Cybersecurity Labelling Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

Cybersecurity Labelling Scheme (CLS)
Publication No. 1

Overview of the Scheme

October 2020
Version 1.0

FOREWORD

The Cybersecurity Labelling Scheme (CLS) is part of Cyber Security Agency's (CSA) efforts to better secure Singapore's cyberspace and to raise cyber hygiene levels.

Under the CLS, the cybersecurity label would provide an indication of the level of security in the network-connected smart devices. It aims to improve security awareness by making such provisions more transparent to consumers and empowers consumers to make informed purchasing decisions for products with better security using the information on the cybersecurity label.

The CLS seeks to incentivise developer/manufacturers to develop and provide products with enhanced cybersecurity provisions. The labels also serve to differentiate smart devices with better cybersecurity safeguards in the market, from their competitors.

At the same time, CSA intends to engage other like-minded partners for mutual recognition of the CLS with the objective of eliminating duplicated assessments across national boundaries.

The CLS is an initiative under the Safer Cyberspace Masterplan, to create a safer cyberspace and protect the public and enterprises against cyber threats, as Singapore moves towards a Digital Economy and Smart Nation.

The CLS is owned and managed by the Cybersecurity Certification Centre (CCC), under the ambit of the Cyber Security Agency of Singapore (CSA).

AMENDMENT RECORD

Version	Date	Author	Changes
1.0	October 2020	Cyber Security Agency of Singapore	Release

CONTENTS

1 INTRODUCTION 5

2 BACKGROUND 5
2.1 Impetus for CLS 5
2.2 Baseline Security in Consumer Products 6

3 ORGANISATION AND MANAGEMENT OF CLS 7

4 OVERVIEW OF THE CLS 8
4.1 Overview 8
4.2 Cybersecurity Labelling Levels 8

5 ASSESSMENT TIERS 9
5.1 Overview of Assessment Tiers 9
5.2 Assessment Tier #1 – Security Baseline Requirements 9
5.3 Assessment Tier #2 – Lifecycle Requirements 9
5.4 Assessment Tier #3 – Software Binary Analysis 10
5.5 Assessment Tier #4 - Penetration Testing 10

6 GENERAL PROCESS FOR LABELLING OF INTERNET-CONNECTED DEVICE 11
6.1 Process Overview 11
6.2 Pre-Application Phase 13
6.3 Application for Labelling 14
6.4 Testing Phase (Only for Tier 3 onwards) 14
6.5 Conclusion - Awarding of the CLS Label 15
6.6 Changes to Conditions for Labelling 15
6.7 Cryptography 15

7 APPLICANT OBLIGATIONS 15
7.1 Vulnerability Disclosure 15
7.2 Defined Support Period for Security Updates 15

8 CYBERSECURITY LABEL 16
8.1 Label 16
8.2 Label Validity 16
8.3 Requirements of the Cybersecurity Label 16
8.4 How the Cybersecurity Label is to be Affixed or Displayed 17
8.5 Labelling Principles 17
8.6 CCC Audit and Testing 17
8.7 Revocation of the Cybersecurity Label 18

9 REQUIREMENTS FOR CLS TEST LABORATORY 19

10 MECHANISM FOR COMPLAINTS, DISPUTES AND APPEALS 20

11 FEES 21

11.1 General Policy 21

12 LIABILITY 22
12.1 Disclaimer 22

REFERENCES 23

ACRONYMS.....23

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 Cybersecurity Labelling Scheme (CLS). It outlines the scheme objectives, description of the scheme, its organisation and management, as well as an overview of the testing process.

1.0.2 This document also sets out the requirements and procedures for the labelling of the internet connected device under the CLS. It also establishes the technical oversight role of Cybersecurity Certification Centre (CCC) in the CLS and sets out general terms and conditions for the developer and/or the Testing Laboratory (TL) that apply for such a label.

2 BACKGROUND

2.1 Impetus for CLS

2.1.1 Cities around the world have ushered in the era of digital transformation and Singapore is no different as we work towards our vision of a Smart Nation. The Smart Nation empowers the Singapore economy through technology and digital innovation and aims to bring about a better quality of life for all. The Government, through policies and initiatives such as the Safer Cyberspace Masterplan, also aims to better prepare and equip Singapore to embrace the ever-changing digital landscape.

2.1.2 The Smart Nation initiative rests on bridging communications and enabling digital services. This brings about the phenomenon of manufacturing every type of device to be “smart”. From traffic cameras to lampposts and even the most mundane of devices like kitchen appliances and baby monitors, they are now part of the “Internet of Things” or IoT.

2.1.3 IoT can bring about huge benefits to enterprises’ productivity and individuals’ quality of life. As IoT gets rapidly proliferated, the issues relating to cyber security threats become increasingly important. Devices with poor security may be easily exploited by individuals or groups with malicious intents to form botnets and potentially used to participate in Distributed Denial-of-Service (DDoS) attacks, as evident from incidents such as the Mirai and Silex malwares.

2.1.4 The “IoT Security Landscape” which is jointly published by CSA Singapore and Ministry of Economic Affairs and Climate Policy, Netherlands, cites “Evaluation and Certification” among one of the security challenges. While there are well-established certification schemes for IT security products such as Common Criteria (CC) or ISO/IEC15408, the same cannot be seen for IoT and cybersecurity provisions for IoT continue to remain opaque to general consumers.

2.1.5 The intent of the Cybersecurity Labelling Scheme is to improve the

transparency of cybersecurity provisions. Under this scheme, the cybersecurity label would provide an indication of the level of security in the products. Consumers are thereby empowered to make informed purchasing decisions. By enhancing consumer security awareness, this scheme seeks to incentivise manufacturer to develop products with better security for the market, leading towards a safer and more secure cyber space.

2.2 Baseline Security in Consumer Products

2.2.1 A majority of consumer IoT products has inadequate cybersecurity provisions. Fundamental security weaknesses such as universal default passwords continue to be prevalent. In addition, consumer smart devices are often characterised by a short time-to-market cycle for new versions to reach the market, where there is less emphasis for good cybersecurity design to be incorporated from the start. Due to such characteristics, formal evaluation and certification schemes such as Common Criteria that provide higher security assurance might be deemed infeasible as the evaluation costs and duration are prohibitive relative to the margins for these devices.

2.2.2 Hence, the Cybersecurity Labelling Scheme is designed to be rapid and cost-effective. The scheme seeks to provide a basic level of security assurance through the elimination of common vulnerabilities and the use of a simple, tiered, and progressive assessment model for IoT devices that avoids resource-intensive security evaluations. The CLS should provide a basic level of security hygiene in which it is typically expected for consumer IoT devices to be able to deter causal adversaries utilizing common attack vectors such as default factory credentials or exploiting vulnerable protocols.

2.2.3 It is important to note that the Cybersecurity Labelling Scheme does not offer formal security assurance. Given sufficient time, determined adversaries who possesses advanced skillsets and tools would likely be capable of compromising such IoT devices, regardless whether it is labelled. Users seeking higher security assurance (e.g. enterprise, manufacturing, industrial applications and healthcare) are strongly recommended to consider devices certified under formal evaluation and certification schemes. Details relating to these higher assurance schemes are available on the CSA website (go.gov.sg/common-criteria).

3 ORGANISATION AND MANAGEMENT OF CLS

3.1 The CLS is owned and managed by the Cybersecurity Certification Centre (CCC), under the ambit of the Cyber Security Agency of Singapore (CSA).

3.2 The overall policy of the CLS scheme is set by the Cybersecurity Certification Centre (CCC). The CCC is responsible for the direction of the CLS scheme, ensuring that the organisation and management of the functions of testing achieve high standards of competency, impartiality, and consistency. The CCC approves standards, publications, and projects.

3.3 The CCC establishes the requirements for the testing laboratories and oversees the testing laboratory approval process. The testing laboratory is approved only after it is assessed to be compliant to the requirements specified in Chapter 9 - Requirements for CLS Test Laboratory.

4 OVERVIEW OF THE CLS

4.1 Overview

4.1.1 The Cybersecurity Labelling Scheme (CLS) is a voluntary scheme, for a start. Products that apply for the Cybersecurity Label shall undergo a series of assessments and tests, depending on the level of Cybersecurity Label that the developer wishes to attain.

4.2 Cybersecurity Labelling Levels

4.2.1 The CLS comprises four (4) cybersecurity levels, with each higher level being more comprehensive in the assessment.

4.2.2 The requirements of testing under each of the cybersecurity levels are summarised in Table 1 - Cybersecurity Levels and Assessment Tiers below.

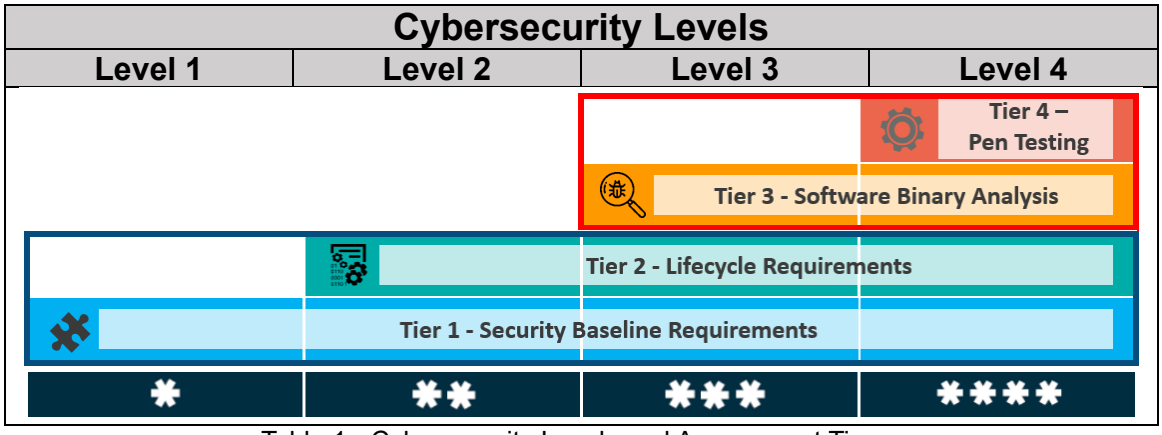


Table 1 - Cybersecurity Levels and Assessment Tiers

4.2.3 Under each labelling level, depending on the intended level of Cybersecurity Label that the manufacturer wishes to attain, the product shall be subjected to the applicable assessment tiers.

4.2.4 There are 4 different tiers of assessment, covering different security requirements. The assessment tiers are briefly described in Chapter 5 - Assessment Tiers. Detailed requirements about each of these testing tiers are provided in CLS Publication #2 – Scheme Specifications [1].

5 ASSESSMENT TIERS

5.1 Overview of Assessment Tiers

No.	Assessment Tier	Format	Involved Roles
1	Security Baseline Requirements	Developer's declaration of conformance. No independent check by the test laboratory.	CCC; Developer
2	Lifecycle Requirements		CCC; Developer
3	Software Binary Analysis	3rd party independent assessment by testing laboratory	CCC; Developer; Testing Laboratory
4	Penetration Testing		CCC; Developer; Testing Laboratory

Table 2 - Overview of Assessment Tiers

5.2 Assessment Tier #1 – Security Baseline Requirements

5.2.1 Assessment Tier 1 seeks to address the most common IoT security problems by requiring developers to conform to security baseline requirements within the ETSI EN 303 645 – Cyber Security for Consumer Internet of Things [2]. The ETSI EN 303 645 technical specification specifies a set of security baseline provisions which includes having no universal default passwords, implementing means to manage vulnerability reporting, and keeping device software updated.

5.2.2 Under Assessment Tier 1, the developer shall complete and submit the conformance checklist (located in CLS Pub #2 – Scheme Specifications [1]) specifying conformance status to the security provisions within the technical specification.

5.2.3 The coverage and requirements increase progressively for the higher security levels. Non-conformance to provisions categorised as "Mandatory" shall lead to the failure of this activity.

