Cybersecurity
Certification Centre
CYBER SECURITY AGENCY OF SINGAPORE

CLS READY

CLS-Ready
Publication No. 1

Overview of the Scheme

April 2022
Version 1.0

AMENDMENT RECORD

Version	Date	Author	Changes
1.0	April 2022	Cyber Security Agency of Singapore	Release

CONTENTS

1 INTRODUCTION 5

2 BACKGROUND 5

2.1 Impetus for CLS-Ready 5

2.2 Benefits 5

3 OVERVIEW OF THE CLS-READY SCHEME 6

3.1 Overview 6

4 SPECIFICATIONS 6

4.1 Types of Microcontroller Platform 6

4.2 Platform Security Features (PSF) 7

4.3 Mapping of the CLS-Ready to CLS 10

5 GENERAL PROCESS OF CLS-READY 11

5.1 Process Overview 11

5.2 Pre-Application Phase 14

5.3 Application for CLS-Ready 14

5.4 Analysis Stage 14

5.5 Device setup and verification of guidance documents 15

5.6 Vulnerability Analysis 15

5.7 Penetration Testing 16

5.8 Conclusion 16

5.9 Changes to Conditions for CLS-Ready certification 16

5.10 Cryptography 17

6 APPLICANT OBLIGATIONS 17

6.1 Vulnerability Disclosure 17

6.2 Defined Support Period for Security Updates 17

7 CLS-READY CERTIFICATE 17

7.1 Validity 17

7.2 Principles 17

7.3 CCC Audit and Testing 18

7.4 Revocation of the CLS-Ready certification 18

8 ASSURANCE CONTINUITY 19

9 REQUIREMENTS FOR CLS-READY TEST LABORATORY 19

10 MECHANISM FOR COMPLAINTS, DISPUTES AND APPEALS 19

11 FEES 20

11.1 General Policy 20

12 LIABILITY 21

12.1 Disclaimer 21

REFERENCES **22**

ACRONYMS **22**

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard 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.

1 INTRODUCTION

1.0.1 This document provides an overview of the CLS-Ready scheme. It outlines the scheme objectives, description of the scheme, as well as an overview of the testing process.

1.0.2 It also establishes the technical oversight role of Cybersecurity Certification Centre (CCC) in the CLS-Ready and sets out general terms and conditions for the developer and/or the Testing Laboratory (TL) that apply for such a label.

1.0.3 The following roles are commonly referred in this document:

- Developer of the Device Under Test (Platform)
- Testing Laboratory (TL) that performs the Assessment
- Cybersecurity Certification Centre (CCC) that oversees the CLS-Ready

2 BACKGROUND

2.1 Impetus for CLS-Ready

2.1.1 The types of IoT or consumer connected devices is so much more diverse, in comparison to enterprise ICT products, ranging from basic sensors to children’s toys and other smart home appliances.

2.1.2 Due to this diversity and the current nascent stage of the ecosystem, it remains challenging for the manufacturers to adequately incorporate cybersecurity elements into the product. This is especially so for small and medium enterprises (SME) or where the products traditionally have no association with cybersecurity, for instances, smart rice-cooker or smart teddy bear.

2.1.3 To develop the entire hardware and software stack from scratch could unknowingly increase the potential for cyber-related risks. Instead, leveraging on a secure underlying hardware/platform would enable the manufacturers of end devices to incorporate security measures in a consistent manner. Such platforms typically include standard tools and methods that can promote good design habits and help developers build strong security into their solutions from the outset

2.2 Benefits

2.2.1 The CLS-Ready strive to bring about the following benefits:

2.2.2 <u>End Device Manufacturers</u>

1. Leveraging on a secure hardware/platform will greatly facilitate end devices to achieve a reasonable level of security. Manufacturers could focus on developing functionalities of the end devices, without

having to invest heavily on a team to develop the cybersecurity aspects of it from scratch.

2. Testing against CLS level 4 for the end devices using CLS-Ready hardware will require lesser efforts (time and cost). Security functionalities provided by the CLS-Ready hardware will no longer be needed to be tested at the end device level. The assessment will also focus more on whether the manufacturer of the end devices is calling the security functionalities provided by the CLS-Ready hardware correctly.

