



# Certificate Report

## Version 1.0

## 31 January 2023

## CSA_CC_22001

## For

## appGuard appShield system version 6.6

## From

## HyperG Smart Security Technology Pte., Ltd.

This page is left blank intentionally

# Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

## Amendment Record

| Version | Date | Changes |
|---|---|---|
| 1.0 | 31 January 2023 | Release |

**NOTICE**

The Cyber Security Agency of Singapore makes no warranty of any kind with regards to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

# Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the appGuard appShield system Version v6.6 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

| Identifier | Version |
|---|---|
| Software | appGuard appShield system Version v6.6<br>File name: install_yyjg.tgz<br><br>Format: CD<br>Delivery method: Delivered and installed by developer at user premise |

Table 1 - TOE components identifier

The list of guidance documents to use with the product in its certified configuration is as follows.

| Name and version | Version |
|---|---|
| White box Crypto System V4.0 User Manual<br><br>Format: PDF<br>Delivery method: Email | V4.0 |
| appGuard 保護黑盒部署文件_20211018<br><br>Format: PDF<br>Delivery method: Used by delivery team | |

Table 2 - List of guidance documents

TOE is a software application that hardens a mobile application executable and its shared library with:

- Reverse engineering protection
- Debugging protection
- Integrity protection
- Local data encryption
- Application and software library binding

TOE consists of the following logical scope:

- Identification and authentication
- Security management
- User data protection
- Cryptographic operation

- Protection of TOE Security Functionality (TSF)

The evaluation of the TOE has been carried out by An Security Pte Ltd, an approved CC test laboratory, at the assurance level CC EAL 2 and completed on 30 Nov 2022.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

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

| TOE Security Functionality |
|---|
| Identification and Authentication:<br>The TOE provides the graphical user interface (GUI) for user identification and authentication via a web browser in the client machine. A TOE accepts username and password via the GUI to perform user identification and authentication. |
| Security Management:<br>The TOE restricts the access to security management functions to the backend administrator and frontend operator. The security management functions available includes the following:<br>• TSF/user data protection deployment<br>• cryptographic operation management<br>• TSF protection management |
| User Data Protection:<br>The TOE-deployed hardening protection deploys the following methods of user data protections:<br>• Mobile application executable, shared library and local data are encrypted; this protects these data from static analysis.<br>• Before launching the mobile executable, the TOE-deployed hardening mechanism verifies o mobile application executable integrity<br>• mobile application executable name<br><br>The TOE-deployed mechanism protects the mobile application against extraction of intelligible information about the mobile application source code in-memory during run-time using the following techniques:<br>• Randomly allocating memory locations of decrypted mobile application executable.<br>• Shared libraries are erased from the memory after use.<br>• Disable and monitor debug interfaces.<br>• Encryption and decryption at granularity level of classes, methods and strings. |
| Cryptographic Operations:<br>The TOE supports the following cryptographic algorithms that are deployed |

| |
|---|
| on the target mobile application executable:<br>• AES<br>• SHA1 (for 2nd preimage resistance) |
| Protection of TSF:<br>The TOE-deployed hardening mechanism reduces the risk of an attacker reverse engineer the mobile application executable and shared library to extract the source code of the mobile application using dynamic analysis. The application of white-box cryptography shall also deter attackers from obtaining the key to the encryption/decryption mechanism and hash of integrity protection mechanism. |

Table 3: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats, and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1]

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

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 applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

## Table of Contents

# 1 Certification

## 1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

## 1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is fully covered by the CCRA.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

# 2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **30 January 2028**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

# 3 Identification

The Target of Evaluation (TOE) is: appGuard appShield system Version v6.6

The following table identifies the TOE deliverables.

| Identifier | Version |
|---|---|
| Software | appGuard appShield system Version v6.6<br>File name: install_yyjg.tgz<br><br>Format: CD<br>Delivery method: Delivered and installed by developer at user premise |

Table 4 - TOE Deliverables

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents.

| Name and version | Version |
|---|---|
| White box Crypto System V4.0 User Manual<br><br>Format: PDF<br>Delivery method: Email | V4.0 |