5.2.4 For CLS Level 1, the assessment tier is premised upon the developer's declaration of conformance to the requirements. For CLS Level 2 and above, the conformance checklist shall be reviewed by CCC prior to approval in Assessment Tier 1.

5.3 Assessment Tier #2 – Lifecycle Requirements

5.3.1 Assessment Tier 2 seeks to ensure that devices are developed according to a security-by-design framework and processes. The development of these devices can be supported through the adoption of lifecycle

processes consisting of general secure software development activities (e.g. threat modelling, secure engineering approach), and by having supporting processes in place to be able to respond to new vulnerabilities.

5.3.2 Assessment Tier 2 references the lifecycle requirements specified in the IMDA IoT Cyber Security Guide [3].

5.3.3 Under Tier 2, the developer shall complete and submit the conformance checklist (located in CLS Pub #2 – Scheme Specifications [1]) specifying conformance to the lifecycle requirements.

5.3.4 The conformance checklist shall be reviewed by CCC prior to approval.

5.3.5 CCC shall review the declaration and rationale prior to approval.

5.4 Assessment Tier #3 – Software Binary Analysis

5.4.1 CLS Tier 3 analyses the device's software (device firmware and companion mobile applications) for malware, known vulnerabilities in third party libraries used, and for software weaknesses such as buffer overflow.

5.4.2 The software of the connected device shall be analysed using a combination of binary, malware, and mobile application scanners.

5.4.3 The developer's testing laboratory of choice shall review and interpret the scan results. At the end of the activity, the testing laboratory shall submit a report outlining test results, identified issues and method of resolution to the CCC.

5.4.4 CCC shall review the testing laboratory's report prior to approval.

5.4.5 The expected duration is around 3 - 4 days.

5.5 Assessment Tier #4 - Penetration Testing

5.5.1 CLS Tier 4 is premised upon penetration testing of the internet-connected device. The penetration testing is intended to assert that the device is reasonably resistant to common attacks usually found applicable to IoT devices and to prove that there are no obvious or critical vulnerabilities.

5.5.2 The developer shall provide sufficient production samples of the device and related user guidance documents to the testing laboratory to facilitate testing.

