Cybersecurity Certification in Brief

Cybersecurity Certification Centre

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.

Cybersecurity Labelling Scheme

About CLS

Cybersecurity Labelling Scheme (CLS) aims to raise cyber hygiene and increase awareness of consumer Internet of Things (IoT) security. The CLS comprises four cybersecurity levels to provide an indication of the progressively higher cybersecurity provisions and assurance in IoT devices.

For consumers:

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

For developers:

- To differentiate products with better cybersecurity provisions.

Singapore Common Criteria Scheme

About SCCS

Common Criteria (CC), also known as ISO/IEC 15408, is a globally recognised technical standard for security evaluation of IT product. Under Common Criteria Recognition Arrangement (CCRA), CC certificates issued in Singapore are mutually recognised amongst more than 30 nations.

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

National IT Evaluation Scheme

About NITES

The National IT Evaluation Scheme (NITES) provides the most stringent requirements needed to safeguard Singapore's national interests. Products intended to be used for handling sensitive government data have to be evaluated in accordance to NITES.

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

CLS Levels

The CLS comprises four cybersecurity levels, corresponding to the number of asterisks on the label which reflects the increasing resistance the product has to basic attacks that they may be commonly subjected to.

Level 1

Meeting Baseline Security Requirements.
The product meets basic security requirements such as ensuring unique default passwords, providing software updates and having a vulnerability disclosure policy.

Level 2

Adherence to International Standards.
The product meets all mandatory security requirements of the international standards[1], and fulfilled Level 1 requirements.

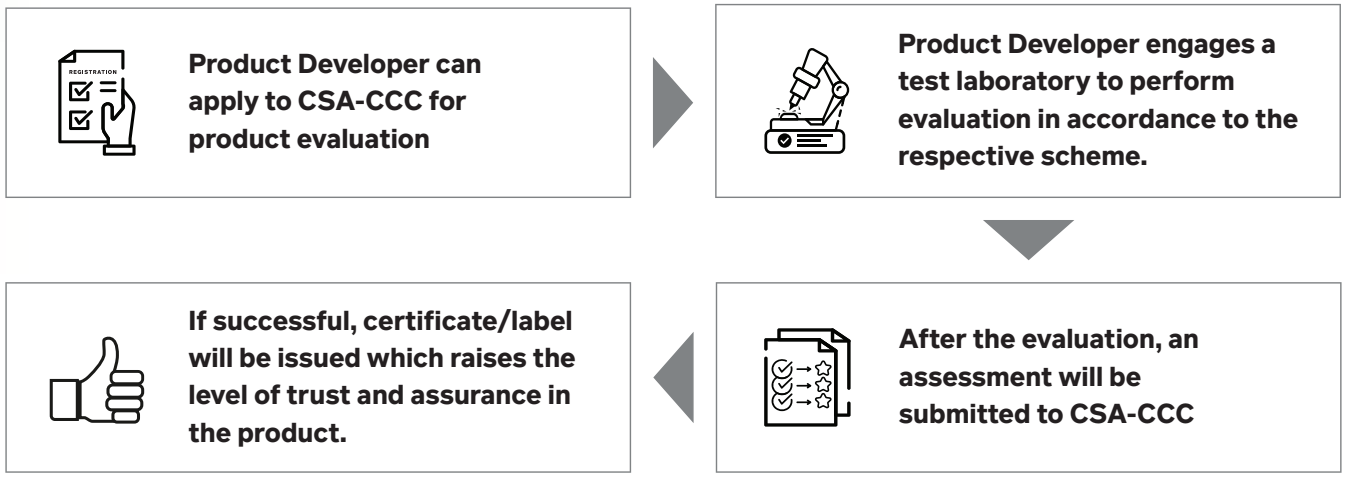
Level 3

Security-by-Design with Absence of Known Common Software Vulnerabilities.
The product has been developed using the principles of Security-by-Design, 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.

Process for CLS[2], SCCS and NITES



[1] Cyber Security for Consumer Internet of Things, ETSI EN 303 645
[2] Applies to CLS Level 3 and 4 only. CLS Level 1 and 2 do not require testing by test laboratories

Cybersecurity Certification Centre

Schemes Enquiries: **certification@csa.gov.sg**

Cyber Security Agency of Singapore

General Enquiries/Feedback: **contact@csa.gov.sg**

For more information, visit us at: **www.csa.gov.sg**

For more information on CLS:

For more information on SCCS: