IoT SECURITY TRUST MARK™ (STM) Certification and Labelling Scheme

DESCRIPTION OF THE SCHEME (DOS)

ISBN 978-0-9953944-2-1 IoT Security Trust Mark™ Description of Scheme (DOS)

Disclaimers

1) Notwithstanding anything contained in this *Scheme Document*:

a) The authors and their organisations disclaim responsibility (including where they, or any of their officers, agents or contractors has been negligent) for any direct or indirect loss, damage, claim or liability any person may incur as a result of any:

i) reliance on or compliance with this *Scheme Document*;

ii) inaccuracy or inappropriateness of this *Scheme Document*; or

iii) inconsistency of this *Scheme Document* with any law; and

b) The authors and their organisations disclaim responsibility (including where they, or any of their officers, agents or contractors has been negligent) for ensuring compliance by any person with this *Scheme Document*.

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

INTRODUCTORY STATEMENT

The purpose of the *Internet of Things Security Trust Mark™ (STM) certification and voluntary labelling scheme (Scheme)* is to provide a common approach to good practice evaluation and certification of IoT vendors product security claims to:

- encourage IoT manufacturers to design their product to meet good practice security
- assist consumers to have confidence in the security of IoT products
- ensure independent assurance is delivered via a scalable, global, sustainable, enduring, standardised and repeatable Scheme framework
- enable value and flexibility, while avoiding duplication

on behalf of the Scheme Senior Executive

https://www.iotsecuritytrustmark.org

1.	**GENERAL**	**5**
1.1	**Introduction**	**5**
1.2	**Scope**	**5**
1.3	**Objectives**	**6**
1.4	**Document Changes**	**6**
1.5	**IoT Security *Trust Mark™ Scheme* review**	**6**
2.	**ACRONYMS, DEFINITIONS AND INTERPRETATIONS**	**7**
2.1	**GLOSSARY AND TERMINOLOGY**	**7**
2.2	**STM ABBREVIATIONS**	**11**
3	**OVERVIEW OF THE SCHEME**	**13**
3.1	**Introduction**	**13**
3.2	**Document Control**	**14**
3.3	**STM Claims Testing**	**14**
3.4	**STM Award**	**15**
3.5	**The Scheme**	**16**
3.6	**STM Claims Testing Overview**	**17**
3.7	**Publications and Publicity**	**18**
3.8	**STM Maintenance**	**18**
4	**ORGANISATION AND MANAGEMENT**	**19**
4.1	**Introduction**	**19**
4.2	**Host Country Association (HCA)**	**19**
4.3	**Decision Authority (DA)**	**19**
4.4	**Scheme Secretariat (SS)**	**20**
4.5	**Accredited Test Facility (ATF)**	**20**
4.6	**Vendor**	**20**
4.7	**IoT Owner/User**	**21**
4.8	**Disputes and Complaints Procedure**	**21**
	APPENDIX A	**23**
	REFERENCES	**24**

1. GENERAL

1.1 Introduction

1.1.1 The development of this *Scheme* has been prompted by significant, and realised concerns, about the security of Internet of Things (IoT) connected devices. Relevant stakeholders comprise representatives from the IoT, technology and communications industries, government, vendors/manufacturers, privacy, safety and user/consumer groups.

1.1.2 The *Scheme Document* should be read in the context of other relevant codes, guidelines, standards and documents.

1.1.3 The *Scheme Document* should be read in conjunction with related domestic and international guidance, codes, standards and legislation, including:

(a) FVEY Guidance: Statement of Intent regarding the security of the Internet of Things;
(b) ETSI EN 303 645 Cyber Security for Consumer IoT: Baseline Requirements;
(c) ENISA ISBN 978-92-9204-236-3 Baseline Security Recommendations for IoT;
(d) NIST NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers;
(e) UK DCMS Code of Practice for Consumer IoT Security; and
(f) Australia DoHA Code of Practice Security the IoT for Consumers.

1.1.4 Compliance with this *Scheme* does not guarantee compliance with any legislation. The *Scheme Document* is not a substitute for legal advice.

1.2 Scope

1.2.1 The IoT Security *Trust Mark™ (STM)* certification and voluntary labelling scheme covers the evaluation of IoT vendors product security claims, including:

(a) data generated by IoT products;
(b) data carried to and from IoT products;
(c) data stored in IoT products;
(d) consumers using IoT products; and
(e) actuators driven by IoT systems.

1.2.2 The *STM* deals with IoT products associated with, but not limited to:

(a) home use by consumers;
(b) business use in the office environment;
(c) industry use in operational systems;
(d) government;
(e) critical infrastructure; and
(f) organisations of significant national interest.

1.2.3 This *STM* document provides specific interpretation of standard security controls in the IoT context and encourages security, safety and privacy in the design and development process. Specifically, it deals with;

(a) evaluation of the claims related to secure use and storage of information obtained through IoT products; and
(b) evaluation of the claims related to integrity of the operating system and application in the product.

1.3 Objectives

1.3.1 The objectives of the *STM* are to:

(a) encourage IoT product manufacturers to develop secure IoT products;
(b) enable IoT Owners/Users to have confidence in the security features claimed in an IoT product; and
(c) provide IoT product evaluators with a framework for predictable, standardised and repeatable testing of products.

1.3.2 The *STM* brings together sources of information relating to the security, privacy, and resilience of IoT to assist the IoT industry in delivering quality products. It does not endorse any specific technology or approach for use, nor warrant any product as inherently "secure".

1.4 Document Changes

1.4.1 All the *Reference Guideline* documents (including this *Scheme Document*) will be subject to review and amendment. Changes to the *Reference Guidelines* will be published on the Scheme website and those participating in the Scheme will be notified at least twenty (20) working days before substantive or material changes in the documents take effect.

1.5 IoT Security *Trust Mark™ Scheme* review

1.5.1 The STM scheme is a living program. The Reference Guidelines have been produced in a form that can be further reviewed and updated over time, and approved by the Scheme Senior Executive, as significant developments and potential risks make changes and additions to the STM Scheme necessary.

2. ACRONYMS, DEFINITIONS AND INTERPRETATIONS

2.1 GLOSSARY AND TERMINOLOGY

The following terms have special meanings within the context of the Scheme.

Accredited Test Facility (ATF)

An organisation accredited by a Scheme Decision Authority (DA) in accordance with the Accredited Test Facility Guidelines (ATFG) and the Generic Claims Test Method (see ATFG) and appointed under the Scheme to work with vendors to develop their Vendor Claims Document (VCD), undertake Claims Tests and issue Test Report (TR), Test Report Summary (TRS), Supplementary Test Report (STR) and Letter of Recommendation (LoR) under the Scheme. A Scheme ATF must be accredited and maintain their accreditation as a testing laboratory against ISO/IEC 17025. The Scheme Senior Executive and Scheme Operator may also appoint interim ATF (iATF), provisional ATF (pATF) or Specialist ATF (SATF) *[collective xATF]*.

Application

The formal request submitted by the Vendor to the Scheme for the IoT Product specified in the Vendor Claims Document (VCD) to be registered with the Scheme. This includes new and STM maintenance applications.

Approved VCD

The version of the Vendor Claims Document (VCD) submitted and approved by a Scheme DA.

Baseline Requirements (BR)

The minimum set of security claim types that must be present in each VCD. These follow, and are compiled from, international good practice IoT security guidelines, recommendations, codes of practice, ISO/IEC standards and regulations. Such as those released by ETSI (EN 303 645), ENISA (Baseline Security Recommendations for IoT), NIST (NISTIR 8259) and the UK & Australian Governments (IoT Security Codes of Practice).

Basic Checks

A series of quality checks to be undertaken by xATFs on VCDs, Test Reports, before submission to the Scheme Decision Authority (DA). Basic checks are documented in the Accredited Test Facility Guideline (ATFG).

Certificate Award

The issue of a formal statement by the Scheme confirming the Vendor's security claims for an IoT Product have been tested by an Accredited Test Facility (ATF) and validated against the VCD, and legitimate use of the STM Label (STM QR Code) on the specific version of the IoT Product evaluated. Products are listed on the STM Evaluated Products List (STM-EPL).

Claims Class (CC)

A Claims Class may be an externally defined, (i.e. by a recognised third-party CDP), public sector requirement for a standard set of IoT functionality or a standard level of service provision for a specified type of IoT Product, these can be pre-approved by a DA for reference in the VCD.

Claims Test

The process carried out by an ATF (or in some cases, an iATF, pATF or SATF *[xATF]*) under the STM Scheme for the independent testing of the security claims of IoT Product stated in the VCD.

Claims Test Method

The test methodology used by the xATF for claims testing under the STM Scheme which must comply with the ATFG.

Cybersecurity Design Pattern (CDP)

The DA may from time to time issue a Cybersecurity Design Pattern (CDP) which provides a predefined set of security claims for a specific category of IoT product which are recognised by the industry. For example, a CDP may be created for SmartTVs or Smart Water Meters to ensure consistency in the baseline security claims expected from all vendors in this category and/or to meet minimum mandated regulatory requirements. CDPs are proactively distributed to Specialist ATFs (SATF) conducting testing of devices in that category, ensuring consistency and comparability across testing of like products. Testing facilities may apply to become a SATF in one, or more, of these specific categories.

Decision Authority (DA)

A technical organisation(s) appointed by the Scheme Operator and approved by the Scheme Senior Executive to independently oversee, audit and accredit Test Laboratories, review VCDs, review xATF Test Reports (TR), review Test Report Summaries (TRS), Supplementary Test Reports (STR) and Letters of Recommendation (LoR) to decide, and Award the STM certificate and voluntary label (STM QR Code).

To ensure currency of certification for products on the STM Evaluated Products List (EPL), the DA also engages in regular monitoring of known/disclosed security vulnerabilities. Notification is given to xATFs and/or vendors when this activity identifies a security issue requiring remediation. While remediation is in process the certification is suspended. This satisfies conformance with the assessment tenet of maintaining surveillance.

DA Review

The process undertaken by the DA in assessing VCDs, xATF TR, TRS, STR and LoR and in deciding whether to Award the STM certificate and label. The results of the assessment are recorded in a DA Review Form (DARF).

Host Country Association (HCA)

An Association or Organisation that may be appointed by the Scheme Senior Executive in a given region (jurisdiction/country/geography) who seek to drive the adoption of safe and secure IoT in their region; and includes the region Scheme Secretariat (SS) function, providing administration, promotion, marketing and Scheme awareness raising through engagement with Government, Industry and Consumers.

Information Assurance (IA)

The confidence that information systems will protect the information they handle, and will function as they need to, when they need to, under the control of legitimate users/consumers.

IoT Owner/User

A person or organisation who purchases, operates or uses an IoT device either directly themselves or on behalf of another user. This includes individual people, small and large organisations, and government.