5.5.3 The TL shall provide a report summarising the tests performed and the results.

5.5.4 CCC shall review the testing laboratory's report prior to approval.

5.5.5 The expected total duration is around 15 days.

6 GENERAL PROCESS FOR LABELLING OF INTERNET-CONNECTED DEVICE

6.1 Process Overview

6.1.1 The labelling of internet-connected devices shall be performed within the framework of the CLS.

6.1.2 The key roles and responsibilities within the CLS are as follows:

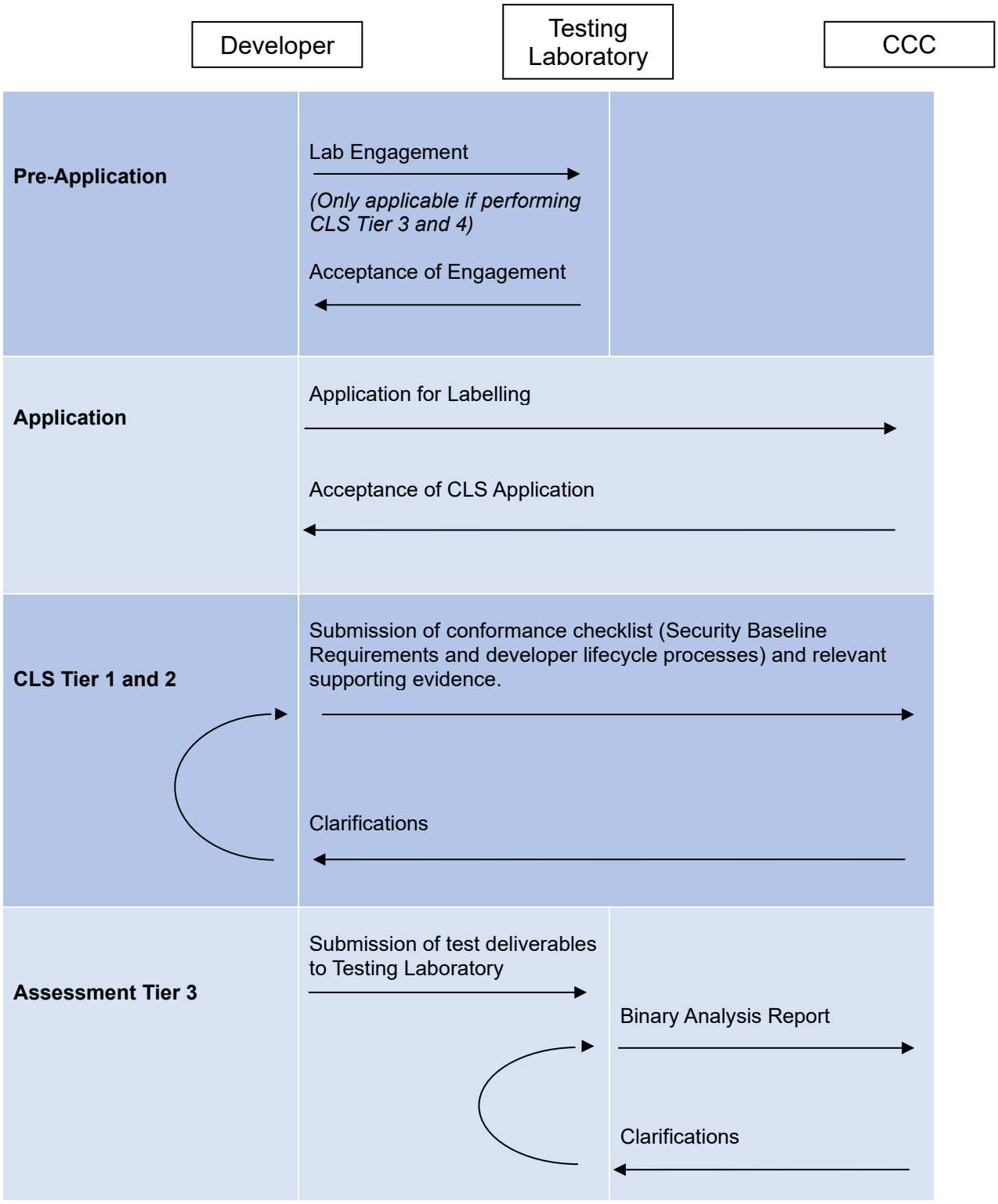
a. CCC: CCC operates under the ambit of CSA. Being the scheme owner, CCC oversees the entire management and operations of the scheme. CCC oversees the procedures, reviews and validates the work performed by the testing laboratory to ensure consistency and quality of the testing. CCC is the authority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