Table 5 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

| | |
|---|---|
| TOE | appGuard appShield system version V6.6 |
| Security Target | HyperG appShield Security Target version 2.0 |
| Developer | HyperG Smart Security Technology Pte Ltd |
| Sponsor | HyperG Smart Security Technology Pte Ltd |
| Evaluation Facility | An Security Pte Ltd |
| Completion Date of Evaluation | 30 November 2022 |
| Certification Body | Cyber Security Agency of Singapore (CSA) |
| Certificate ID | CSA_CC_22001 |
| Certificate Validity | 5 years from date of issuance |

Table 6: Additional Identification Information

# 4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- Identification and authentication
- Security management
- User data protection
- Cryptographic operations
- Protection of TSF

Specific details concerning the above-mentioned security policy can be found in Chapter 1 of the Security Target [1].

# 5 Assumptions and Scope of Evaluation

## 5.1 Assumptions

The assumptions defined in the Security Target [1] 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 and are listed in the tables below:

| Environmental Assumptions | Description |
|---|---|
| OE.Trusted_User | The operational environment shall ensure:<br>• TOE users are well-trained to operate the TOE securely in accordance with the operational guidance.<br>• System administrators are well-trained to setup the IT environment in accordance with the preparative guidance.<br>• Both TOE users and system administrators are trusted. |
| OE.Trusted_CPU | The System Administrator shall ensure the CPU and hardware peripherals on the server and client machine are trusted and secure i.e. in compliance with organisation's security policy. |
| OE.Trusted_OS | The System Administrator shall ensure the server and client machine, respectively, are trusted and secure i.e. in compliance with organisation's security policy. |
| OE.Trusted_IT_Products | The System Administrator shall ensure the following external IT products that support the TOE operations are trusted and secure i.e. in compliance with organisation's security policy. |

| | |
|---|---|
| | • Server side<br>  ○ Files system<br>  ○ Database<br>  ○ Application container<br>  ○ Service scheduling<br>• Client side<br>  ○ Web browser |
| OE.Physical | The System Administrator shall ensure the:<br>• TOE and external IT products are deployed in the same physically secure environment where only authorised TOE users and system administrators have access.<br>• interconnect between the server machine and client machine is physically protected from tamper.<br>• TOE is logically isolated from external network. |
| OE.Trusted_Channel | The System Administrator shall ensure the following:<br>• The server machine and client machine shall establish a trusted channel. |
| OE.Trusted_Mobile_Platform | The TOE user shall inform the Mobile app user to ensure the following:<br>• The mobile platform, consisting of underlying hardware and mobile OS, which the TOE-hardened mobile |

Table 7: Environmental Assumptions

Details can be found in section 4.2 of the Security Target [1].

## 5.2 Clarification of Scope

The scope of evaluation is limited to the claims made in the Security Target [1].

## 5.3 Evaluated Configuration

The appGuard appShield system version v6.6 is a software application that hardens a mobile application executable and its shared library against:

- Reverse engineering
- Debugging
- Tamper
- Disclosure of its local data

The TOE is deployed in a private cloud environment (Figure 1); users can harden mobile application executable via a web browser on a client machine. The deployed protection mechanism includes:

- Identification and authentication
- Security management
- User data protection
- Cryptographic operations
- Protection of TSF

The TOE hardens mobile application that runs on Android, iOS and H5 platform. However, the scope of evaluation **only includes the Android platform**.