3. A change in the hardware/platform to another CLS-Ready hardware/platform with the same set of Platform Security Functions will undergo a simpler process of assurance continuity with significant lower efforts.

2.2.3 Hardware/Platform Manufacturers

1. A single CLS-Ready hardware will be able to support multiple end devices, expanding market reach.

2. With the CLS gaining popularity around the world, hardware/platform manufacturers will be able to differentiate their hardware/platform with the CLS-Ready label from their competitors.

3 OVERVIEW OF THE CLS-READY SCHEME

3.1 Overview

3.1.1 The CLS-Ready is a complementary scheme to the CLS itself. It is likewise a voluntary scheme, for a start.

3.1.2 Unlike CLS, the CLS-Ready has no concept of levels. Given that the end devices have diverse use cases and require different functionalities, it is impractical to define them exhaustively.

3.1.3 Under the CLS-Ready, hardware/platform developers would instead, specify the functionalities provided and have these functionalities evaluated by an approved test laboratory.

3.1.4 The CLS-Ready will focus initially on microcontrollers and extendable, in future, to other common underlying platforms such as Wi-Fi chipsets and Bluetooth modules etc.

4 Specifications

4.1 Types of Microcontroller Platform

4.1.1 The following types of platforms are defined:

1. Basic Microcontroller Unit (MCU)

  a. A basic MCU typically does not provide any Trusted Execution Environment (TEE) for separating trusted and untrusted code.
  b. A basic MCU could still provide other security features which are typically implemented by software.
  c. A basic MCU typically does not have protection against physical attacks.

2. Single Core MCU with TEE
  a. A single core MCU could include TEE that provides a soft separation between trusted and untrusted code (i.e., software sandboxing).
  b. Given both trusted and untrusted code share the same resources, a single core MCU might not be resistant against certain attacks such as side channel analysis.
  c. A single core MCU could incorporate additional hardware extensions for protection against basic physical attacks.

3. Dual/Multi Cores MCU with TEE
  a. With dual/multi cores MCU, the TEE is being implemented on a different core providing full hardware separation between trusted and untrusted codes.
  b. A dual/multi cores MCU could incorporate additional hardware extensions for protection against basic physical attacks.

4. Secure Element
  a. Discrete security controllers that provide tamper-resistant hardware features for protection against physical attacks.
  b. The security features are usually certified according to Common Criteria (ISO/IEC15408).
  c. Secure element could be incorporated as a companion chip to the main MCU.

4.2 Platform Security Features (PSF)

4.2.1 The developer of the DUT may select the security features that are implemented. The developer is recommended to select all features by the hardware into the scope of evaluation, rather than just a subset of the security features.

4.2.2 The following is a list of platform security features that could be selected. However, depending on the type of platform, certain features may not be selectable due to inherent nature of the platform not able to resist against specific attacks:

Platform Security features (PSFs)	**Description**
Secure Key Storage	Keys are stored in dedicated memory space that prevent unauthorised access / disclosure.

Secure Key Generation	Platform provides features for the secure generation of cryptographic keys. This could include the use of a True Random Number Generator (TRNG) to ensure the sufficiency of entropy. Cryptographic keys generated shall be securely stored.
Secure Key Update	Platform provides cryptographically authenticated means for the secure update of keys.
Root-of-Trust	Platform implements a Root-of-Trust (RoT). The RoT may be “fixed function” or “programmable”. The RoT is protected against physical and logical manipulations. “Programmable” RoT shall be updated in a secure manner.
Secure Boot	Platform provides features to securely boot up, ensuring the boot up sequence cannot be tampered. Platform may rely on the Root-of-Trust as part of secure boot.
Secured Device Identity	Platform provides features to cryptographically verify the identity of the platform. Stored identity shall be protected against physical attacks.
Attestation	Platform provides cryptographic attestation service for reporting on the device identity, platform integrity and measurement status for remote verification.
Platform Integrity Verification	Platform provides features to verify the platform integrity during runtime of the application.
Secure Firmware Update	Platform provides feature for securely updating the application firmware. The integrity of the firmware shall be cryptographically verified.
Secure Data Storage	Platform provides features for the confidentiality and integrity protection of the data that is stored.
Secure Access Policy	Platform provides security policy features to secure and govern the usage of the data and credentials, for instances: 1. Access conditions to govern the usage of data and credentials 2. Policy attributes to govern the access to data and credentials