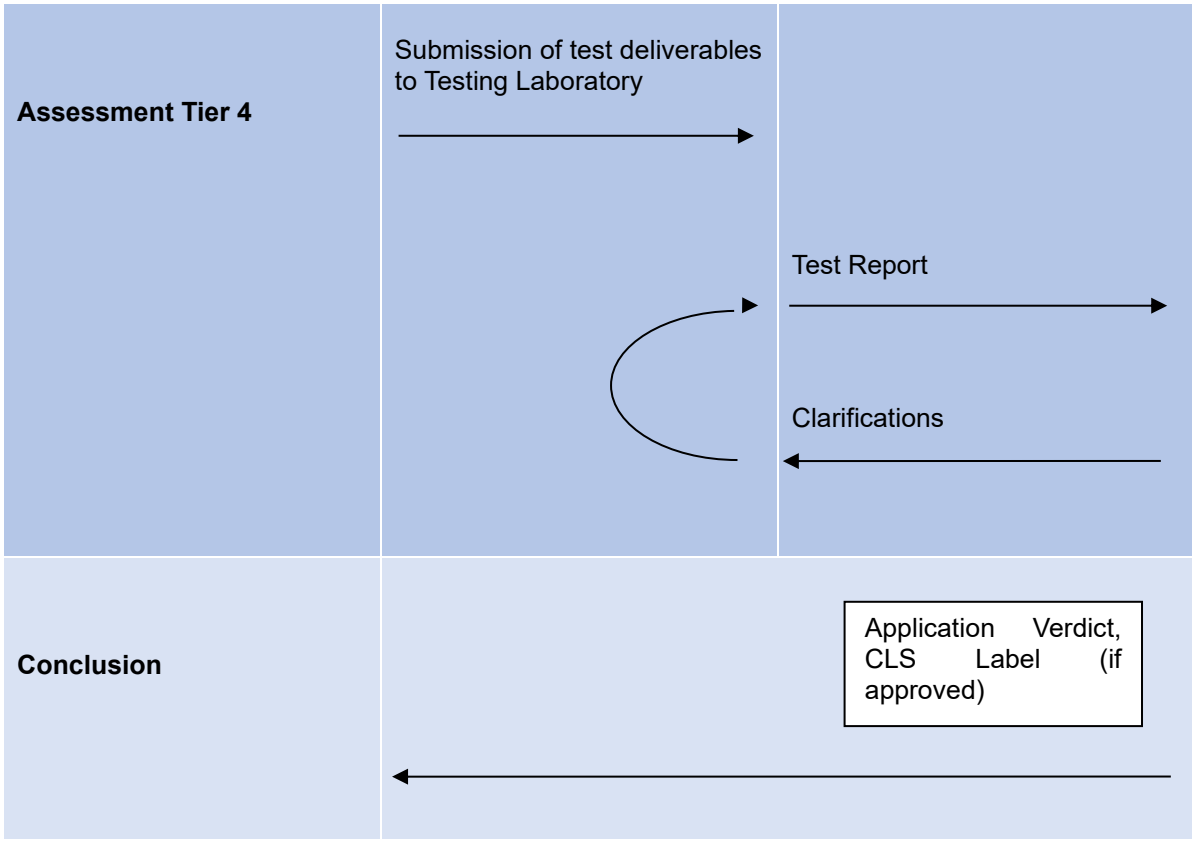
b. Developer[1]: The developer is the applicant who develops, manufactures, or creates the consumer product. The developer is responsible for providing the information required by the CLS and supports the TL for the conduct of the testing. In lieu of the developer, the application can be sponsored by either a distributor or retailer. 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. The TL is involved only in Tier 3 and Tier 4. The TL conducts assessment tests on the consumer product provided by the developer and reports its results to the CCC and the developer.

[1] An exemption is made for Wi-Fi routers intending to attain only CLS Label Level 1: Apart from the manufacturer, the developer can also be an importer that intends to supply the Wi-Fi router in Singapore.

6.1.3 There are four main phases to the entire labelling process.





6.2 Pre-Application Phase

6.2.1 Feasibility Study

Apart from commercial considerations, a developer intending to apply for label should carefully study the requirements of the four (4) tiers of CLS and determine which tier of the labelling scheme is suitable for the product. The developer shall ensure that the required evidences are available before making an application. Depending on the tier, this could include:

a. Development process documents and/or work instructions;
b. Product guidance documents and screenshots;
c. Product hardware, firmware, companion mobile applications, etc.

6.2.2 Lab Engagement

For CLS Level 3 and 4, the developer is required to engage a TL to perform the associated tasks required at the specific tiers. 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.

6.2.3 Enquiry for Labelling

a. Enquiry for labelling under the CLS should be addressed to the CCC at the following address:

The Technical Manager,
Cybersecurity Labelling Scheme
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

6.3 Application for Labelling

6.3.1 All applications for labelling are to be made via the CLS application form which is located at the CLS website (https://www.go.gov.sg/csa-cls).

6.3.2 The following deliverables (depending on the intended CLS Label level) shall be submitted during the online application:

CLS Label	Assessment Tiers and Submission Requirements
Level 1	Tier 1: Conformance Checklist
Level 2	Tier 1 and 2: Conformance Checklist
Level 3	Tier 1 and 2: Conformance Checklist Tier 3: Binary Files (Device firmware and companion mobile applications are to be provided to the TL)
Level 4	Tier 1 and 2: Conformance Checklist Tier 3: Binary Files (Device firmware and companion mobile applications are to be provided to the TL) Tier 4: Penetration Testing

Table 3 - Application Submission Requirements

6.3.3 More specific application requirements and the conformance checklist are available in CLS Publication #2 – Scheme Specifications [1].

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

6.4 Testing Phase (Only for Tier 3 onwards)

6.4.1 The required testing tasks are dependent on the CLS tier that the developer wishes to attain. Detailed requirements of the each of the CLS tiers are detailed in CLS Publication #2 – Scheme Specifications [1].

6.4.2 In the instance of Wi-Fi routers at CLS Level 1, the developer can be the importer that intends to supply the Wi-Fi router in Singapore. The importer shall be solely responsible for ensuring that all required information from the developer are available.

6.5 Conclusion - Awarding of the CLS Label

6.5.1 Upon completion of testing, and if the product is deemed to fulfil CLS requirements, CCC will issue the CLS label and update the list of labelled products that is published on the CLS website.

6.5.2 The labelled consumer product shall be listed on CSA's website.

6.6 Changes to Conditions for Labelling

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

6.7 Cryptography

6.7.1 The CLS does not address the inherent qualities of cryptographic algorithms.

7 APPLICANT OBLIGATIONS

7.1 Vulnerability Disclosure

7.1.1 One of the fundamental requirements under CLS 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.

7.2 Defined Support Period for Security Updates

7.2.1 Another fundamental requirement under the CLS 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 device. Security updates to the device should be provided in a secure and timely manner.

7.2.2 Minimally, the defined support period must be provided on the developer's website.

8 CYBERSECURITY LABEL

8.1 Label

8.1.1 A sample of the CLS label as follows:

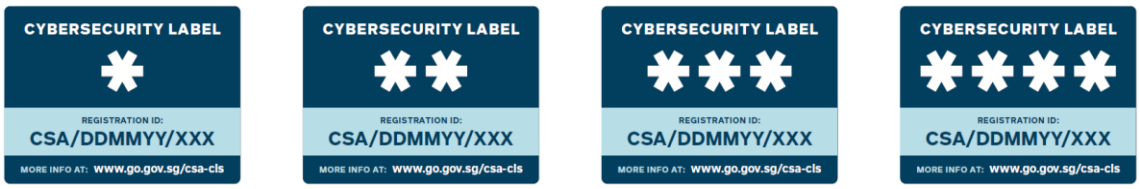


Figure 1 - Sample of CLS Label

8.1.2 The following details are provided in the label:

a. Cybersecurity level as denoted in the number of asterisk symbols present on the label.

b. Registration Identifier in the format of “CSA/ddmmyy/xxx”, where “ddmmyy” refers to the date that the device was approved for labelling.

8.2 Label Validity

8.2.1 Labels are valid for the period in which the developer will support the device with security updates, up to a maximum of a period of 3 years.

8.2.2 While the general validity is for a period of a maximum of 3 years, the label could be revoked if any of the conditions in Section 8.7 is met.

8.2.3 Labels cannot be renewed upon expiry.

8.3 Requirements of the Cybersecurity Label

8.3.1 The Cybersecurity Label must:

a. Be of the dimensions 4cm (width) by 3cm (height) or be proportionately larger;

b. Be of font, typeface, font colour as indicated in the logo guide;

c. Be of the shape, colour and contain text that is of the typeface as what is specified by the logo guide, legible and in the English language only;

d. Contain information that is consistent with or drawn from the test report for the tested good to which the Cybersecurity Label relates;

e. Be printed in an indelible manner and with a minimum resolution of 300 pixels per inch; and

f. Be made of such material as CCC may approve.

8.4 How the Cybersecurity Label is to be Affixed or Displayed

8.4.1 The Cybersecurity Label shall be affixed on either the product packaging or on the product itself.

8.4.2 The Cybersecurity Labels can be displayed in all advertisements and promotional material of labelled products in local print, broadcast and digital media. This includes, but is not limited to websites, online stores and printed catalogues.

8.4.3 In cases where the available space is too small for the Cybersecurity Label to be seen clearly, the rating must be prominently displayed.