IoT Product

A "test target"/Product Under Evaluation (PUE) that is the subject of a STM Security Claims evaluation comprising of software, firmware, hardware, service and its associated administration, user/consumer guidance documentation and marketing material supplied by the Vendor and covered by the VCD. An IoT product is tested by methodically analysing the physical product in accordance with the test method described by an xATF in the VCD.

IoT Service

A service supplied to a consumer or business by a vendor that utilises IoT devices but where neither the consumer or the vendor is the owner or operator of those devices (thus, only a service is supplied). An IoT Service is also the subject of a STM Security Claims evaluation comprising software, firmware, hardware, service and its associated administration, user/consumer guidance documentation and marketing material supplied by the vendor and covered by the VCD. Unlike an IoT Product, an IoT Service is tested by interviewing customers or distributors of the IoT Service, as there is no physical device to be tested.

ISO/IEC 17025

The standards set out in the document entitled "ISO/IEC Guide 17025: General requirements for the Competence of Testing and Calibration Laboratories" *[ISO 17025]*.

Letter of Recommendation (LoR)

A document produced by a STM xATF that is submitted to the DA which details any additional Claims Test findings or issues raised in the Test Report of the Product Under Evaluation (PUE) and makes a recommendation for pass or fail, which will be used by the DA to inform and assess whether the STM can be awarded.

Marketing Claims Statement

A short (no more than 400 words) statement that summarises the security claims of the IoT Product or IoT Service to which the STM will apply. The Marketing Claims Statement is submitted with the VCD for either a New Application (NA) or a Review Application (RA).

Quality Management (QMS)

The ATF must maintain an effective, and auditable, QMS such as ISO9001. Refer §4.2.1 of ATFG.

Scheme

The IoT Security Trust Mark™ (STM) certification and voluntary labelling scheme that is described in this *Scheme Document* and the Reference Guidelines.

Scheme Documents

The full suite of documents describing the Scheme property, comprising:

Description of Scheme (DOS) ISBN 978-0-9953944-2-1
Vendor Guideline (VG) ISBN 978-0-9953944-9-0
Accredited Test Facility Guideline (ATFG) ISBN 978-0-9953944-8-3
Decision Authority Guideline (DAG) ISBN 978-0-9953944-7-6

Scheme Senior Executive

Representative(s) appointed by the organisation that own the IoT Security Trust Mark™ certification and voluntary labelling scheme, who sets the objectives, policy, governance and standards for the operation of the Scheme, and who licence and appoints those to operate and administer the Scheme. The Scheme Senior Executive oversees contracts and the maintenance of Scheme Documents.

Scheme Secretariat (SS)

A subsidiary of, or appointed under licence by, an HCA. The Scheme Secretariat is the organisation responsible for supporting the day-to-day activity of the Scheme, and those involved in the Scheme, within the HCAs region.

Specialist Testing (ST)

Several technologies require specialised testing methods and equipment. ATFs and Test Laboratories can apply for, and be accredited to, undertake Specialist Testing, as a SATF. Refer §3.4 of ATFG.

Specialist Accredited Test Facility (SATF)

A Test Laboratory, or ATF, that has undergone accreditation in a specialist area in order to conduct Specialist Testing (ST). Refer Appendix D for a list of specialist test areas.

STM Evaluated Products List (STM-EPL)

Evaluated Products are listed in the IoT Security Trust Mark™ Evaluated Products List (STM-EPL), along with their Summary Test Report (STR). *Access to the STM-EPL is via the Scheme website.* Products successfully passing certification can voluntarily display the IoT Security Trust Mark™ label (STM QR Code), issued by the DA, on their product packaging and/or marketing material for the duration of their active certification. These link to their product on the official IoT STM-EPL enabling IoT consumers to quickly check and confirm currency of certification at any point in time *(using the IoT STM "traffic light system" of; certified (green), suspended (amber) or expired (red))*.

Supplementary Test Report (STR)

From time to time the DA may seek clarification, qualification, or additional test execution and assurances that must be demonstrably addressed by either the xATF or vendor, this may be via written response or a formal Supplementary Test Report (STR). Refer §5.7 of DAG.

Test Approach (TA)

The methodology documented by the xATF in the VCD that is used to evaluate the vendors product security claims and validate compliance with the Baseline Requirements (BR). Note that the TA proposed by the xATF may be different for each type of Product Under Evaluation (PUE). This satisfies conformance with the assessment tenet of detailing determination.

Test Laboratory

An entity who conducts testing of technology products and services that is not Accredited by the Scheme and is therefore nor permitted to conduct Claims Testing for the Scheme. Test Laboratories may apply for either Full, interim or provisional Accreditation in accordance with the procedures of §5 of the ATFG. They may also apply for SATF Accreditation.

Test Officer (TO)

A suitably qualified and experienced tester who is employed by an xATF and authorised by them to responsibly execute the test approach submitted in the VCD, to the standard of their xATF and the Scheme, and clearly document the results in the TR.

Test Report (TR)

A report produced by an xATF and submitted to the DA detailing the findings of the Claims Tests for the "Test Target"/Product Under Evaluation (PUE), which will be used by the DA in conjunction with the Letter of Recommendation (LoR) to assess whether the STM should be awarded. This satisfies conformance with the assessment tenet of providing attestation.

Test Report Summary (TRS)

The summary of the main findings from the Test Report written by the xATF and submitted by the Test Laboratory to the DA along with a TR and LoR. This Test Report Summary, *if approved by the Scheme*, is published on the Scheme website, following the award of the STM certificate and voluntary label (STM QR Code).