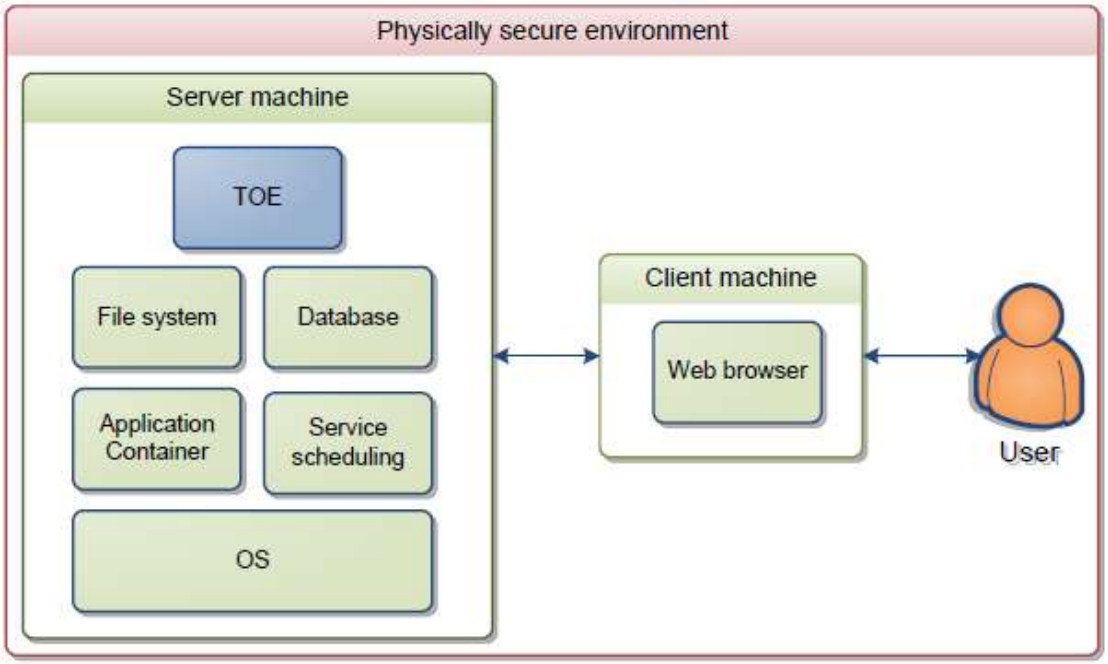


Figure 1 – Evaluated configuration

## 5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2.

## 5.5 Non-TOE Components

The TOE requires additional components (i.e., hardware/software/firmware) for operation. These non-TOE components include:

- Server
- OS
- Database
- Application Container
- Service scheduling
- File system
- Web browser

# 6 Architecture Design Information

As described in the Security Target *[1]*, the TOE consists of one component; a software application that hardens mobile applications. The TOE is deployed in a private cloud environment (Figure 2); users can harden mobile application executable via a web browser on a client machine.

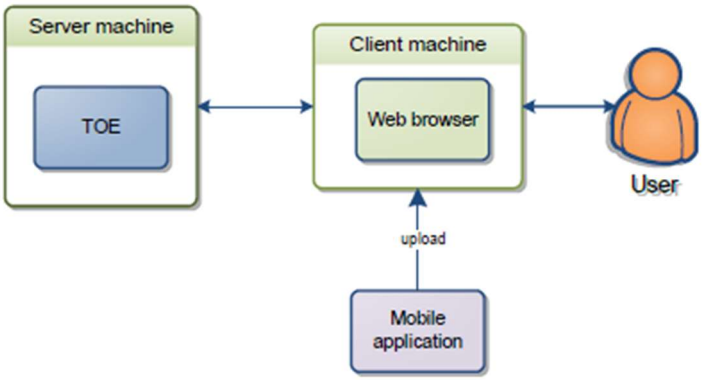


Figure 2 – TOE Usage

The TOE consists of the following seven subsystems:

- Runtime Monitoring
- Hook Detection
- Root Detection
- Encryption
- Decryption
- White-box Decryption
- Integrity Protection

# 7 Documentation

The evaluated documentation as listed in Table 5 - Guidance Document (part of TOE deliverables) is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

# 8 IT Product Testing

## 8.1 Developer Testing (ATE_FUN)

### 8.1.1 Test Approach and Depth

Based on the Development (ADV) analysis, the evaluator understands that the TSF of can be modelled in the following manner (Figure 3). The evaluator notes two groups of TSFs exists i.e. TSF1 runs on the server and TSF2 runs on the mobile platform.