8.4.4 If the devices are to be affixed with the Cybersecurity Label, they must have affixed to each of them a Cybersecurity Label that satisfies the following requirements:

a. The Cybersecurity Label is not damaged, defaced or obliterated so as to prevent any information on the Cybersecurity Label from being read;

b. The Cybersecurity Label is affixed in a conspicuous and unobstructed position on the product.

8.5 Labelling Principles

8.5.1 Upon receipt of the CLS label, the developer agrees to continuously adhere to the following principles:

a. The labelled product continues to fulfil the security requirements for the tier that the product is being labelled with.

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

c. The developer must not make any statements about its product labelling that CCC deems to be misleading or unjustified. Examples include all models labelled when it is only a specific model that has been issued with the label; claiming the product received a label of higher rating than what is being issued.

d. The developer must not use the cybersecurity label in any way that could discredit the Cyber Security Agency of Singapore and the Cybersecurity Labelling scheme.

e. The label must not be modified and shall be used exactly as issued by CCC.

8.6 CCC Audit and Testing

8.6.1 CCC reserves the right to conduct random checks and testing of the labelled products. The purpose of the audit is to ensure that labelled products are compliant to the requirements of the CLS publications.

8.6.2 For this purpose, CCC may choose to re-test the labelled device using a separate testing laboratory that was not used during the labelling process.

8.7 Revocation of the Cybersecurity Label

8.7.1 CCC is entitled to revoke a CLS label issued under the CLS forthwith if:

a. The TL or developer is in breach of any terms of CLS 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 label;

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 label, CLS status, or any proprietary names and marks associated with CCC or CLS;

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

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 device;

g. The labelled device no longer meets the conditions under which the label was granted or does not meet any changed conditions for labels introduced by CCC after the device was originally labelled.

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

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

8.7.3 CCC will inform the developer and the testing laboratory in writing of the revocation of the CLS label and will remove the listing of the labelled product from the Labelled Product List (LPL). The project details will be put into the common Historical Product List (HPL).

9 REQUIREMENTS FOR CLS TEST LABORATORY

9.1.1 The testing laboratory must first and foremost, be an approved Common Criteria Test Laboratory (CCTL) under the Singapore Common Criteria Scheme (SCCS) and satisfy all requirements (as stated in SCCS Publication #2 – Requirements for Approving Common Criteria Test Laboratory [4]) imposed by the SCCS.

9.1.2 The testing laboratory is allowed to provide both consultancy and evaluation services for the product under the CLS if the testing laboratory is able to demonstrate with clear role and logical separation procedures in place as well as appointing qualified evaluators and qualified consultants for the project.

9.1.3 If the testing laboratory is part of an organisation that performs activities other than IT security evaluation (e.g. consultation to product developer), the testing laboratory shall identify actual and potential conflicts of interest and ensure clear separation of control to ensure that there is no undue influence on the evaluation activities.

10 MECHANISM FOR COMPLAINTS, DISPUTES AND APPEALS

10.1.1 The objective of the CLS's Complaints, Disputes and Appeals process[2] is to track feedback from stakeholders and to ensure that issues are resolved:

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 looks into 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.

[2] 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.

11 FEES

11.1 General Policy

11.1.1 The fees for CCC's work in connection with the labelling 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 Labelling fees are always charged as agreed – regardless of whether a label 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 labels that CCC has already approved, the additional effort will be charged to the developer. This also applies to performing re-labelling, if these become necessary due to reasons caused by the developer.

11.1.5 All fees mentioned in CLS 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, TLs, or any testing conducted or labels awarded under the CLS, 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, TLs, or testing conducted, or labels awarded under the CLS 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 or any decisions by CSA or any such person in relation to the CLS if made in good faith in the ordinary course of the discharge of the CSA's duties under the CLS, 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] C. S. A. o. Singapore, “CLS Publication #2 - Scheme Specifications,” Version 1.0, October 2020.

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

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

[4] C. S. A. o. Singapore, “SCCS Publication #2 - Requirements for Approving Common Criteria Test Laboratory,” Version 5.0, June 2018.

ACRONYMS

The following acronyms are used in CLS Publication 1 and 2:

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