Vendor

A person or organisation that owns and develops an IoT Product or IoT Service.

Vendor Claims Document (VCD)

The document which identifies the security functionality claims of the vendor to be tested and the Test Approach (TA) methodology of the xATF for the defined IoT Product to meet the IoT Security Baseline Requirements (BR). This satisfies conformance with the assessment tenet of describing requirement.

2.2 STM ABBREVIATIONS

ATF	Accredited Test Facility
ATFG	Accredited Test Facility Guideline
BC	Basic Checks
BGT	Brand Guidelines for ATFs
BGV	Brand Guidelines for Vendors
BR	Baseline Requirements
CDP	Cybersecurity Design Pattern
CP	Certification Period
DA	Decision Authority
DAG	Decision Authority Guideline
DARF	Decision Authority Review Form
DOS	Description of the Scheme
ENISA	European Network and Information Security Agency
EPL	IoT Security Trust Mark™ Evaluated Products List
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard (FIPS PUB 140-2)
HCA	Host Country Association
IA	Information Assurance
iATF	Interim Accredited Test Facility
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
LoR	Letter of Recommendation
NA	New Application
NIST	National Institute for Standards and Technology
pATF	Provisional Accredited Test Facility
PUE	Product Under Evaluation
QMS	Quality Management System
QM	Quality Manual
QP	Quality Procedures
RA	Review Application
SATF	Specialist Accredited Test Facility
Scheme	IoT Security Trust Mark™ (STM) certification and voluntary labelling scheme
SS	Scheme Secretariat
ST	Specialist Testing
STM	IoT Security Trust Mark™ (STM) certification and voluntary labelling scheme
STM-EPL	IoT Security Trust Mark™ Evaluated Products List
STM Label	IoT Security Trust Mark™ Label (aka STM QR Code)

STM QR Code	IoT Security Trust Mark™ Quick Response Code (aka STM Label)
STR	Supplementary Test Report
TA	Test Approach *(Methodology)*
TO	Test Officer
TR	Test Report
TRS	Test Report Summary
VCD	Vendor Claims Document
VG	Vendor Guideline
xATF	[x]*variable* = interim, provisional, Specialist; or fully; Accredited Test Facility

3 OVERVIEW OF THE SCHEME

3.1 Introduction

3.1.1 The IoT Security Trust Mark™ (STM) Scheme (referred to as the "Scheme" or "STM" in this document) was established in 2019 to test the validity of vendors' claims of security functionality in Internet of Things (IoT) Products and IoT Services, in which Information Assurance (IA) is a major consideration.

3.1.2 In the context of this Scheme, IoT security means the protection of information and information systems from a wide range of threats in order to ensure continuity, minimise damage; and support safety & privacy principles. IoT security is categorised as the preservation of:

a. **Confidentiality** - The property that information is not made available or disclosed to unauthorised individuals, entities, or processes;
b. **Integrity** - The property of safeguarding the accuracy and completeness of assets;
c. **Availability** - The property of being accessible and usable upon demand by an authorised entity;
d. **Safety** – The property of being able to be used without harm to a person or persons;
e. **Resilience** – The property of not being able to sustain continuous operation even when under attack.

Any or all of these aspects may be of importance in a particular case.

The **Baseline Requirements** (BR) of the Scheme are structured around these attributes to articulate the minimum set of capabilities that will **preserve** each of the attributes

The scheme is compliant with the premise of the conceptual framework for a conformity assessment program set out by the National Institute of Standards and Technology (NIST SP 2000-1/-2) and covers the principal tenets of;

REQUIREMENT – How should it perform?
DETERMINATION – How do we know it performs?
ATTESTATION – Who says its performance has been demonstrated?
SURVEILLANCE – What about assurances next week?

3.1.3 Information Assurance (IA) means the confidence that information systems will protect the information they handle, and will function as they need to, when they need to, under the control of legitimate users/consumers.

3.1.4 The objective of the Scheme is to meet the needs of Government and Industry for cost effective and efficient functionality claims testing of the security of IoT Products and IoT Services. The STM requires IoT Products and IoT Services to meet good practice Baseline IA Requirements, as defined by organisations such as ETSI, ENISA, NIST and global government departments, agencies and regulators, thereby ensuring suitability for purchase by central government and the wider public sector, particularly in the areas of transport, health, agricultural, industrial systems (IIoT), smart cities and consumer smart devices.

3.1.5 The Scheme may be represented by a Host Country Association (HCA) in each geography who provides a Scheme Secretariat (SS) to provide administrative support for the Scheme locally in that country or region. STM certification will be awarded to IoT Products that meet the terms and conditions of the Scheme. Those products will then be able to voluntarily display the STM label (STM QR Code) which links to their product on the STM Evaluated Products List (STM-EPL), located on the Scheme website. The STM-EPL operates the "STM traffic light system" which shows green,

amber and red, representing a products current certification status, being certified, suspended or expired respectively.

3.1.6 This document "IoT STM Description of the Scheme" (DOS) ISBN 978-0-9953944-2-1 describes the Scheme and the procedures applied under it. It is intended for use by those participating in the Scheme as well as potential IoT Owners/Users who are involved with the evaluation, procurement, purchasing and use of IoT Products in which IA is a consideration.

3.1.7 For details of the process and objectives, applied by the STM Scheme Decision Authority (DA) in assessing Vendor Claims Documents (VCDs) and Test Reports, and in deciding whether to Award the STM certification to IoT Products see the "IoT STM Decision Authority Guideline" (DAG) ISBN 978-0-9953944-7-6.