Memory Protection	Platform provide features to configure selected sectors as unreadable and/or unexecutable. This includes firmware readout protection.
Debug Access Port	Platform provides features to permanently remove access to debug port(s).
Secure Reset	Platform provides features to reset the device in a secure manner. For instances when readout protection is turned off, keys, firmware and application data are securely erased. Similarly, when debug ports are re-enabled, keys, firmware and application data are securely erased. The platform could also provide features to ensure the device no longer could be reset upon entering a specific operational state or configuration.
Temporary Decommissioning	Platform provides features to temporarily decommission the platform, for instances, files storing critical data and secret credentials can be cryptographically disabled temporarily to prevent these files from being access during temporary decommission state. Platform provides features to cryptographically re-commission the platform into the operational state.
Permanent Decommissioning	Platform provides features to permanently decommission the platform, for instances, files storing critical data and secret credentials can be cryptographically erased permanently to prevent these files from being access any further, in a similar manner as per Secure Reset.
Secure Communication to external entities (e.g., cloud)	Platform provides features to establish secure communication to external entities.
Secure bus communication	Applicable only for Secure Element. Platform provides bus encryption between the MCU and SE to protect the confidentiality and integrity of the data and credentials transferred between the MCU and SE.
Secure binding of MCU with SE	Applicable only for Secure Element. Platform provides cryptographic binding features to secure the pairing of MCU with SE and provide protection against the physical removal of the SE and attaching to un-authorized MCU.

Others	This list is not meant to be exhaustive. Given developers from time to time may develop innovative security measures to mitigate threats, developers may additionally include such measures into the scope of evaluation.

4.3 Mapping of the CLS-Ready to CLS

4.3.1 As outlined, one of the intents of the CLS-Ready is to streamline the testing and lower the effort needed for an end device manufacturer to achieve CLS Level 4.

4.3.2 A CLS-Ready platform would contribute towards the fulfilment of the following CLS Level 4 requirements.

Platform Security Functions (PSF)	**CLS Level 4 Minimum Test Spec**	**ETSI EN 303 645**	**IMDA Lifecycle Checklist**
Secure Key Storage	Physical Attacks Side channel analysis and fault injection	5.4-1	CK-LP-02, CK-LP-03, CK-LP-05, CK-LP-06, CK-LP-07, CK-LP-09
Secure Key Generation	Physical Attacks Side channel analysis and fault injection	5.4-4	
Secure Key Update	Physical Attacks		
Root-of-Trust	Physical Attacks Side channel analysis and fault injection	5.4-2, 5.7-1	
Secure Boot	Side channel analysis and fault injection	5.6-3, 5.7-1	
Secured Device Identity		5.4-2	
Attestation			
Platform Integrity Verification	Physical Attacks Side channel analysis and fault injection	5.4-2	
Secure Firmware Update	Tests related to FW update	5.3-7, 5.3-9, 5.3-10	
Secure Data Storage	Physical Attacks	5.4-1	

	Side channel analysis and fault injection		
Secure Access Policy		5.6-8	
Memory Protection		5.6-8	
Debug Access Port Security	Tests related to FW retrieval from debugging ports Physical Attacks To ensure that the device does not have unnecessary exposed physical interfaces.	5.6-3. 5.6-8	
Secure Reset		5.11-1	
Temporary Decommissioning		5.11-1	
Permanent Decommissioning		5.11-1	
Secure Communication to external entities (e.g., cloud)	Communications, Ports and Services	5.5-1, 5.5-6, 5.5-7	
Secure bus communication	Physical Attacks Side channel analysis and fault injection	5.5-6, 5.5-7, 5.6-3	
Secure binding of MCU with SE	Physical Attacks Side channel analysis and fault injection	5.5-8	

