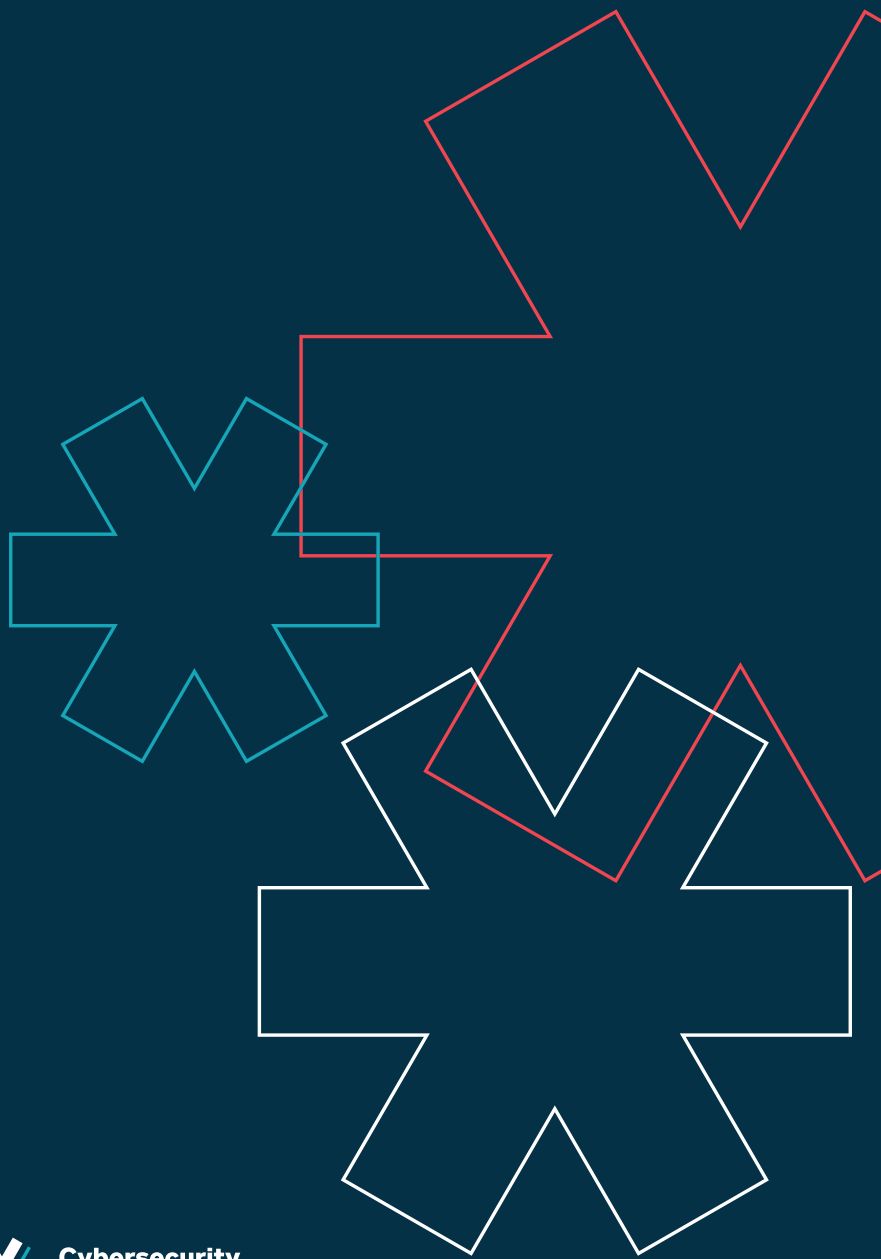
Cybersecurity Certification Guide



A publication by

CSA SINGAPORE

Cybersecurity Certification Centre
CYBER SECURITY AGENCY OF SINGAPORE

CONTENTS

■ OVERVIEW	1	Global Cyber Landscape
	2	Opportunities for Certification
■ SCHEMES	4	Cybersecurity Label Scheme (CLS)
	8	Singapore Common Criteria Scheme (SCCS)
	13	National IT Evaluation Scheme (NITES)
	14	Frequently Asked Questions (FAQ)
	17	Contacts

Published in 2021

Global Cyber Landscape

The global cyber landscape has changed dramatically in recent years, with increasing awareness of the risks and threats faced by states, businesses, and individuals. Ransomware attacks, data breaches, and other cyber incidents have made the headlines as a stark reminder that cybersecurity must be taken seriously.