3.1.8 For details of the Assessment Criteria Trial Test applied by the DA, to accredit a Test Facility, see Appendix A of the "IoT STM Scheme Accredited Test Facility Guideline" (ATFG) ISBN 978-0-9953944-8-3 and Appendix A of the "IoT STM Decision Authority Guideline" (DAG).

3.1.9 For details about Vendors' responsibilities and admission to the Scheme, see the "IoT STM Scheme Vendor Guideline" (VG) ISBN 978-0-9953944-9-0.

3.1.10 For details about Test Laboratory responsibilities and participation in the Scheme, see the "IoT STM Scheme Accredited Test Facility Guideline" (ATFG).

3.2 Document Control

3.2.1 All the Scheme documents will be subject to review and amendment. Changes to the Scheme documents will be published and those participating in the Scheme will be notified at least twenty (20) working days before materially substantive changes in the documents take effect.

3.3 STM Claims Testing

3.3.1 STM Claims Testing is the independent testing of vendors' security claims of their IoT Product(s) by a Test Laboratory accredited by the Scheme Decision Authority (DA) as an Accredited Test Facility (ATF) and the STM label (STM QR Code) provides IoT Owners/Users of IoT Products or IoT Services with confidence that the Vendor's security functionality claims of the IoT Products and IoT Services have been independently validated and they meet the IoT Security Baseline Requirements (BR).

3.3.2 The IoT Product or IoT Service will be tested against the Vendor Claims Document (VCD), which demonstrates the security requirement specifying the security functionality claims, versions and platforms of the IoT Product or IoT Service and period of assessment for the Product Under Evaluation (PUE).

3.3.3 Where applicable, the Vendor Claims Document (VCD) should provide a mapping of individual claims to controls specified in the NIST Cybersecurity Framework. Where the claims conform to a Cybersecurity Design Pattern (CDP), this should be specified.

3.3.4 More detailed guidance on the process for registering a STM application, testing and approval under the Scheme is provided in the Reference Guidelines.

3.4 STM Award

3.4.1 The Scheme provides the independent review of Claims Test results, and thereby ensures impartiality of results across all Claims Tests under the Scheme.

3.4.2 The Award of the STM confirms that:

a. The determination that an IoT Product or IoT Service has been Security Claims Tested and the test results confirm that the security functionality claims in the VCD are valid;
b. The testing has been conducted in accordance with the requirements and integrity of the Scheme and an independent Accredited Test Facility (ATF) is willing to provide that attestation.

3.4.3 The Award of the STM does not endorse an IoT Product or IoT Service in any other respects. Moreover, it is not a guarantee that other claims made by the Vendor outside the VCD are valid, or a guarantee of inherent security.

The vendor may voluntarily display the IoT STM label (STM QR Code) in material relating to their certified product.

Fig 1. Sample STM QR Code label

This label links directly to the product listing on the STM Evaluated Product List (STM-EPL) and enables consumers to quickly ascertain the currency of the certification according to the "STM traffic light system" which shows green, amber and red, representing a products current certification status, being certified (green), suspended (amber) or expired (red).

3.4.4 The Award of the STM applies to a specific version and the product(s) specified in the VCD. The STM for an IoT Product or IoT Service is valid for a maximum of two (2) years from the date of the Award. This is known as the Certification Period (CP). All IoT Products and IoT Services must undergo a review at the 12-month anniversary of the Award via the submission of a Review Application (RA).

3.4.5 Should the version or name of the IoT Product or IoT Service change at all within the CP, the Award for an IoT Service can be maintained for a further 12 months provided the product goes through, and passes, an STM review (via the submission of a RA), ensuring that standards and security claims have been maintained.

3.4.6 The Award of the STM applies to the specific claims indicated in the VCD and tested for within the Scheme. Marketing statements which will be used should the IoT Product or IoT Service be awarded the STM should therefore be included in the VCD. Marketing materials for the IoT Product or IoT Service must also be submitted within the Application to the Scheme to ensure continuity between the claims, tests and STM labelling and marketing.

The Decision Authority (DA) undertakes surveillance by regularly reviewing relevant publicly known vulnerabilities to ensure certified products listed on the Evaluated Product List (EPL) have no known released vulnerabilities. Should a vulnerability be released then the product certification will be moved to a suspended (amber) state and the vendor will be contacted to ensure awareness and remediation, once remediated the product will be moved back to a certified state (green). Should a vendor fail to remediate within the nominated period then the certification will be revoked and moved to an expired (red) state on the STM EPL.

3.5 The Scheme

3.5.1 The Scheme provides an organisational and procedural framework for the conduct of independent Claims Testing. The Scheme framework includes:

a. registration of ATFs (interim (iATF), provisional (pATF) and Specialist ATFs (SATF*[xATFs]*) approved to undertake Claims Testing under the Scheme;

b. establishing procedures to enable Vendors to validate the security claims of their IoT Products and IoT Services through independent testing of those claims.

3.5.2 The Scheme establishes one, or more, Decision Authorities (DAs) to accredit test facilities and approve the Award of the STM. The Scheme may appoint Host Country Associations (HCAs) to establish a local Scheme Secretariat (SS) to work alongside the DA; notionally one HCA and SS for each region (jurisdiction or country). The DA will review all VCDs, Test Reports (TR), Test Report Summaries (TRS) and Letters of Recommendation (LoR) within its geographical remit and conduct routine surveillance activities on evaluated products.