5 GENERAL PROCESS OF CLS-READY

5.1 Process Overview

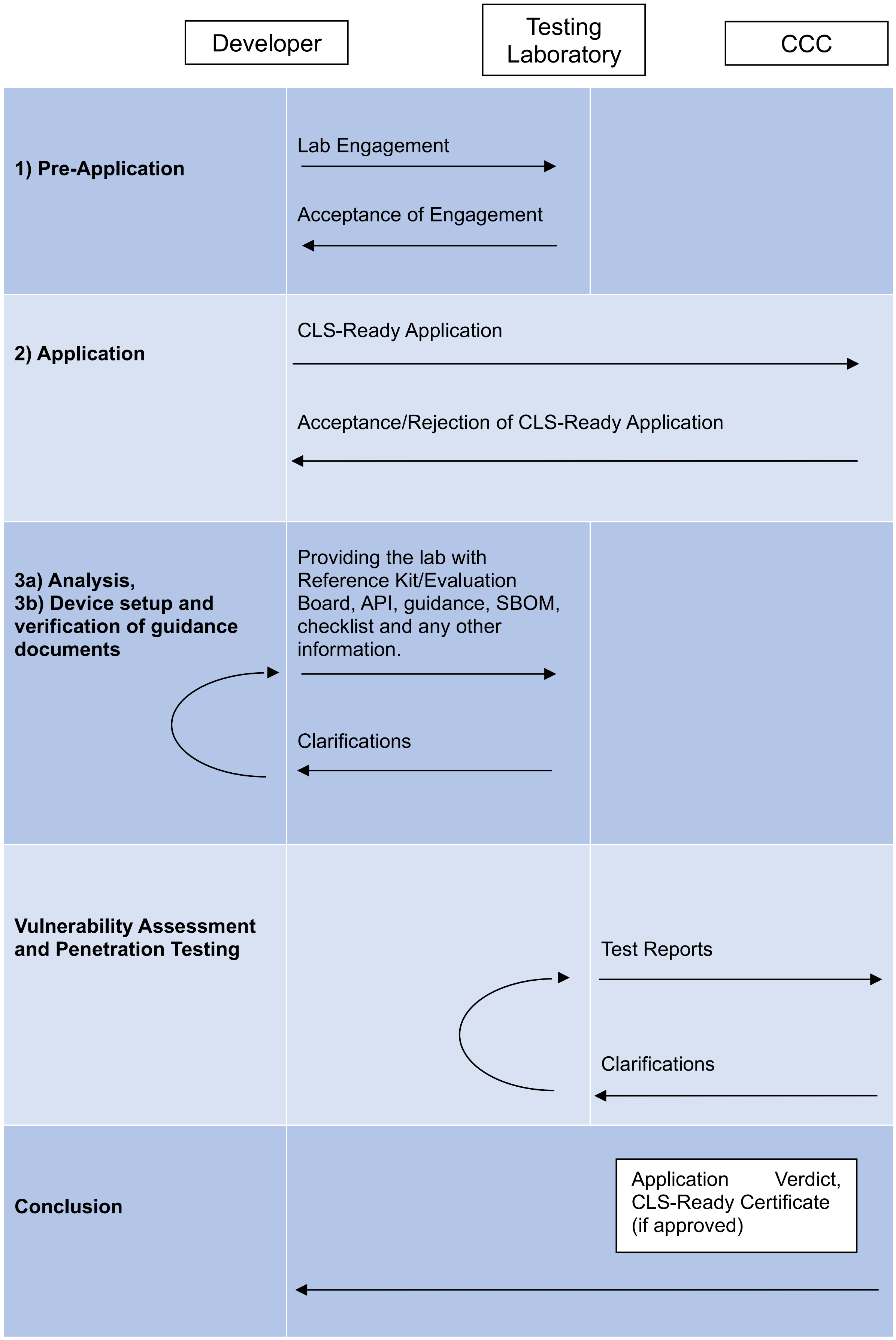
5.1.1 The key roles and responsibilities within the CLS-Ready are as follows:

a. CCC: CCC operates under the ambit of CSA. Being the scheme owner, CCC oversees the entire management and operations of the scheme. CCC oversees the procedures, reviews and validates the work performed by the testing laboratory to ensure consistency and quality of the testing. CCC is the authority to issue the CLS-Ready label and to conduct random checks on developers to ensure that the CLS labels are correctly used.

