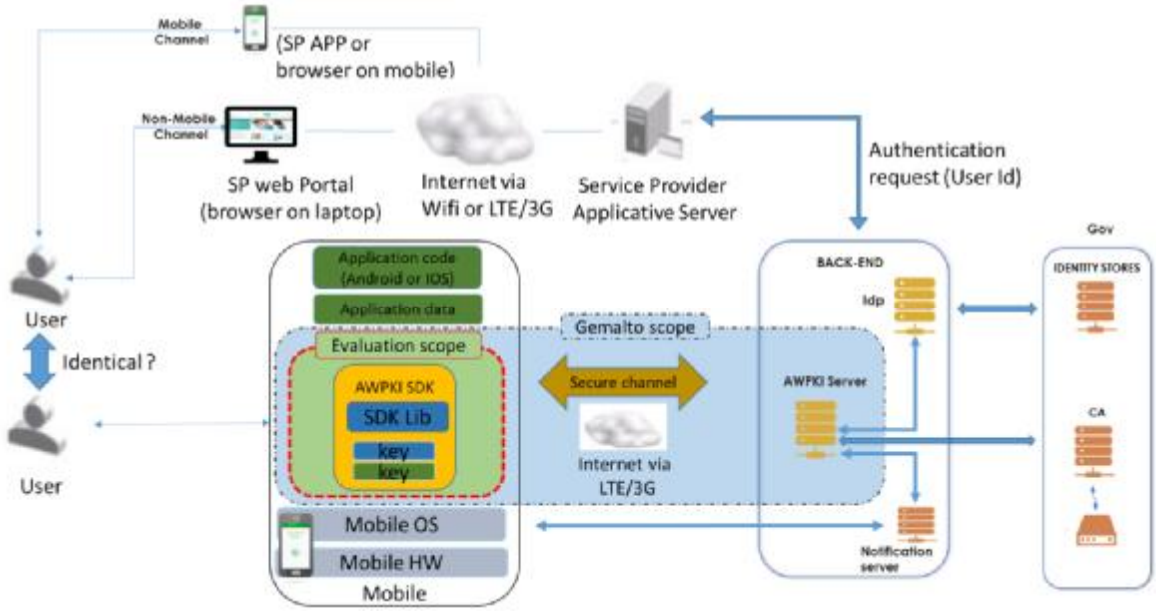
2.3.2 Clarification of scope

The objective for the environment that the TOE is installed on Android 6.0 or above must be met to ensure a hardware-backed key store is provided.

2.4 Architectural Information

TOE performs (on AWPKI server request) an authentication cryptographic operation (ECDSA signature) using information from AWPKI Server, user mobile, and user. When operation is completed, authentication cryptographic operation result is transferred securely to AWPKI server which decides the result of the authentication and communicates the result to the authentication request originator. The TOE also provides administration features to manage sensitive data and establishment of a secure channel with the AWPKI server. However, these functionalities are not part of the TSF nor in scope of the evaluation.

The logical architecture of the TOE can be depicted as follows:



Gemalto provides items in the deployed solution:

- a SDK (also named AWPKI SDK) to be integrated in the service provider Mobile application,
- a AWPKI Server software deployed on AWPKI Server in the service provider infrastructure.

Both items work together to provide user authentication service to service provider.

2.5 Documentation

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

Identifier	Version
Security Rules for User of Application including Gemalto Advanced Whitebox PKI SDK V1.0.1	1.5
Preparation Guidance for Gemalto Advance Whitebox PKI SDK V1.0.1	1.5
Advanced Whitebox PKI Library Developer Guide (Android)	1.13
Security Rules for Application development based on Gemalto Advance Whitebox PKI SDK V1.0.1	1.6
Security Rules for Server Development & Integration associated to Gemalto Advanced Whitebox PKI SDK V1.0.1	1.2
AWPKI Server Integration Guide	1.2

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 4 different types of functional tests to provide extensive test evidence of the correct behaviour of the TOE security functionality and TSFI:

- Unit tests: Performed using development tools. Intended to test specific internal functions of the TOE/TSF.
- VTA tests: Performed using an ad-hoc application that automatically run a regression test and emulates the AWPKI server. Intended to test the TOE API (TSFI I_SDK_APP)

- Manual tests: Performed using the “demo app” and a test server. Intended to test the operation requiring human user actions, e.g. PIN entry.
- Security tests: Intended to test the security mechanisms (anti-root, anti-hook, etc.)