3.5.3 Each DA has overall responsibility for:

a. determining whether the STM Application, including the VCD, submitted by the Vendor for the IoT Product or IoT Service meets the terms and conditions of the Scheme, and can therefore be accepted into the Scheme;

b. approving the Award of the STM to the IoT Product or IoT Service as appropriate, including the review of the TR, TRS and LoR submitted by the xATF.

3.5.4 Test Laboratories are required to be accredited by the DA to undertake Claims Testing under the Scheme as ATFs.

3.5.5 The scope of the Test Laboratory accreditation under the Scheme is limited to facilities that reflect the following principles:

a. Impartiality - testing is demonstrably free from bias (neither the xATF, nor any individual member of the xATF team has a commercial or financial interest in the outcome of the testing);

b. Objectivity - test results are obtained from the evidence provided, with the minimum of subjective judgement or opinion.

3.5.6 An xATF shall not test the IoT Product or IoT Service of any group or division of the parent company to which it belongs.

3.5.7 ATFs and SATFs are required to be re-accredited every three (3) years Refer ATFG, §5.7.7)

3.6 STM Claims Testing Overview

3.6.1 The IoT Security Trust Mark (STM) is a quality label with determination assured by independent testing. IoT Owners/Users purchasing IoT Products or IoT Services that have been awarded the STM, and voluntarily displaying the label of the scheme, can be confident that security claims have been independently attested. All IoT Products and IoT Services also undergo evaluation against the minimum IoT Security Baseline Requirement (referred to in §3.6.3 below) in order to successfully attain the STM.

3.6.2 Claims testing under the Scheme must be performed by testing facilities accredited by the Scheme (xATFs or SATFs). The Vendor is responsible for agreeing a contract with an xATF to assist with the preparation of the Vendor Claims Document (VCD) and to undertake Claims Tests against the VCD once accepted under the Scheme.

3.6.3 The Vendor is responsible for preparing the VCD but is required to first contract an xATF to assist with the compilation of the VCD, contributing especially to covering the Baseline Requirements, the test approach and proposed test methodology by the xATF documented in that VCD. The xATF is also required to undertake a series of quality Basic Checks on the format and content of the VCD, ensuring the Product Under Evaluation (PUE) covers the Scheme's Baseline Requirements (BR) and any applicable Cybersecurity Design Patterns (CDPs), before it can be submitted for review by the Decision Authority (DA).

3.6.4 It should be noted that some large software or complex products, such as operating systems, may be unsuitable for testing under the Scheme.

3.6.5 IoT Products and IoT Services are tested against the VCD which has been accepted under the Scheme. All claims in the version of the VCD accepted under the Scheme must be tested. Where an xATF is not accredited to undertake Specialist Testing, the xATF is required to sub-contract the Specialist Testing to a Specialist Accredited Test Facility (SATF).

3.6.6 Review of the VCD by the DA should take no more than five (5) working days following satisfactory submission of the VCD by the Vendor, unless the Vendor is notified that the DA requires additional time to consider the Application.

3.6.7 Testing should only commence after the DA has confirmed to the Vendor and xATF that the VCD has been formally approved by the Scheme to be used in their Claims Tests.

3.6.8 Any DA required changes to the VCD that impact the Claims Tests must be addressed by the Vendor and the updated VCD resubmitted to the DA for approval prior to commencement of the Claims Tests. Access to the updated VCD will also facilitate any DA advice that may be required during the subsequent Claims Tests.

3.6.9 The Claims Test by the xATF (or SATF as appropriate) should not exceed twenty-five (25) days effort and should be completed within eight (8) weeks of the start of testing. Some flexibility in these targets is acceptable, in the case of more complex products or for concurrent testing of product families or multiple platforms, but the Vendor will seek the prior agreement from the SS to this. The DA is entitled to monitor case level experience of xATFs in respect of time and cost.

3.6.10 The Vendor is required to provide the xATF with technical documentation and/or a technical briefing, and access to the Technical Manager as required. This will assist the xATF in defining the Test Approach and setting up the test environment.

3.6.11 The xATF should document the results of the Claims Tests in a TR according to the format and procedure described in the ATFG. The xATF is responsible for ensuring that the TR conforms to the correct format and meets the DA requirements for reporting test results.

3.6.12 The final version of the STM TR, TRS and LoR should be submitted to the DA for review who will decide on the STM Award. The TRS will be published in the STM Evaluated Product List (STM-EPL), to confirm the Award of the STM.

3.6.13 The VCD, TR and TRS remain the property of the Vendor who submitted the Application to the Scheme. The Vendor will grant a non-exclusive license to copy, use, publish and distribute the TRS in accordance with the requirements of the Scheme. This includes publication of the TRS for the IoT Product or IoT Service which is awarded the STM and added to the STM-EPL.

3.7 Publications and Publicity

3.7.1 This document (DOS) is part of the Reference Guidelines. Other documents in the Reference Guidelines include the Vendor Guideline (VG), Accredited Test Facility Guideline (ATFG) and Decision Authority Guideline (DAG), which are available upon completion of the Scheme Mutual Non-Disclosure Agreement (STM MNDA) and by request via the Scheme website – www.iotsecuritytrustmark.org

3.7.2 All press releases and similar statements referring to the Scheme may be made provided agreement is first obtained from a DA, or SS. A DA, or SS, is responsible for approving press releases and similar statements relating to the Scheme.

3.7.3 References to the STM in publications, advertising and documentation must only refer to the IoT Product or IoT Service for which the STM has been awarded, and the exact version, platforms and specific claims tested in the VCD and TRS for which the STM has been awarded. The use of the STM publications, advertising and documentation must also conform to the STM branding guidelines available from the Scheme website.