At the same time, people are keen to maximise the opportunities presented by the rapid advances in digitalisation and innovation. Singapore is embarking on an initiative to create a “Smart Nation”, and businesses and individuals are keen to harness the power of technology at work and play. Singapore’s Cybersecurity Strategy aims to create a resilient and trusted digital environment to facilitate that.

New technology products are constantly coming to market. CSA offers and supports the use of Certification Schemes to provide assurance to customers that the product has been objectively assessed to be more cyber secure, and has adopted a Security-by-Design approach throughout the product life cycle.

Cybersecurity Certification Guide

Opportunities for Certification

The speed of technology adoption continues to accelerate for both work and play, with new business models and market opportunities still being unlocked.

With greater digitalisation and connectivity comes increased emphasis on cybersecurity. While cybersecurity is a concern, it is also a market opportunity. The global cybersecurity market size is forecast to grow to 345.4 billion U.S. dollars by 2026[1]; and the demand for higher quality and secure products will continue to increase.

An internationally recognised certification mark has become a necessity for local developers to expand their market reach globally.

CSA Cybersecurity Certification Centre operates the following schemes aimed at providing the security assurance that the product has undergone impartial examination and testing to ascertain that it is securely designed, implemented, and appropriate in mitigating the specified security threats.

The three schemes listed in this guide, catering to different market segments, are:

- **Cybersecurity Labelling Scheme (CLS), for labelling of network-connected consumer smart devices, to enable consumers to discern the security levels in the devices and make more informed purchase decisions;**
- **Singapore Common Criteria Scheme (SCCS), for certification of commercial IT products targeting the international marketplace;**
- **National IT Evaluation Scheme (NITES), for evaluation and certification of IT products that meets high assurance requirement for Singapore government agencies.**

Through these schemes, companies are able to demonstrate the security of their product, benchmarked against international standards.

[1] Cybersecurity Market Revenues Worldwide 2021-2026, Statista Research Department, 26 August 2021, https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/

Cybersecurity Certification Centre

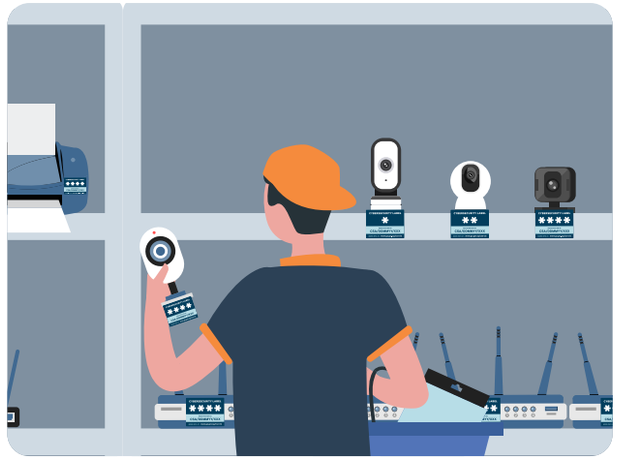
CYBER SECURITY AGENCY OF SINGAPORE

Cyber Security Agency of Singapore (CSA) is the national agency that provides dedicated and centralised oversight of national cybersecurity functions including strategy, international policy, R&D, outreach, system and industry development.

Under the ambit of CSA is the Cybersecurity Certification Centre (CCC) which focuses on the evaluation and certification of cybersecurity products.

The Smart Consumer Device

In recent years, there has been an exponential increase in the number of connected Internet of Things (IoT) devices in the world. It is estimated that 50 billion IoT devices by 2030[2].



What's going on?

In the market, a large number of devices are being sold with poor cybersecurity provisions. Hackers generally look for the easiest systems to attack that will net the most damage and returns.

Information on the amount of security that is built into these devices is not made readily available by the developers. Thus, consumers are unable to make informed decisions towards purchasing more secure devices.

Amidst the growth in number of IoT products in the market, and in view of the short time-to-market and quick obsolescence, many consumer IoT products have been designed to optimise functionality and cost over security. As a result, many of them have little to no security features built-in. This poses cybersecurity risks such as the compromise of consumers' privacy and data. Compromised IoT devices can also be used by threat actors to form a botnet to launch Distributed Denial of Service attacks which could bring down Internet services. One example of this is the Mirai botnet attack in 2016 which were carried out via innocuous IoT devices, such as home routers and IP cameras. The attack left much of the internet inaccessible in the US East Coast.

[2] IoT connected devices worldwide 2030, Statista Research Department, 22 January 2021, https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

Cybersecurity Labelling Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

About CLS

As part of efforts to better secure Singapore's cyberspace, raise cyber hygiene levels ,and increase awareness of consumer IoT security, CSA introduced the Cybersecurity Labelling Scheme (CLS) for network-connected smart devices.

The CLS, which marks a first in the Asia-Pacific region, comprises different levels of cybersecurity ratings to provide an indication of the level of security embedded in the device.

This helps consumers to choose more secured devices and hence, to better protect themselves against basic cyber-attack.

For more information

https://go.gov.sg/csa-cls

CLS: Benefits

For consumers:

- To make security-informed purchase decisions to better safeguard against cybersecurity risks.

For developers:

- To differentiate products with better cybersecurity provisions.

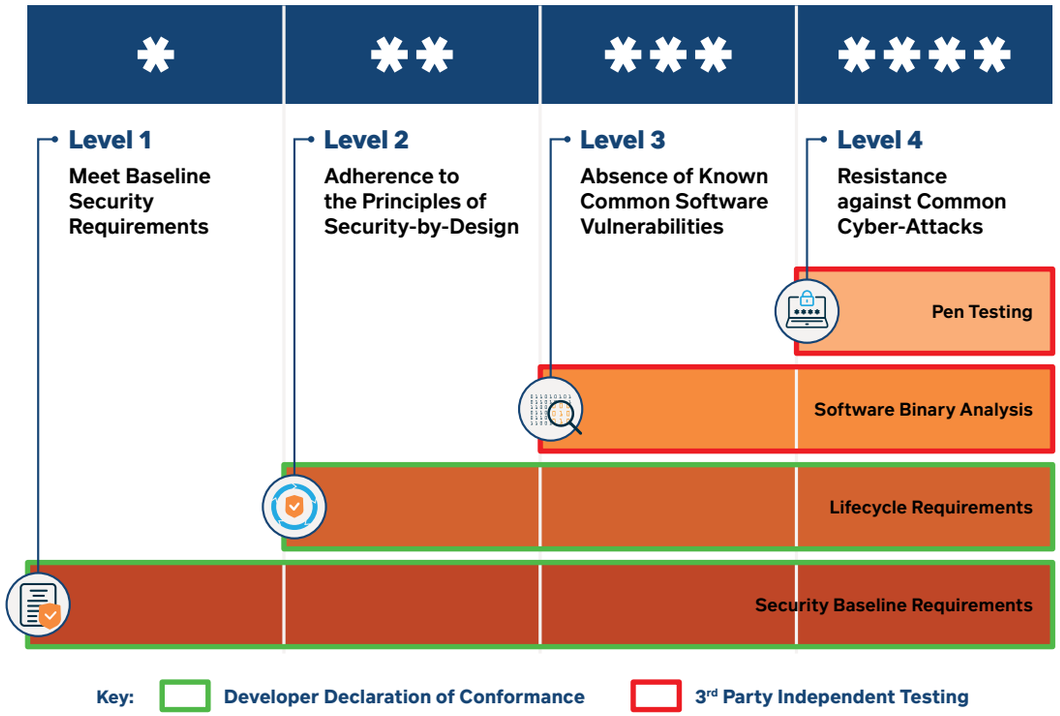
Cybersecurity Label

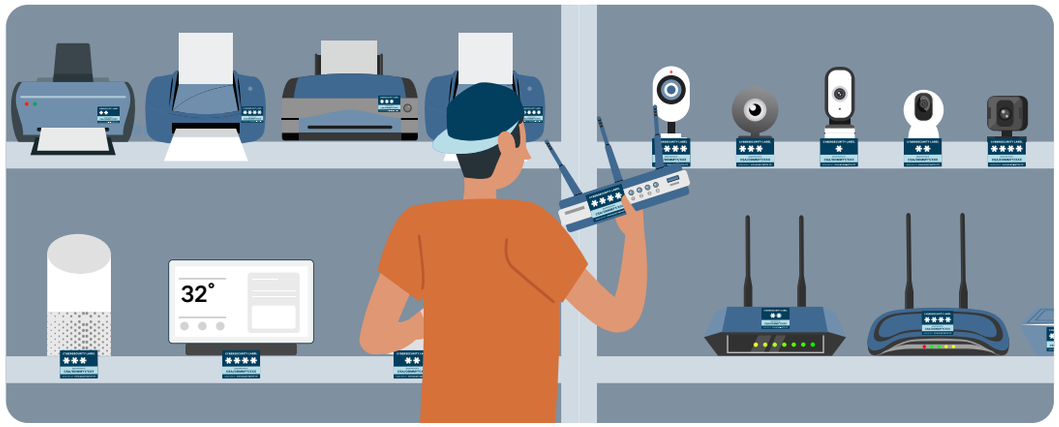
The label will comprise of the product's registration ID which will come in the format:

CSA/Date of Label Expiration in DDMMYY/
Product ID number assigned by CSA

Cybersecurity Levels

The CLS has four progressive rating levels that allows consumers to discern the level of security offered by the product and imbues security consciousness when making purchases.





Level 1:
Meet Baseline Security Requirements

The product meets basic security requirements[3] such as ensuring unique default passwords and providing software updates.

Level 2:
Adherence to the Principles of Security-by-Design