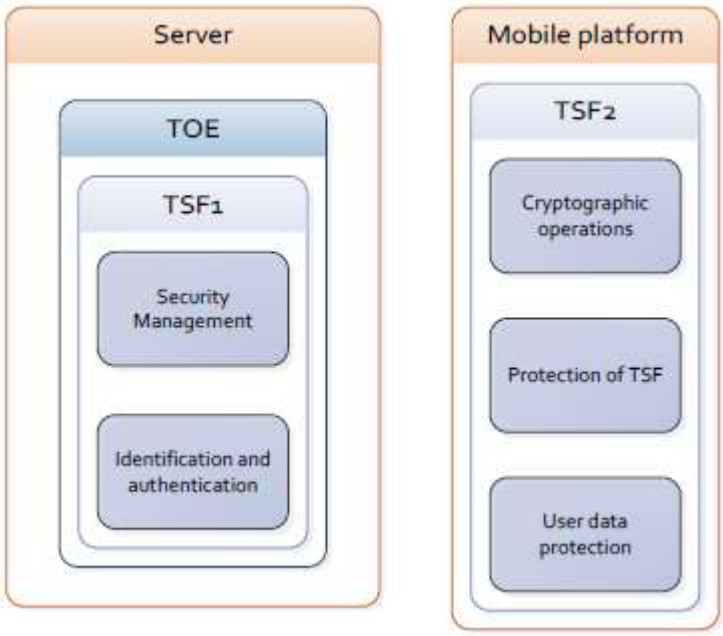


Figure 3 – TOE model

According to the evaluated configuration (Figure 1), ADV has determined that TSF1 is deployed physically secured environment (OE.Physical), managed by trusted users (OE.Trusted_User) and runs on trusted platform (OE.Trusted_IT_Products); no threat is anticipated in this environment, hence, none of the interfaces qualifies as TSFI (TSF Interface). These OEs has also been verified through Guidance Document (AGD) analysis. As a result, TSF1 shall be not examined further. Instead, TSF2 shall be the focus in the rest of the Vulnerability Assessment (AVA) analysis.

### 8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [9].

### 8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

## 8.2 Evaluator Testing (ATE_IND)

### 8.2.1 Test Approach and Depth

The evaluator sampled and repeated developer's test cases that are related to rot detection, hook detection and runtime monitoring subsystems to ensure that the implementation of debug protection function (root detection, hook detection and runtime monitoring) at static rest is correct.

In addition, the evaluator also devised a set of independent tests that supplements or augments developer's existing test plan to gain assurance of security of the TOE, cryptographic operation, hook detection, root detection

and runtime monitoring in both dynamic and static operation modes.

### 8.2.2 Test Results

The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan.

## 8.3 Penetration Testing (AVA_VAN)

### 8.3.1 Test Approach and Depth

The evaluator performed public vulnerability search to identify potential vulnerabilities in the TOE and analysed potential vulnerabilities. The evaluator also devised attack scenarios based on these potential vulnerabilities and performed theoretical analysis on the related attack potential including attack scenarios with basic or slightly above basic attack potential. The evaluator analysed the results of these tests with the aim to determine if there is at least one of the attack scenarios with the attack potential basic was successful.

For the potential vulnerabilities being applicable to the TOE in its operational environment and, hence, which were candidates for testing applicable to the TOE in its operational environment, the evaluator devised the attack scenarios where these potential vulnerabilities could be exploited. For each such attack scenario he firstly performed a theoretical analysis on the related attack potential. Where the attack potential was Basic or near to Basic, the evaluator conducted penetration tests for such attack scenarios. He analysed then the results of these tests with the aim to determine, whether at least one of the attack scenarios with the attack potential Basic was successful. The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. No residual risks were identified.

# 9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

# 10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 2 - List of guidance documents 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 [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

The TOE hardens mobile application that runs on Android, iOS and H5 platform. However, within the scope of evaluation, The TOE is evaluated **only for the Android platform**.

No additional recommendation was provided by the evaluators.

# 11 Acronyms

| | |
|---|---|
| CCRA | Common Criteria Recognition Arrangement |
| CC | Common Criteria for IT Security Evaluation |
| CCTL | Common Criteria Test Laboratory |
| CSA | Cyber Security Agency of Singapore |
| CEM | Common Methodology for Information Technology Security Evaluation |
| cPP | Collaborative Protection Profile |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| IT | Information Technology |
| PP | Protection Profile |
| SAR | Security Assurance Requirement |
| SCCS | Singapore Common Criteria Scheme |
| SFR | Security Functional Requirement |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |

# 12 Bibliography


[1] HyperG, “HyperG appGuard Security Target version 2.0”, Taiwan, 2021.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[3] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[5] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[9] HyperG, “White-box Crypto System User Manual (AGD_OPE) version 4.0”, HyperG, Taiwan, 2021.


----------End of Report ----------