b. Developer: The developer is the applicant who develops, manufactures, or creates the platform. The developer is responsible for providing the information required by the CLS-Ready and supports the TL for the conduct of the testing. The application can also be submitted by a Testing Laboratory on behalf of the applicant.

c. Testing Laboratory (TL): The TL is an independent commercial testing laboratory which is approved under the CLS and CLS-Ready. The TL conducts evaluation on the platform provided by the developer and reports its results to the CCC and the developer.

5.1.2 The following outlines the various stages of the CLS-Ready process:


Developer
Testing Laboratory
CCC
1) Pre-Application
Lab Engagement
Acceptance of Engagement
2) Application
CLS-Ready Application
Acceptance/Rejection of CLS-Ready Application
3a) Analysis,
3b) Device setup and verification of guidance documents
Providing the lab with Reference Kit/Evaluation Board, API, guidance, SBOM, checklist and any other information.
Clarifications
Vulnerability Assessment and Penetration Testing
Test Reports
Clarifications
Conclusion
Application Verdict, CLS-Ready Certificate (if approved)

5.2 Pre-Application Phase

5.2.1 Feasibility Study

Apart from commercial considerations, a developer intending to apply for CLS-Ready should carefully study the requirements. The developer shall ensure that the required information is available before making an application.

5.2.2 Lab Engagement

The developer is required to engage a TL to perform the evaluation. The terms of engagement shall be as negotiated between the developer and the TL. CCC will not be involved in any contractual arrangements between the developer and the TL, nor shall CCC be a party to the contract between the developer and the TL.

5.2.3 Enquiry for CLS-Ready

a. Enquiries should be addressed to the CCC at the following address:

The Technical Manager,
CLS-Ready
Cybersecurity Certification Centre
Cyber Security Agency of Singapore (CSA)
5 Maxwell Road MND Complex #03-00 Tower Block
Singapore 069110

Or

certification@csa.gov.sg

5.3 Application for CLS-Ready

5.3.1 All applications are to be made via the application form which is located at the CLS-Ready website (https://go.gov.sg/apply-cls-ready), which includes submitting the relevant documents. Any application fees shall be duly paid.

5.3.2 All documents and deliverables to be submitted shall be provided in English.

5.3.3 Upon the submission of the application, CCC shall review the application and inform the applicant via email of the application outcome.

5.4 Analysis Stage

5.4.1 To facilitate the testing, the following should be provided to the testing laboratory:

- Reference Kits/Evaluation Boards;
- API scripts for testing the PSFs;

- User guidance;
- Software Bill of Materials (SBOM);
- Duly completed CLS-Ready checklist; and
- Any other information as deemed useful by the applicant to facilitate the testing.

5.4.2 The testing laboratory shall review the checklist and any other information regarding the platform in order to identify any potential security concerns and to devise appropriate test cases.

5.5 Device setup and verification of guidance documents

5.5.1 Guidance documents is an important aspect in order to ensure that the end device manufacturers could leverage on the security features provided by the underlying platform.

5.5.2 The guidance document shall be written in a manner that is easily understood by the end device manufacturers. If the hardware platform's functions are configurable, the guidance document shall indicate secure values as appropriate.

5.5.3 The guidance document shall also describe possible modes of operation of the platform, their consequences, and procedures for reverting/restoring the platform back into a secure configuration.

5.5.4 The testing laboratory shall examine the guidance document(s) provided to ensure that the guidance document provided meets the requirements stated above.

5.6 Vulnerability Analysis

5.6.1 The testing laboratory shall examine sources of information publicly available to identify potential vulnerabilities of the platform.

5.6.2 The testing laboratory shall also examine sources of information publicly available to identify generic vulnerabilities (vulnerabilities discovered on similar device-type) that could potentially be applicable for the platform and its components and determine if they are applicable for the RF.

5.6.3 The testing laboratory can make use of several established sources, such as Common Vulnerabilities and Exposures (CVE), and public search engines.