The product has been developed using the principles of Security-by-Design[4] such as conducting threat risk assessment, critical design review and acceptance tests, and fulfilled Level 1 requirements.

Level 3:
Absence of Known Common Software Vulnerabilities

The product has undergone assessment of software binaries by approved third-party test labs, and fulfilled Level 2 requirements.

Level 4:
Resistance against Common Cyber-Attacks

The product has undergone structured penetration tests by approved third-party test labs, and fulfilled Level 3 requirements.

[3] Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI EN 303 645, outlines 14 broad security provisions and seeks to address the most common security problems.

[4] IMDA IoT Cyber Security Guide, March 2020. The guide seeks to provide baseline recommendations and foundational concepts for IoT.

Singapore Common Criteria Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

About SCCS

Common Criteria (CC), also known as ISO/IEC 15408, is a globally recognised technical standard for IT security evaluation. To date, more than 30 nations have signed the Common Criteria Recognition Arrangement (CCRA), whereby CC certificates issued by an authorised nation are mutually recognised across all member nations.

As of January 2019, Singapore is recognised as a CC Certificate Authorising Nation.

Singapore subscribes to the objectives of the CCRA: to improve the availability of IT products evaluated under high and consistent standards, and to eliminate the burden of duplicating evaluations while improving the efficiency and effectiveness of the evaluations.

SCCS: Benefits

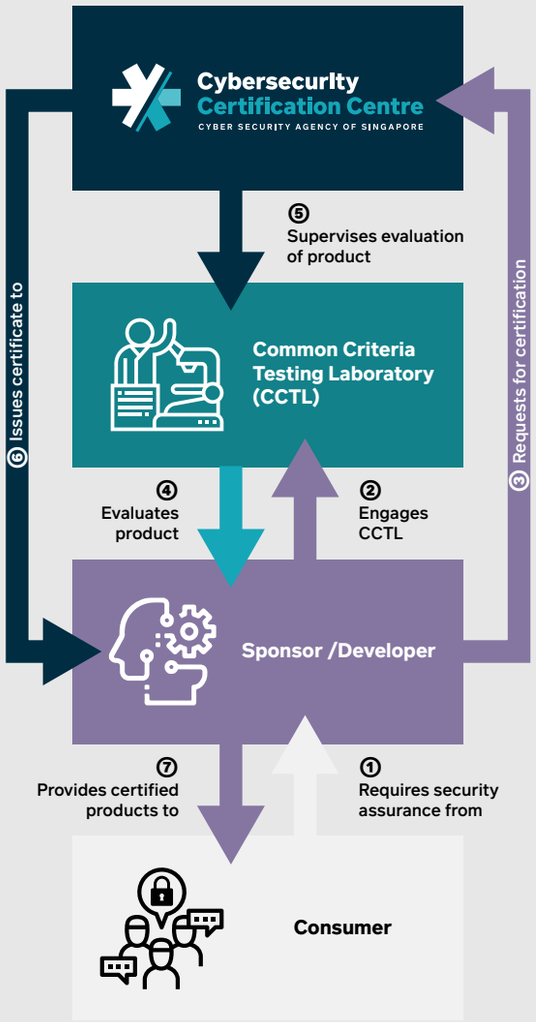
For users:

- Better safeguard their digital assets and services
- Gain assurance that the security evaluation of a product is done consistently, impartially, and according to international standards

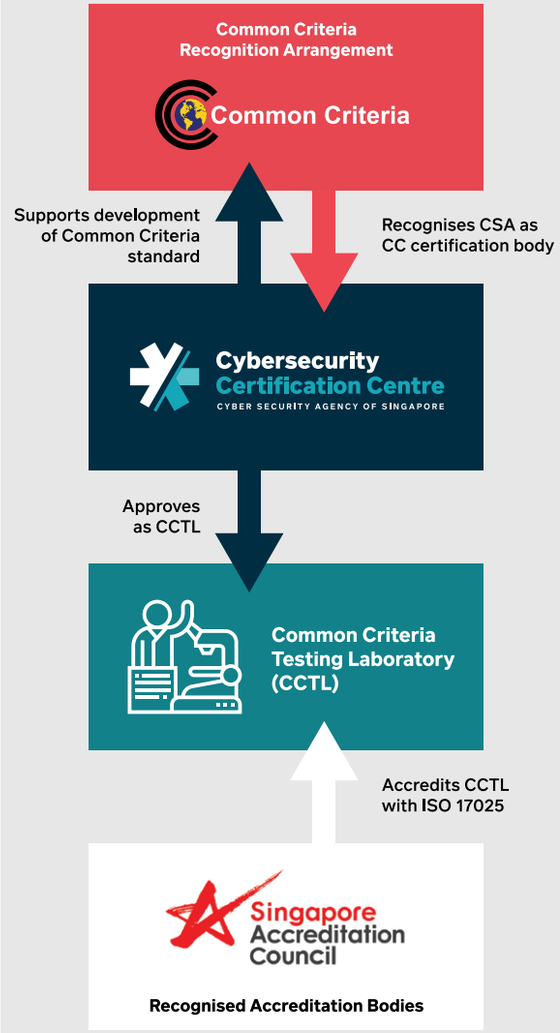
For developers:

- Meet regulatory requirements
- Gain market access without burden of duplicated evaluations
- Develop more secure products and differentiate themselves

Product Security Evaluation & Certification



Accreditation & Recognition



For more information:

Process of Evaluation

① Developers of a product can apply to CSA-CCC to have their product evaluated under SCCS.

② Developers engage a CCTL approved by SCCS to undergo evaluation in accordance to internationally recognised standards.

③ After the evaluation, an assessment will be submitted to CSA-CCC.

④ If successful, CC certificate will be issued which raises the level of trust and assurance in the product.

Scan to find out more information about **SCCS Certified Products**:

Common Criteria Users Forum (CCUF)

The Common Criteria Users Forum (CCUF) was founded in 2012 and is a community based around those using the Common Criteria and ISO/IEC 15408 standards. The Common Criteria Users' Forum mission is to provide a voice and communications channel between the CC community and the CC organisational committees, CC evaluation schemes, and policy makers.

For more information about CCUF:

National IT Evaluation Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

About NITES

The National IT Evaluation Scheme (NITES) was launched in November 2009. Products intended to be used for handling sensitive government data have to be evaluated in accordance with NITES. The most stringent requirements are needed when it comes to safeguarding Singapore's national interests.

Apart from additional national requirement, NITES largely adopts the CC methodology of evaluating the products at high assurance level.

NITES: Benefits

For users:

- Gain assurance that the security measures provided by the product is able to safeguard the highly classified information

For developers:

- Meet the policy requirements for government procurement

Frequently Asked Questions

Cybersecurity Labelling System (CLS)

Is the Cybersecurity Labelling Scheme (CLS) compulsory?

The CLS is launched as a voluntary scheme to allow time for the market and developers to understand how the scheme benefits them. CSA will monitor the response to the scheme and consider when it will be suitable for the labelling scheme to be made mandatory for IoT consumer devices. For more information on the categories of IoT devices which are required to have Cybersecurity Label, please refer to CLS website.

What are the applicable fees for CLS?

CSA may charge a small fee for label registration (refer to CLS fees schedule document on CLS website). The approved test laboratory will set their fees for Software Binary Analysis and Penetration Testing; please contact the laboratory for details.

How long does the process take?