3.7.4 No reference should be made to the status of the application registered with the Scheme for the IoT Product or IoT Service, except for IoT Products or IoT Services where the Award of the STM is still valid.

3.8 STM Maintenance

3.8.1 STM Maintenance arrangements only apply:

a. where there has been a change of product name or ownership, but no change in the IoT Product or IoT Service awarded the STM.
b. for IoT Products or IoT Services where the STM can be extended for a second-year subject to confirmation that service levels have been maintained.

3.8.2 The STM award for an IoT Product or IoT Service is valid for a maximum of two (2) years from the date of the Award and all IoT Products and IoT Services have to undergo a Review Application (RA) 12-months after being Awarded the STM. All IoT Products and IoT Services have to undergo a New Application (NA) process at the end of the two-year period.

3.8.3 To maintain the STM for IoT Products or IoT Services, upon receipt of a RA the xATF will interview or issue questionnaires to Vendor's customers (or in the case of consumer mass-market products, local distributors/retailers), and/or potentially re-test claims, as agreed by the SS and the DA, process the responses and/or results and issue a TR and LoR detailing whether, or not, service levels and claims have been maintained.

3.8.4 Detailed guidance on the process for STM application, testing and approval under the Scheme is provided in the Vendor Guideline (VG).

4 ORGANISATION AND MANAGEMENT

4.1 Introduction

4.1.1 This section describes the roles of the principal participants in the process of claims testing and approval. It describes the associated policy and approach. The principal participants in the STM process are:

- Host Country Association (HCA)
- Decision Authority (DA)
- Scheme Secretariat (SS)
- Accredited Test Facility (ATF)
- Vendor
- IoT Owner/User

4.1.2 The respective relationships are illustrated in the diagram at Appendix A.

4.2 Host Country Association (HCA)

4.2.1 A HCA may be appointed by the Scheme Senior Executive to administer the Scheme in a particular jurisdiction or region, the Scheme Secretariat (SS) is appointed from the HCA.

4.2.2 The terms of reference for each HCA are:

a. Represent the Scheme in their domestic market, to set local objectives, globally align, and review policy and standards for the operation of the Scheme. This should take account of the identified requirements of Vendors, Users/Consumers, Test Facilities, government departments, agencies, regulators and other interested parties, including requirements identified through customer stakeholder groups;

b. to consider and keep under review the rules for the operation of the Decision Authority (DA) and the Scheme as a whole,

c. Where a DA has not yet been appointed by the Scheme in that HCA's region then the HCA will work in conjunction with the Scheme Senior Executive to select and appoint a suitable DA. Note that a DA may be appointed by the Scheme Senior Executive to cover multiple regions.

d. Promote and Market the Scheme in their domestic market.

e. managing disputes and complaints under the Scheme;

f. to arbitrate in disputes arising in the context of the Scheme.

4.3 Decision Authority (DA)

4.3.1 Each Decision Authority (DA) is appointed by the Scheme Senior Executive to operate the scheme, accredit test facilities, formally accept Applications made to the Scheme, Award the STM and conduct assurance surveillance.

4.3.2 Each DA is responsible for:

a. reviewing applications from test facilities for accreditation, and providing a letter of recommendation to the Scheme Senior Executive for test facilities to become accredited as xATFs under the scheme;

b. reviewing the VCD for claims testing by an xATF of the IoT Product under the Scheme;

c. advising the xATF and/or SS of the decision on the acceptance or rejection of VCDs;

d. reviewing and accepting the TR, TRS, STR and LoR;
e. awarding the STM to IoT Products under the Scheme and notifying SS/xATF and/or Vendor of the same;
f. providing advice and guidance, where necessary, in response to questions or issues raised through the SS.
g. Conducting regular assurance surveillance activities to ensure currency of evaluated products certification.

4.3.3 Each DA will:

a. oversee the technical operation of the Scheme;
b. prioritise work as necessary;
c. provide an annual report on the Scheme operation to the Scheme Senior Executive.

4.4 Scheme Secretariat (SS)

4.4.1 Each Scheme Secretariat is responsible for supporting the operation of the Scheme on a day to day basis by:

a. acting as the first point of contact for all queries from Vendors, xATFs and IoT Owner/Users concerning their Applications and participation in the Scheme, and referring these queries to the HCA or DA or where appropriate;
b. registering and tracking Applications made under the Scheme;
c. notifying Vendors of the progress and outcome of their Applications under the Scheme;
d. providing information and support to those involved in the Scheme;
e. publishing and maintaining details of the current/past Awards on the Evaluated Product List (EPL) on the Scheme Website, including the TRS;
f. making arrangements for presentations of STM certificates;

4.4.2 Each Scheme Secretariat works in conjunction with their respective DA.

4.5 Accredited Test Facility (ATF)

4.5.1 Test Laboratories are accredited by the scheme to become Accredited Test Facilities (ATFs) by the DA to operate under the Scheme based on a letter of recommendation from the DA to the SS following application and accreditation review. Test Laboratories are obliged as a condition of their accreditation to:

a. observe all rules of the Scheme as laid down by the Scheme Senior Executive and operated by the HCA, SS and DA;
b. be accredited and maintain their accreditation as a testing laboratory against ISO/IEC 17025;
c. observe the highest standards of neutrality, independence and commercial confidentiality.

Note: there exists options for Test Laboratories to carry interim, and provisional, accreditation. There is a Specialist test laboratory accreditation also.