The evaluator witnessed on site the functional test execution (on a preliminary TOE version 1.0.0.233), verified that the tests are performed according ATE documentation and collected a sample of test results.

For the testing performed by the evaluators, the developer provided an example APP and a test environment. The evaluators performed a small number of additional test cases designed by the evaluator.

2.6.2 Independent Penetration Testing

The focused vulnerability analysis was conducted along the following steps:

- During the evaluation of all performed assurance classes the evaluator labelled the identified potential vulnerabilities, if any.
- ADV_IMP a thorough implementation representation review was performed on the TOE resulting in the identification of additional potential vulnerabilities. This analysis was performed according to the public sources and known software related attack.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. For the potential vulnerabilities relevant for the TOE a penetration test was defined. Several potential vulnerabilities were found to be not exploitable due to an impractical attack path.

The distribution of the different penetration test categories executed by the evaluator is as follows:

Penetration test category	**% of total number of penetration tests**
Bypassing Security countermeasures	25%
Reverse engineering	50%
Run time memory extraction	25%
Total	100%

The overall conclusion is that the TOE is protected against attackers possessing an enhanced-basic attack potential, under the condition that the TOE user guidance is followed.

2.6.3 Test Configuration

The developer tested the TOE v1.0.1.300 in the following platforms:

- Samsung S6, Android 6.0.1
- Samsung S7 Edge, Android 7.0
- Huawei Honour 10, Android 8.1.0
- Google Pixel 3A, Android 9.0
- Nokia 7 Plus, Android 8.1.0

The following Android platforms were used during the repetition of developer functional testing, performed on TOE version 1.0.0.233:

- Unit tests: Samsung S7 Edge, Android 7.0
- VTA tests: Samsung S7 Edge, Android 7.0
- Security tests: Nexus 6P, Android 8.1.0
- Manual tests: Huawei Honor 10, Android 8.1.0

Evaluator independent functional testing was performed across the following platforms with TOE version 1.0.0.233, re-run on TOE v1.0.1.300 where applicable:

- Nexus 5X, Android 8.1.0
- Nexus 5, Android 5.1.1

- Bluestacks 4, Android v7.1.2
- Android Studio, Android 7.1.1 and Android 8.0.0

Evaluator independent penetration testing was performed on the following platform with TOE version 1.0.0.233, re-run on TOE v1.0.1.300 where applicable:

- Nexus 5X ArmV8, Android 8.1.0

2.6.4 Testing 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.

2.7 Re-used evaluation results

There has been extensive re-use of the ALC aspects for some of the sites involved in the development and production of the TOE.

One site has been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number: Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*.

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

Based on the above evaluation results the evaluation lab concluded the Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 3 augmented with AVA_VAN.3, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1 and ALC_TAT.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE.

The mobile platform does not reliably detect that the device has been rooted. When the mobile platform reports that the device has been rooted, the TOE is able to act on that warning and prevents operation. However, even in the case that the platform does not reliably provide root detection, the TOE defends against attacks with an enhanced-basic attack potential.

In addition, all aspects of assumptions, threats and policies 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 for the TOE is required and thus requested from the sponsor of the certificate.

3 Security Target

The Security Target for Gemalto Advanced Whitebox PKI SDK, v1.7, 13 November 2019 *[ST]* is included here by reference.

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

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
APP	(mobile) Application
AWPKI	Advanced Whitebox Public Key Infrastructure
ECDSA	Elliptic Curve Digital Signature Algorithm
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
SDK	Software Developer Kit
TOE	Target of Evaluation
VAD	Verification Authentication Data
VTA	Verification Test Automatic

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.
[ETR]	Evaluation Technical Report Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300, 19-RPT-492, Version 7.0, 12 December 2019.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[ST]	Security Target for Gemalto Advanced Whitebox PKI SDK, v1.7, 13 November 2019.
[ST-lite]	Security Target for Gemalto Advanced Whitebox PKI SDK (Public version), v1.7, 13 November 2019
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).