Title: IoT Security Trust Mark™ Certification & Voluntary Labelling Scheme
Author: Matt Tett
Advisor - Subject Matter Expert, IoT Security Trust Mark™ Scheme
Ref: https://www.iotsecuritytrustmark.org/
Audience: National Institute of Standards and Technology
Class: COMMERCIAL-IN-CONFIDENCE

To Whom It May Concern:

This paper describes relevant details of the Internet of Things (IoT) Security Trust Mark™ Certification Scheme *(STM or Scheme)* and how it addresses the common problems. We noticed your recent request calling for papers[1] and would like to draw your attention to the program of works that we have undertaken in developing and launching the IoT STM, currently in Pilot. The formation work was initially commenced in 2006 with the design for certification of products' electronic security for use in Information Assurance (IA) programs, renewed and directed towards IoT in 2017, formalised in 2019.

The Scheme has been developed to be global, scalable *(federated principles)*; technology and standards agnostic. It is rigorous and independent and offers good value *(self-funding*); without compromise. It complies with accepted conformance assessment "norms" *(such as NIST.SP.2000-01/02)*. STM is designed to support both product manufacturers/vendors as well as consumers, at all levels. We encourage vendors to innovate and incorporate good security, safety, and privacy by design principles in their development and manufacturing processes. We acknowledge without good, inherent, security in smart devices they cannot underpin consumer/user safety and/or their information privacy.

Traditional ICT cyber security practices have never worked effectively. Requiring consumers/users to implement reactive security controls, policies and procedures is not the answer. That issue will be amplified exponentially when it comes to IoT 'smart' devices. The paradigm needs to shift. Consumers should seek vendors' products that inherently offer them higher levels of security, and therefore safety and privacy. Vendors in turn should identify that the greater levels of safety and privacy assurance they can demonstrate to their market, by embedding good security-by-design principles, the more trusted they are. IoT Security needs to become a unique selling point delivered that informed consumers seek.

Unfortunately to-date regulation, compliance, and certification in general, *(security or otherwise)*, is seen as a cost centre and burdensome by vendors typically to be avoided if possible. The STM addresses the concerns held by many that costs and time to comply outweigh the benefits. Indeed, the Scheme needs to address this as it is self-funding and relies on offering practical value and timeliness as a measure of operating success. A good example of this timeliness is that a pass/failure is delivered within 8~12 days on average and is capped by the Scheme at no more than 30-days. Supporting vendors who are striving to deliver the right thing with their IoT device security, by independently validating their security claims and ensuring they meet IoT Security Baseline Requirements (BR).

[1] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-papers-cybersecurity-labeling

Not all certifications are equal, it is one thing to build a certification program that measures something against a predefined standard, say telecommunications emissions or electrical safety for example. However cyber security is an ever-moving target. It would be virtually impossible to define a "one-size-fits-all" standard that is applicable to the diverse nature of products that may at any point in time be connected to the Internet globally. STM successfully addresses this diversity by being a security certification and labelling framework that incorporates flexibility to adopt and incorporate the criteria of IoT Security Baseline Requirements (BR) used for STM evaluation from several diverse sources as they evolve, such as global standards bodies; *(i.e. ETSI, ENISA, NIST),* and Codes and Guidelines (or legislative requirements) produced by Governments, or their Departments and Agencies. The STM also combines evaluation and assurance to Baseline Requirements, but also verifies vendors security claims.

Internet of Things security is not just the issue of one country or jurisdiction, international experience demonstrates this. Supporting this, in late 2019, Ministers from the United States, United Kingdom, Canada, Australia and New Zealand, the Five Eyes (FVEY) countries, agreed and signed a Statement of Intent regarding the security of the Internet of Things[2]. They recognise the problem and consequences, and publicly acknowledge that the solution to good IoT security is not something that any single country alone can solve. Further that they require the industry itself to step up to avoid making the same mistakes made with ICT cyber security. The STM Scheme covers this, being designed to be a global program, and most importantly scalable, it employs a federated governance model, appointing a number of stakeholders in key positions of responsibility, while maintaining consistency, transparency and independence.

Other programs may rely on vendor self-attestation of security, while this may provide some level of assurance to consumers, vendors stating their security claims, it is no guarantee of security. Often written to requirements that are open to interpretation by the organisation applying the claim of compliance, or even the individuals' level of expertise in the matter. Indeed, in the past other industries have seen consortia of vendors organised to influence standards or "self-certify" ultimately to the detriment of the consumer, who their technologies are inherently supposed to serve. The STM operates with Accredited Test Facilities (ATFs), who are independent, ISO 17025 accredited testing laboratories, their approved Test Officers work with vendors to create Vendor Claims Documents (VCDs) which are in-turn approved by a third-party Decision Authority (DA) prior to any STM evaluation commencing. Ensuring transparency and independence while maintaining value and timeliness.

A remark often levelled at security compliance programs is that it is only as good as the day of audit/test. And while this is indeed true, the IoT Security Trust Mark™ Scheme incorporates significant levels of ongoing surveillance by a technical Decision Authority, ensuring that any known vulnerabilities and exposures are reported to certified product vendors and the product certification is suspended until that vulnerability is addressed.

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

The Security Trust Mark™ Evaluated Products List (STM-EPL) lists each product that has been evaluated and includes a Test Report Summary (TRS) from their STM ATF. The STM EPL is fully searchable by consumers/users researching products, and it also incorporates the STM 'traffic light system' which enables consumers to easily visually identify the currency of certification according to the colour displayed next to the evaluated product. Green for currently certified, Amber for suspended, and Red for expired. That leads on neatly to the final point, labelling.

The IoT Security Trust Mark™ Certification itself is one thing, however the labelling of certified products is another. The market provided feedback that labelling in some instances may be beneficial, but not all. And as such the STM offers a voluntary label (STM QR code), at no further cost, which vendors may apply to their certified products should they choose. This unique code for each certified product links directly to the STM Evaluated Product List. Thus, ensuring high levels of usability for IoT consumers.

Ultimately IoT consumers must be empowered to make informed decisions when it comes to buying smart devices with inherent security, underpinning their safety and privacy.

The IoT Security Trust Mark™ Certification and voluntary labelling scheme is currently in open Pilot, and seeking expressions of interest from various stakeholders, including Vendors seeking Pilot participation, and prospective; Host Country Associations (HCAs), Decision Authorities (DAs) and Accredited Test Facilities (ATFs).

All enquiries can be made via the organization's website: https://www.iotsecuritytrustmark.org/

For further information of relative STM stakeholders there are a series of documents that set out in detail various requirements under the IoT Security Trust Mark™ Scheme:

Description of Scheme (DOS) v1.6, 503KB, 24-pages, PDF (ISBN 978-0-9953944-2-1)
Vendor Guideline (VG) v1.5, 759KB, 27-pages, PDF (ISBN 978-0-9953944-9-0)
Accredited Test Facility Guideline (ATFG) v1.6, 926KB, 37-pages, PDF (ISBN 978-0-9953944-8-3)
Decision Authority Guideline (DAG) v1.3, 791KB, 25-pages, PDF (ISBN 978-0-9953944-7-6)

These are available upon execution of the STM Mutual Non-Disclosure Agreement (MNDA)