4.6 Vendor

4.6.1 The Vendor is the person or organisation that has developed the IoT Product. Applications for claims testing can only be accepted from the Vendor of the IoT Product to be tested.

4.6.2 The Vendor is responsible for:

a. submitting the Application under the Scheme;
b. contracting with an xATF to undertake testing under the Scheme;
c. preparation of the VCD, assisted by the xATF, and supporting documentation for the New Application (NA).
d. abiding by the conditions of the Scheme.

4.7 IoT Owner/User

4.7.1 The IoT Owner/User is the person or organisation who purchases or procures the IoT Product.

4.7.2 The IoT Owner/User, especially a commercial, government or industrial IoT Owner/User, is strongly encouraged to:

a. check the STM Evaluated Product List (STM-EPL) for details of IoT Products which have been awarded the STM, currency of the certification, and information about the Scheme;
b. read the relevant TRS to check suitability for the assured functionality and related recommendations;
c. contact the Vendor about the IoT Product which has been awarded the STM for further information.

4.8 Disputes and Complaints Procedure

4.8.1 In the event of a dispute concerning Applications submitted to the Scheme, the Vendor should raise the matter in writing as soon as practical with the Scheme Secretariat (SS) for resolution.

4.8.2 If the dispute remains unresolved within ten (10) working days of the matter being received in writing by the SS, the dispute can be escalated in writing to the Host Country Association (HCA).

4.8.3 The decision of the HCA will be given in writing to the Vendor within twenty (20) working days of the matter being received in writing.

4.8.4 The decision of the HCA on disputes concerning the acceptance of Applications by the Scheme, the Award or Maintenance of the STM is final.

4.8.5 In the event of a dispute between a Vendor and the xATF engaged by the Vendor, concerning the conduct of either party under the Scheme, a complaint may be raised by either party with the SS. However, the Vendor and xATF should first attempt to resolve the matter through their own contractual arrangements and/or mediation.

4.8.6 Complaints to the Scheme should be sent to the SS where it will be logged.

4.8.7 The SS will, within forty-eight (48) hours of receipt of the complaint, acknowledge receipt.

4.8.8 The SS will investigate complaints made directly about the operation of the Scheme. Complaints about the performance of the Vendor's IoT Product should be directed to the Vendor in the first instance.

4.8.9 The Scheme may decide to refer a complaint to be dealt with under the disputes procedure for Vendors or xATFs, where this is appropriate, at any time during the complaints procedure. The disputes procedures are described in the Vendor Guideline (VG) and may also be covered by a Vendor Agreement and Test Facility Agreement.

4.8.10 The SS will investigate and report on complaints within twenty (20) working days of receipt of the complaint. This includes notifying all parties to the complaint about the outcome of the investigation of the complaint. The SS will notify all parties to the complaint when all corrective action has been completed.

4.8.11 If the matter cannot be resolved by the SS within twenty (20) working days, the complaint will be escalated to the HCA. All parties to the complaint will be notified of this action.

4.8.12 If the HCA cannot resolve the complaint within ten (10) working days of the complaint being escalated, the matter will go into dispute.

Note: In lieu of a HCA/SS in a region then a DA will assume that role in the matter of Disputes and Complaints.

APPENDIX A

STM GOVERNANCE

https://iotsecuritytrustmark.org/wp-content/uploads/2021/07/IoT-STM-Presentation-v0.12.pdf

REFERENCES

https://www.iotsecuritytrustmark.org

IoT Security Trust Mark™ Description of Scheme (DOS) ISBN 978-0-9953944-2-1
IoT Security Trust Mark™ Decision Authority Guideline (DAG) ISBN 978-0-9953944-7-6
IoT Security Trust Mark™ Accredited Test Facility Guideline (ATFG) ISBN 978-0-9953944-8-3
IoT Security Trust Mark™ Vendor Guideline (VG) ISBN 978-0-9953944-9-0

[ISO 17025] ISO/IEC Guide 17025:2005, General Requirements for the Competence of Testing and Calibration Laboratories

Five Eyes Nations (FVEY) Guidance: Statement of Intent regarding security of the IoT.

https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things

ETSI – European Telecommunications Standards Institute – Cyber Security for Consumer Internet of Things: Baseline Requirements

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

National Institute of Standards and Technology (NIST), Foundational Cybersecurity Activities for IoT Device Manufacturers 8259

https://csrc.nist.gov/publications/detail/nistir/8259/final

European Network and Information Security Agency (ENISA) – Baseline Security Recommendations for IoT

https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

UK Govt (DCMS) – Code of Practice for Consumer IoT Security

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

Australian Govt (DoHA) – Code of Practice for Consumer IoT Security

https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, ver. 1.1, 16 April 2018.

https://www.nist.gov/cyberframework/framework

National Institute of Standards and Technology (NIST), Conformity Assessment

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.2000-02.pdf

[BGV] STM Brand Guidelines for Vendors [Available from SS]

[BGT] STM Brand Guidelines for Accredited Test Facilities [Available from SS]

Assessor Resource Kit (ARK) - *https://www.nata.com.au/images/pdf_files/ARK.pdf*

cPP – collaborative Protection Profiles
https://www.commoncriteriaportal.org/pps/collaborativePP.cfm?cpp=1&CFID=51599019&CFTOKEN=2044982022d0d18b-CD8660D6-155D-642E-2BBE5A052587A24F

FIPS 140-3 -- *https://csrc.nist.gov/publications/detail/fips/140/3/final*