IOT SECURITY TRUST MARK ™

CERTIFICATION & LABELLING SCHEME

MATT TETT – ADVISOR, SUBJECT MATTER EXPERT

MATT@IOTSECURITYTRUSTMARK.ORG

HTTPS://WWW.LINKEDIN.COM/IN/MTETT/

IN-CONFIDENCE

INTRODUCTION

The Internet of Things (IoT) Security Trust Mark™ (STM) https://iotsecuritytrustmark.org is a third-party conformity assessment, certification and voluntary 'live' labelling scheme providing IoT users (consumers) with a recognisable level of assurance that IoT provider's (vendor/manufacturer) security claims about their product have been independently evaluated and conform with internationally established baseline security requirements.

IN-CONFIDENCE 2021 © SECURITY MARK P/L

- History
- Key Tenets
- Reasons
- Requirements
- Governance
- Process
- International IoT Security Standards, Recommendations, Guidelines & Codes
- Alignment with IoT Security Trust Mark™ Baseline Requirements
- Next steps

IN-CONFIDENCE 2021 © SECURITY MARK P/L

IN-CONFIDENCE

HISTORY

- With the evolution of the “Internet of Things” it became evident that a globally applicable certification framework was required to ensure vendors security claims were valid, and their IoT products met general security baseline principles for IoT as set by Governments and International Standards bodies, such as ETSI, ENISA, SSC and NIST.
- In 2012 Enex, formerly the RMIT University IT Testing Laboratory, Australia, continued R&D on a project *(“SEPR”)* that was commenced in the Enex (UK) Lab in 2006. That original work involved a government initiated (Cabinet Office & Home Office) assurance programme focused on the independent evaluation, validation and certification of vendors claims about the electronic security of their products. An article[1] about it was published by CSO Magazine in 2013. In 2017 focus shifted to IoT.
- In late 2019 the UK, US, Canada, Australia and New Zealand, collectively known as the Five Eyes (FVEY) released a joint statement of intent[2] regarding the security of the Internet of Things. Acknowledging that the lack of security in IoT devices is a global issue, expecting manufacturers to incorporate security-by-design, and actively seek out opportunities to enhance trust and raise awareness of security safeguards associated with IoT devices in those respective nations.
- In 2019 the research IP was transferred from Enex P/L to Security Mark P/L for the purpose of commercially licensing a number of cyber security and information assurance technology related third-party conformity assessment marks, covering areas such as Information Technology (IT), Information Communications Technology (ICT) and the Internet of Things (IoT).
- The governance, policies and procedures that comprise the IoT Security Trust Mark™ Certification and voluntary Labelling scheme were formalised and the program licenced and commercially launched by IoT Security Mark P/L. With the scheme Pilot program opening in 2021.
- The global IoT Security Trust Mark™ certification and labelling scheme supports the IoT Security objectives stated by FVEY.

[1] https://www2.cso.com.au/blog/cso-bloggers/2013/04/05/baseline-security-evaluation-serp/

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

KEY TENETS

- The IoT Security Trust Mark™ (STM) is a certification and product labelling scheme established to test the validity of vendors claims of security functionality in Internet of Things (IoT) Products, in which Information Assurance (IA) is a major consideration.
- The objective of the Scheme is to meet the needs of Government and Industry for efficient, cost-effective testing of IoT Products security claims. The STM is primarily aimed at IoT Products to meet IA requirements at the higher impact levels, for purchase by central government and the wider public sector, particularly in the areas of consumer, transport, health, agricultural, industrial systems, and smart cities.
- Integrity, Neutrality, Scalability and Longevity are key tenants of the STM scheme governance structure;
  - The STM scheme engenders Trust by maintenance of clear Independence which it does through federation with distinct functional, and organisational, separation of duties, roles and responsibilities.
  - It has to scale, the STM is an internationally applicable scheme, it achieves this via the distributed governance structure.
  - The STM needs to endure, it has been designed to have no single point of failure or reliance on a single source of funding, sector or body, i.e., Government policy, resourcing and budgets etc.
  - The STM scheme uses globally accepted IoT Security Recommendations, Guidelines and Codes published by governments, and standards organisations such as ETSI, ENISA, SSC and NIST to set the security Baseline Requirements (BR)[1]

[1] https://iotsecuritytrustmark.org/baseline/

IN-CONFIDENCE 2021 © SECURITY MARK P/L

REASONS & REQUIREMENTS

- 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 *(SP.2000-01/02)* and covers the principle 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?