5.6.4 The testing laboratory may make use of vulnerability scanning tools and techniques to identify potential or known vulnerabilities.

5.6.5 From information collected through the preceding search for potential vulnerabilities in the public domain or through scanning tools, the testing laboratory shall devise a list of potential security vulnerabilities and potential attack paths. The testing laboratory should take into consideration the sensitive assets that must be protected, in order to devise adequate test plans. The test plans shall incorporate all relevant minimum test specifications as set out by the Cybersecurity Labelling Scheme and those of which specified in section 4.3.

5.6.6 In addition, the test laboratory could leverage on Malformed Input Testing (also known as fuzz testing), where applicable, to discover coding errors, security loopholes in the software of the platform. The testing laboratory is encouraged to make use of automated fuzzing software tools and prioritise on the interfaces that are deemed to be more critical. It should be noted that a device crash due to fuzz testing doesn’t always necessarily signify a potential exploitable vulnerability. The developer, together with the testing laboratory, shall analyse the results to determine whether the crashes could lead to an exploitable vulnerability.

5.7 Penetration Testing

5.7.1 The testing laboratory shall prioritise the test cases to ensure the intended outcome of the CLS-Ready programme could be achieved.

5.7.2 The testing laboratory shall also arrange for a meeting with CCC to present the results. The testing laboratory may be required to perform additional testing if CCC deems the testing performed to be insufficient/inadequate.

5.7.3 Following the penetration testing, the test laboratory shall submit a concise test report containing at least the following:

- Executive Summary
- Verdict on the analysis of guidance document
- Results on the search for potential vulnerabilities in the public domain, including the list of search terms.
- Test results from PT stage -
  - For test cases which the platform passed, an indicative statement by the lab would suffice.
  - For test cases which the platform failed, the lab shall record the detailed setup and procedure such that the results could be reproduced.
- Recommendations or additional comments, if any.

5.8 Conclusion

5.8.1 Upon completion of testing, and if the product is deemed to fulfil CLS-Ready requirements, CCC will issue the CLS-Ready certificate and update the list of certified platforms that is published on the CSA website.

5.9 Changes to Conditions for CLS-Ready certification

5.9.1 CCC reserves the right to make changes to CLS-Ready Publications and to any conditions for certification under the CLS-Ready. If such changes substantially affect ongoing test activities, CCC shall be entitled to require the developer to submit a fresh application for labelling.

5.10 Cryptography

5.10.1 The CLS-Ready does not address the inherent qualities of cryptographic algorithms. Nonetheless, the implementation of the cryptographic algorithm is within the scope of CLS-Ready.

6 APPLICANT OBLIGATIONS

6.1 Vulnerability Disclosure

6.1.1 One of the fundamental requirements under CLS-Ready is for the developer to implement a Vulnerability Disclosure Program. Whenever a vulnerability is reported to the developer, the developer shall notify CCC as early as possible, detailing the vulnerability, the impact, remediation plans and timeline.

6.2 Defined Support Period for Security Updates

6.2.1 Another fundamental requirement under the CLS-Ready is for the developer to provide information on the defined support period. The defined support period refers to the minimum period in which the developer agrees to provide security updates to the platform. Security updates to the platform should be provided in a secure and timely manner.

6.2.2 Minimally, the defined support period must be provided on the developer’s website.

7 CLS-READY CERTIFICATE

7.1 Validity

7.1.1 CLS-Ready certificate is valid for the period in which the developer will support the device with security updates, up to a maximum of a period of 5 years.

7.1.2 While the general validity is for a period of a maximum of 5 years, the label could be revoked if any of the conditions in Section 7.4 is met.

7.1.3 Upon expiry, a new CLS-Ready application is required to obtain a new certificate.

7.2 Principles

7.2.1 Upon receipt of the CLS-Ready certificate, the developer agrees to continuously adhere to the following principles:

a. The certified platform continues to fulfil the security requirements of CLS-Ready.

b. CCC shall be informed immediately of any changes that could affect the ability of the developer/platform to fulfil the CLS-Ready requirements.

c. The developer must not make any statements about its platform that CCC deems to be misleading or unjustified. Examples include all models being certified when it is only a specific model that has been issued with the certificate; or claims a larger set of PSFs being included in the scope of certification.

d. The developer must not use the certificate in any way that could discredit the Cyber Security Agency of Singapore, Cybersecurity Certification Centre and the CLS-Ready.