Applications for Tiers 1 and 2 will take up to 5 working days to be processed. Applications for Tiers 3 and 4 will take an estimation of 3 weeks to be processed, due to the involvement of lab tests and assessments.

How long will a Cybersecurity Label be valid for?

The validity of the label is the period during which the developers will support the device with security updates, up to a maximum of a period of 3 years.

How is the Cybersecurity Label used?

Developers can affix the Cybersecurity Label in a conspicuous and unobstructed position on the product packaging. The labels can also be displayed in all advertisements and promotional material of labelled products. This includes, but is not limited to, websites, online stores and printed catalogues.

How do I verify the authenticity of the Cybersecurity Label?

You can check the current list of CLS labelled products in the CLS website. Only products labelled by CSA will be listed. If you come across a product that is not listed on the CSA's website but bears the Cybersecurity Label, please alert us at certification@csa.gov.sg.

Would there be enforcement or revocation of the labels?

When a product is found not to satisfy the requirements declared, CSA will request that the developer undertake rectification measures, or have the label reviewed or removed.

Is it impossible to hack a CLS labelled product?

CLS offers a basic level of security assurance to improve device cybersecurity hygiene by implementing basic safeguards and eradicating common mistakes and vulnerabilities.

CLS labelling does not preclude the device from being hacked given the dynamism of the cybersecurity threat landscape. However, developers applying for CLS are required to have an open vulnerability report and management channel, and for them to update their software in a timely manner.

Users seeking higher security assurance for industrial use (e.g. enterprise, manufacturing, industrial, healthcare usage) are strongly recommended to consider devices certified under formal evaluation and certification schemes such as the Singapore Common Criteria Scheme.

Is the Cybersecurity Label recognised in other nations?

CSA has established arrangements with partners for CLS labelled products to be recognised. For more information on mutual recognition, please refer to CLS website.

CC, NITES, and CLS

Which scheme to choose? CC, NITES, or CLS?

Developers who are keen to obtain an internationally recognised certification to facilitate the exportability of their products should strive for CC certification.

The NITES is a high-assurance national scheme that is recognised only by the Singapore Government.

On the other hand, the CLS is a basic cybersecurity hygiene scheme for consumer smart devices.

Frequently Asked Questions

Common Criteria (CC)

How long do evaluations take?

A typical evaluation takes around 3 to 6 months. The scope of evaluation, complexity of the product, and readiness of the developer may also affect the duration of evaluation. Products evaluated at higher assurance levels will likely take longer with more effort needed.

What can developer do to shorten the duration of an evaluation?

Developers are recommended to adopt the security-by-design approach during the product design phase. A product with well-designed security implementations often takes a shorter period of time for evaluation. Developers who are new to CC could consider engaging an independent CC consultant to support them through the evaluation process. Additional time and cost will be incurred when the developer tries to fit additional security measures into their existing product design during evaluation.

How long will a CC certificate be valid for?

Each CC certificate issued will be valid for 5 years from the date of issue.

What are the applicable fees for CC?

CSA charges a nominal fee (refer to CSA Common Criteria website) for certification services. For evaluation fees, please contact the approved CCTL under SSCS as cost varies based on the scope of evaluation and complexity of product.

If a product is CC certified with the highest Evaluation Assurance Level (EAL), does it mean that it is impossible to hack the product?

A product with a higher EAL is not an assurance of an elevated level of security; instead, it signifies it has undergone more testing. To achieve balance among cost, time, and effort, an evaluation done at a higher EAL is also often for a more targeted scope; while an evaluation done at a lower EAL is likely to be of a broader scope.

Consumers and developers should consider the security requirements and the intended deployment locations to determine which EAL is more appropriate.

Members of the CCRA:

To what levels are the CC certificates mutually recognised?

The Common Criteria Recognition Arrangement mutually recognised certificates based on:

- collaborative Protection Profile (cPP) up to and including EAL4 and ALC_FLR
- Up to EAL2 and ALC_FLR

What are the different Evaluation Assurance Levels (EALs) under Common Criteria?

The EALs provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance.

EAL1 – Functionally tested
EAL2 – Structurally tested
EAL3 – Methodically tested and checked
EAL4 – Methodically designed, tested and reviewed
EAL5 – Semiformally designed and tested
EAL6 – Semiformally verified design and tested
EAL7 – Formally verified design and tested

What is the difference between an authorising nation and consuming nation?