- The scheme provides assurance to purchasers of IoT products that hold current IoT Security Trust Mark™ certification that the claims vendors are making in their scheme Vendors Claims Document (VCD); requirement; about their product security have been independently verified by an STM Accredited Test Facility (ATF) that maintain ISO/IEC17025; determination; and meet Baseline IoT security Requirements (BRs) as set by Standards Bodies and Governments, are certified by a scheme Decision Authority (DA); attestation.

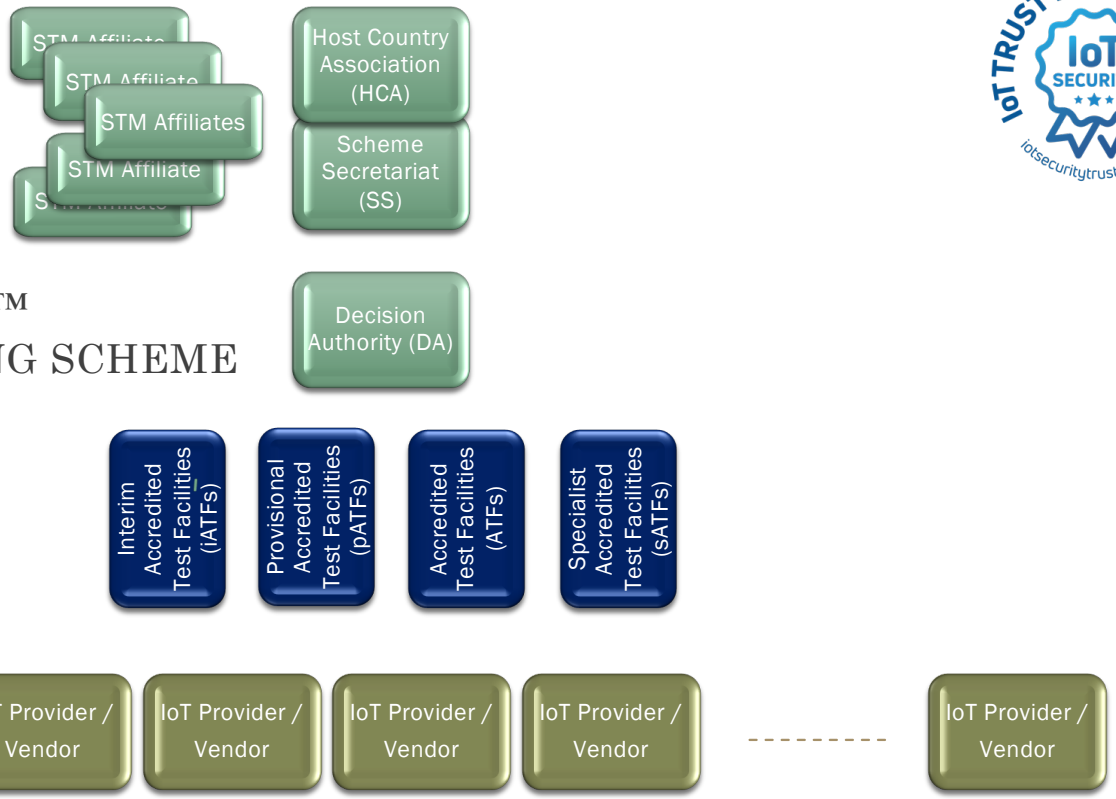
- It is imperative not to convey a false sense of security to the IoT consumers or users through the certification mark. Common Vulnerabilities & Exposures (CVE®), National Vulnerability Database (NVD) and software bill of materials (SBOM) Vulnerability Exploitability eXchange (VEX) profiles are actively monitored by scheme DA; surveillance; to ensure vendors of certified products are notified and aware of any vulnerabilities and those are remediated, during this process the certification is appended to a suspended state until remediation is achieved. If remediation is not successfully achieved within a period then the certification is expired.

IN-CONFIDENCE 2021 © SECURITY MARK P/L

IN-CONFIDENCE

GOVERNANCE

IOT SECURITY TRUST MARK™ CERTIFICATION & LABELLING SCHEME



IN-CONFIDENCE 2021 © SECURITY MARK P/L

IN-CONFIDENCE

PROCESS

- *Appoints Scheme Senior Executive*
- *Licensor of STM to HCAs*
- *Licensor of STM to DAs*
- Hosts and publishes STM website and Evaluated Product List (EPL) *(including Summary (STR)*
- Manages STM documentation

- Markets STM
- Liaises with Government
- Liaises with Industry
- Raises STM awareness with consumers
- Acts as, or appoints, SS

STM Affiliates

- Supporters of the Scheme

- Provides scheme administration for the HCA

- Accredits ATFs, iATFs, pATFs, and sATFs
- Reviews Vendor Claims Documents (VCD)
- Reviews Test Reports (TR)
- Oversees technical function of STM
- Issues/Revokes Certificates
- Monitors Common Vulnerabilities and Exposures (CVEs)

- Engage with vendors
- Assist in the creation of VCDs
- Performs Testing
- Issues TR, TRS, and Letter of Recommendation (LoR)
- Collects revenue

iATF

pATF

sATF

- Funds the scheme *(<USD$30k <30-days for pass/fail, avg. $10k~$15k)*
- Engage with ATFs
- Selects and ATF, create an VCD
- Submit VCD to DA
- Display STM label on certified products *(opt.)*

- Requests STM from suppliers
- Seeks STM label on IoT products
- Prioritises/weights STM certified products when procuring
- Chooses products from the STM EPL
- Reads TRSs

GLOSSARY

(i/p/s)/ATF ~ Accredited Test Facility (interim, provisional, specialist)
DA ~ Decision Authority
EPL ~ Evaluated Products List
HCA ~ Host Country Association
LoR ~ Letter of Recommendation
SS – Scheme Secretariat *(function of, or appointed by, HCA)*
STM ~ IoT Security Trust Mark™ Scheme
TRS ~ Test Report Summary
TR ~ Test Report
VCD ~ Vendor Claims Document

IN-CONFIDENCE 2021 © SECURITY MARK P/L

IN-CONFIDENCE

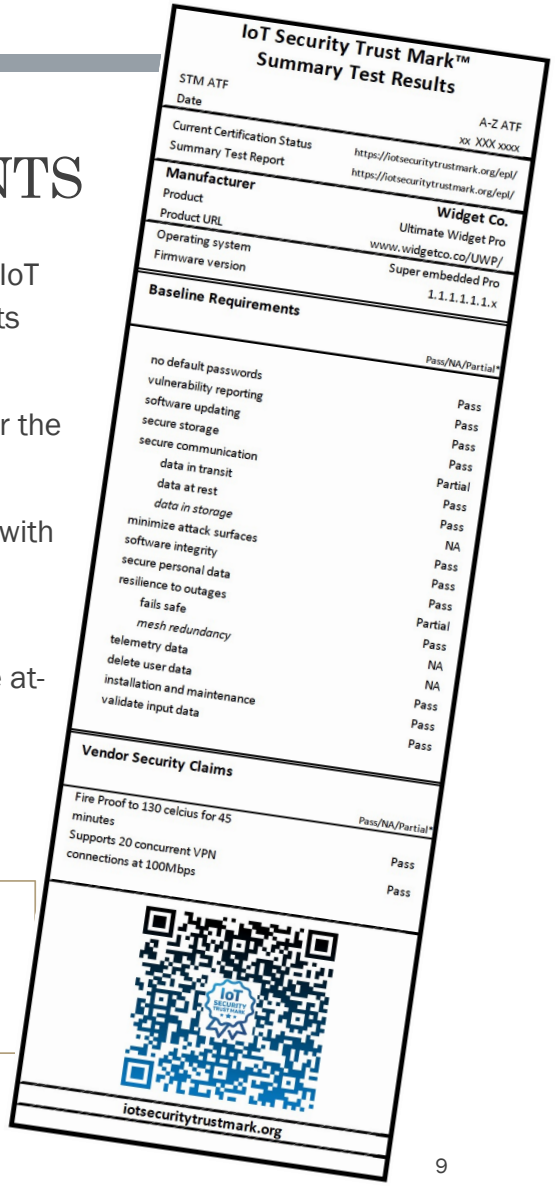
STANDARDS, RECOMMENDATIONS, GUIDELINES & CODES