7.3 CCC Audit and Testing

7.3.1 CCC reserves the right to conduct random checks / surveillance and testing of the certified platform. The purpose of the audit is to ensure that certified platforms are compliant to the requirements of the CLS-Ready. Manufacturers are **not** expected to pay for the random check / surveillance.

7.3.2 For this purpose, CCC may choose to re-test the certified platform using a separate testing laboratory that was not used during the initial testing process.

7.4 Revocation of the CLS-Ready certification

7.4.1 CCC is entitled to revoke a CLS-Ready certification issued under the CLS-Ready forthwith if:

a. The TL or developer is in breach of any terms of CLS-Ready Publications, and/or any other terms as agreed to in writing with CCC;

b. The developer has failed to disclose any known or discovered vulnerabilities that, in CCC's opinion, can undermine the CLS-Ready certificate;

c. The developer fails to take any corrective measures during the period of grace given by CCC, to the satisfaction of CCC;

d. The developer misuses the CLS-Ready certificate, CLS-Ready status, or any proprietary names and marks associated with CCC or CLS-Ready;

e. The developer makes any statement that misrepresents any aspect of testing or the effect of the labelling under the CLS-Ready;

f. CCC finds that the TL was in a position of conflict that impaired its ability to conduct a fair and impartial testing of the platform;

g. The certified platform no longer meets the conditions under which the certificate was granted or does not meet any changed conditions for certification introduced by CCC after the device was originally certified.

h. CCC discovered that the developer has made a false statement or declaration in any deliverables submitted to CCC.

7.4.2 Upon the revocation of a CLS-Ready certificate, the developer and the testing laboratory shall immediately cease all use of the CLS-Ready certificate, or any proprietary names and marks associated with CSA, CCC, or the CLS-Ready, and desist from holding the applicable products out as being labelled under the CLS-Ready.

7.4.3 CCC will inform the developer and the testing laboratory in writing of the revocation of the CLS-Ready certification and will remove the listing on CSA's website.

8 ASSURANCE CONTINUITY

8.1.1 Assurance Continuity defines the approach to minimising redundancy in platform assessment, allowing a determination to be made as to whether independent assessments need to be re-performed as changes are made to a certified platform to address security issues, minor bugs, improve the operation of the hardware or peripherals, and to add support for new models of equipment.

8.1.2 For major changes that would invalidate the previous test results the developer shall subject the platform for retesting with a Testing Laboratory.

8.1.3 For minor updates/patches, the CLS-Ready certificate will continue to remain valid.

9 REQUIREMENTS FOR CLS-READY TEST LABORATORY

9.1.1 All testing laboratories approved to conduct CLS Level 4 testing are also approved for conducting tests on CLS-Ready platforms.

10 MECHANISM FOR COMPLAINTS, DISPUTES AND APPEALS

10.1.1 The objective of the CLS-Ready Complaints, Disputes and Appeals process[1] is to track feedback from stakeholders and to ensure that issues are resolved:

[1] A dispute is a written statement to CCC indicating disagreement with a decision made by CCC. A complaint is a written statement to the CCC indicating dissatisfaction with a service provided by CCC or the Testing Laboratory. An appeal is a written statement to CCC indicating dissatisfaction with the resolution of a complaint or dispute.

a. Developers may contact CCC directly if they are dissatisfied with any services provided by the testing laboratories regarding their project. CCC holds all raised concerns in strict confidence.

b. Developers or testing laboratories may contact the Head of Cybersecurity Certification Centre directly if they disagree with a decision. CCC holds all raised concerns in strict confidence.

10.1.2 CCC shall acknowledge the receipt of a formal complaint, dispute or appeal and investigates the content of the complaint, dispute, or appeal to determine whether the complaint, dispute or appeal relates to test activities for which CCC is responsible.

a. If CCC does not accept the complaint, dispute, or appeal, this is explained in writing to the party lodging the complaint.

b. If CCC accepts the complaint, dispute, or appeal, it then processes it, recording and verifying all the necessary information (as far as possible) in order to reach a decision regarding the complaint, dispute, or appeal.

10.1.3 To begin with, an attempt is made to reach an agreement regarding the disputed matter with the certifier responsible for the procedure concerned.

10.1.4 If any issue cannot be resolved to the satisfaction of the originating party, the originating party may contact CCC. Resolution of the issue is under the responsibility of the Head of the Cybersecurity Certification Centre, whose decision made on any issue raised is final.

11 FEES

11.1 General Policy

11.1.1 The fees for CCC's work in connection with the CLS-Ready process shall be prescribed by CCC and published on the CSA website. CCC reserves the right to review the fees as and when necessary. These costs are based primarily on the type of procedure requested, the specific object to be labelled, the scope desired and the degree of assessment envisaged or required. However, the procedure costs are charged irrespective of the ordering party's attributes (company name, company size, registered office, division, etc.).

11.1.2 All fees are in Singapore dollars and are subjected to GST.

11.1.3 Application fees are always charged as agreed – regardless of whether a CLS-Ready certificate has been issued or could not be issued due to technical deficiencies or other deficiencies, the applicant cancelled the procedure or CCC suspended the procedure due to failure to provide the necessary information.

11.1.4 If the developer requires modifications to reports, expert opinions or certificate that CCC has already approved, the additional effort will be charged to the developer. This also applies to performing re-certification, if these become necessary due to reasons caused by the developer.

11.1.5 All fees mentioned in CLS-Ready publications are exclusive of fees charged by testing laboratories for testing work performed.

12 LIABILITY

12.1 Disclaimer

12.1.1 CSA makes no representations, warranties, or covenants of any kind, whether express, implied, or statutory, with respect to the CLS-Ready, TLs, or any testing conducted, or certificates awarded under the CLS-Ready, including without limitation any warranties of merchantability, satisfactory quality, fitness for a particular purpose or non-infringement of third-party rights and any warranties that they are accurate, reliable, or error-free. All implied warranties of any kind are excluded to the maximum extent permitted by law. Any person's use of and/or reliance on the CLS-Ready, TLs, or testing conducted, or labels awarded under the CLS-Ready shall be at their own risk.

12.1.2 To the extent permissible by law, in no event will CSA, its officers, directors, employees or any other person acting under the direction of CSA be liable to a developer, developer, TL or any other person for any loss or damage under any theory of liability, whether direct, indirect, incidental, special, consequential or exemplary in nature, arising out of or in connection with the CLS-Ready or any decisions by CSA or any such person in relation to the CLS-Ready if made in good faith in the ordinary course of the discharge of the CSA's duties under the CLS-Ready, including but not limited to lost profits, loss of goodwill and business opportunities, costs of procurement of substitute goods or services, business interruption or loss of business information and data, even if the CSA has been advised of the possibility of such damages.

References

[1] ETSI, “Cyber Security for Consumer Internet of Things,” ETSI EN 303 645.

[2] Info-communications Media Development Authority of Singapore, “IMDA Internet of Things (IoT) Cyber Security Guide”.

[3] Cyber Security Agency of Singapore, “CLS Publication #2 - Scheme Specifications,” Version 1.1, April 2021.

[4] Cyber Security Agency of Singapore, “SCCS Publication #2 - Requirements for Approving Common Criteria Test Laboratory,” Version 5.0, June 2018.

ACRONYMS

The following acronyms are used:

CC	Common Criteria for Information Technology Security Evaluation
CCC	Cybersecurity Certification Centre
CCTL	Common Criteria Testing Laboratories
CLS	Cybersecurity Labelling Scheme
CSA	Cyber Security Agency of Singapore
DUT	Device Under Test
ETSI	European Telecommunications Standards Institute
HPL	Historical Product List
IMDA	Info-communications Media Development Authority
IoT	Internet of Things
LPL	Labelled Product List
SCCS	Singapore Common Criteria Scheme
TL	Testing Laboratory