The authorising nation is a compliant Certification Body operating in their own country and under the CCRA, that is able to issue certificates which are mutually recognised. Consuming nation do not operate any compliant Certification Body, nonetheless has expressed interest in the use of certified IT products.

Contact

Cyber Security Agency of Singapore

General Enquries/Feedback:
contact@csa.gov.sg

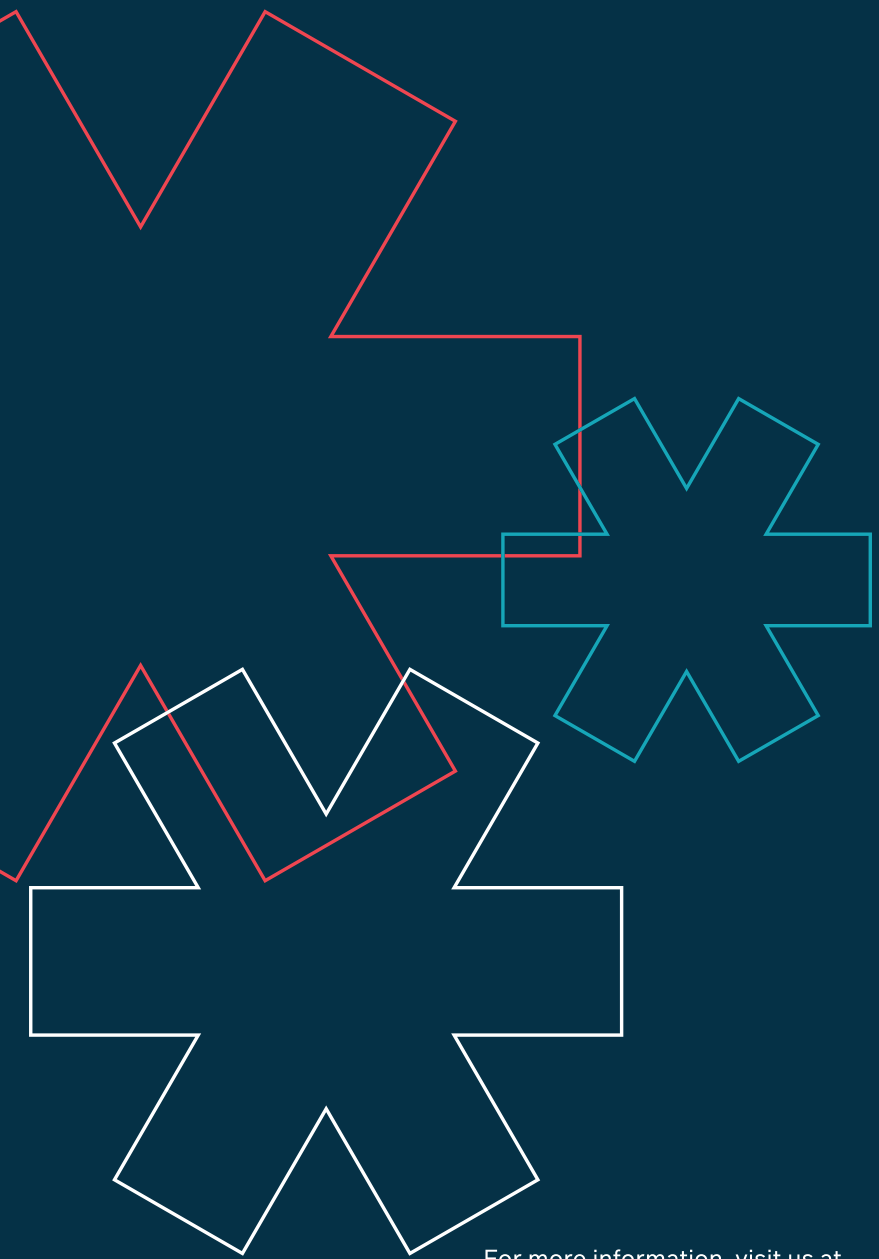
Cybersecurity Certification Centre

Schemes Enquries:
certification@csa.gov.sg

Scan for the latest list of CCTL approved for SCCS:

Scan for the latest list of Third Party Independent Laboratory approved for CLS:

Designed by:
APT811 Design & Innovation Agency



For more information, visit us at

www.csa.gov.sg