- Where to start?[1] The Baseline Requirements for the IoT Security TrustMark™ scheme are comprised of;
- International Standards Bodies
  - ISO/IEC – 27400 – Cybersecurity – IoT Security and Privacy Guidelines
  - Europe ETSI – EN 303 645 – Cyber Security for Consumer Internet of Things: Baseline Requirements
    - ETSI – TS 103 701 – Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements
  - Europe ENISA – Baseline Security Recommendations for IoT for Critical Information Infrastructures
  - United States NIST – NISTIR 8259 – Foundational Cybersecurity Activities for IoT Device Manufacturers
    - NISTIR 8259A – IoT Device Cybersecurity Capability Core Baseline
    - NISTIR 8259B – IoT Non-Technical Supporting Capability Core Baseline
    - NISTIR 8228 – Considerations for Managing IoT Cybersecurity and Privacy Risks
    - NIST Draft Baseline Security Criteria for Consumer IoT Devices
  - Singapore SSC – TR 91 : 2021 – Cybersecurity labelling for consumer IoT
  - ISO/SAE – 21434 – Road Vehicles – Cybersecurity Engineering
- Government Departments and Agencies
  - United Kingdom – DCMS – Code of Practice for Consumer IoT Security
  - Australia – DoHA – Code of Practice Securing the Internet of Things for Consumers
  - India – TEC – Code of Practice for Securing Consumer Internet of Things
- IoT Industry self attestation initiatives
  - IoXt Alliance – IoXt Security Pledge

[1] https://iotsecuritytrustmark.org/baseline/

ALIGNMENT WITH IOT STM BASELINE REQUIREMENTS

- Taking each of the published standards, recommendations, guidelines, and codes and distilling those into the IoT STM Baseline Requirements ensures global applicability in compliance with the security of IoT vendors products that successfully pass the conformance evaluation.
- It also ensures currency with the latest good practice IoT security requirements as they develop and evolve over the years. Ensuring there are a number of bodies setting the requirements.
- The value for vendors is greater given the IoT STM is a “one-stop-shop” when it comes to providing consumers with assurance of conformance.
- Consumers can visit the STM Evaluated Product List published on the website to ascertain the currency of a products certification at any given point in time and also to review the published Test Report Summary and the at-a-glance “nutrition” label itemising the areas of Baseline Requirement conformance applicability that the IoT product passed during evaluation.



IoT vendors may also voluntarily attach the IoT STM “live” label to their product and product marketing material at no additional cost, which incorporates a Quick Response (QR) code which links directly to that product on the STM Evaluation Product List enabling consumers to make an informed decision at the Point of Sale.

IN-CONFIDENCE 2021 © SECURITY MARK P/L

IN-CONFIDENCE

NEXT STEPS

- The IoT Security Trust Mark™ (STM) is currently in open pilot inviting expressions of interest from leading IoT vendors to participate in the scheme.
- IoT products that pass the Pilot scheme are granted full certification, which enables grandfathering when the scheme is fully released.
- IoT vendors are offered an attractive discount for participation in the Pilot and are also featured as case studies.
- The IoT STM is currently being socialized and harmonized internationally to gain wider recognition of the STM certification framework, process and governance.
- Seeking parties interested in becoming Host Country Associations in international territories, as well as STM Accredited Test Facilities
- All details can be found on the IoT STM organisation website ; https://www.iotsecuritytrustmark.org
- Follow the Twitter account for daily #IoTsecurity news and updates ; @iot_trust_mark

THANK YOU

IN-CONFIDENCE 2021 © SECURITY MARK P/L