Building trust in the IoT through security standards, testing and accreditation

Version 1.0

CRYPTO
QUANTIQUE

Introduction

Building and sustaining trust is challenging, even among friends who have known each other for years. Building and sustaining trust in Internet of Things (IoT) devices and ecosystems is doubly challenging, because the technology is relatively new, it is being deployed at such massive scale, and the risks of trust being misplaced can be so high. The IoT sector's security record so far has not been great, and the resultant loss of trust is constraining market growth: according to some estimates, one in three consumers would not buy a smart device for their home due to security concerns.

IoT developers are now deploying a combination of hardware, software, checklists, standards, certifications, business processes and legislation to try to rebuild and grow consumers' trust in the security of the IoT devices and ecosystems with which they interact. It's a long job.

Barriers to security

There are many barriers to implementing effective IoT security, **according to a 2021 Security Report by PSA Certified**, an industry body that promotes a security assurance scheme based on the Platform Security Architecture framework introduced in 2017 to simplify the implementation of IoT security measures.

The report, based on a November 2020 survey of 628 technology decision makers, found that 48% of respondents believed the biggest barrier to implementing IoT security was the fragmentation of both standards and regulations. This article considers the standards issue.

Back in October 2018, the UK government's Department for Digital, Culture, Media & Sport tried to work out how well its emerging guidelines for consumer IoT security matched other efforts. The resultant report, *Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security,* considered around 100 documents from almost 50 organisations. It ran to 223 pages

This fragmentation seems to persist to this day. Speaking during an online roundtable on IoT security organised by PSA Certified in June 2021, Jan Muenther, head of digital product security at ams OSRAM, said: "Regulation is a mess and it's only going to get more complex, because everyone thinks they can do better."

Muenther argued that, given this context, IoT developers should not focus on implementing regulations but on applying security best practices – because regulations are designed to encourage designers to use these best practices anyway.

“Then if there are specific ‘deltas’ [differences, additional measures] that we need to implement to enter a market, we can do that afterwards,” he added. “But if you try to follow every evolving standard and take all their regulatory requirements into account, that gets very messy very fast.”

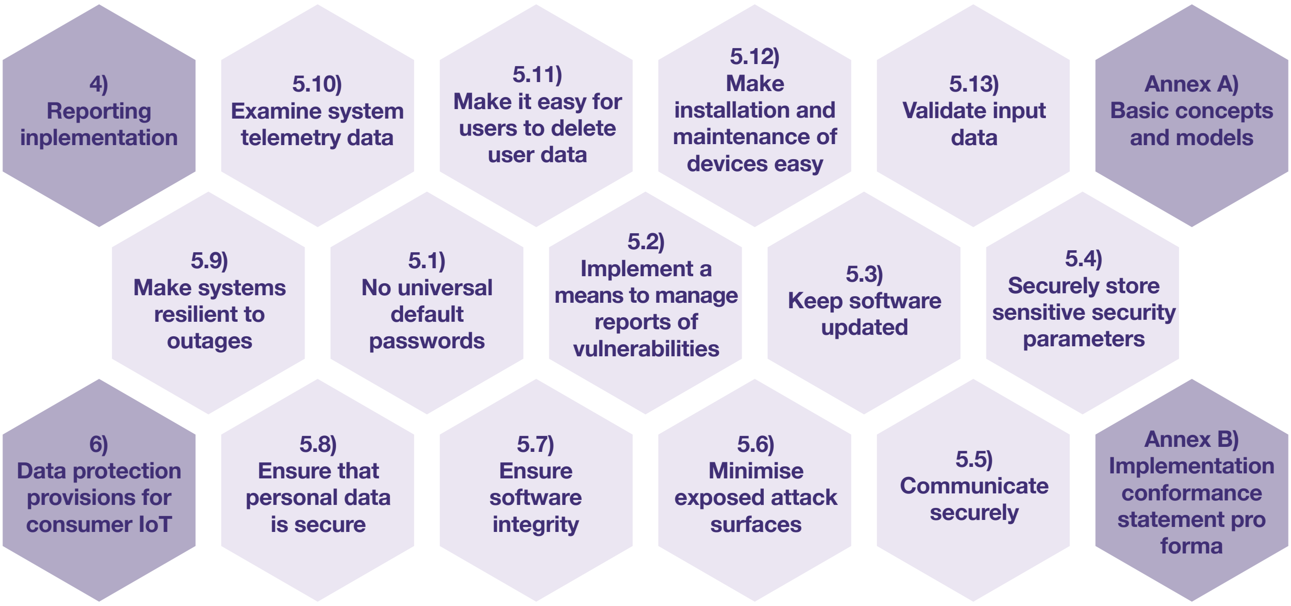
The other barriers to implementing a secure IoT device or ecosystem included a lack of understanding of the issue within the business (42% of respondents), liability issues (27%), the effect on time to market (27%), and the likely return on investment (25%).

Protecting consumers

One standardisation effort that is gaining some momentum comes from ETSI (**www.etsi.org**), an EU standards body that has more than 900 member organisations, drawn from 65 countries and a diverse pool of private companies, research entities, academia, government and public organisations. ETSI's technical committee on cybersecurity (TC CYBER) released the first version of its technical specification, TS 103 645, in February 2019. This was developed into EN 303 645, an IoT cybersecurity standard, and published in June 2020. It is meant to establish a security baseline for consumer IoT devices such as baby monitors, door locks, and smoke detectors, and provide a basis for certification schemes. It has 13 general provisions for IoT device security, and five specific provisions for data protection.

The standards development process drew on input from the ETSI membership and other industry bodies such as CEN/CENELEC JTC 13, two more European standards bodies, and the core content of the DIN SPEC 27072 developed by the German Institute for Standardization. Other contributors include the UK's National Cyber Security Centre, IBM, Huawei, Samsung, Philips, Bosch, BT and many others.

It's a telling reflection on the state of cybersecurity today that all this coordinated effort delivered a standard whose provisions, outlined in the graphic below, are so basic: don't ship product with default passwords; make sure there's a way to report issues; keep software updated; secure personal data and make it easy to delete etc.


4) Reporting inplementation
5.10) Examine system telemetry data
5.11) Make it easy for users to delete user data
5.12) Make installation and maintenance of devices easy
5.13) Validate input data
Annex A) Basic concepts and models
5.9) Make systems resilient to outages
5.1) No universal default passwords
5.2) Implement a means to manage reports of vulnerabilities
5.3) Keep software updated
5.4) Securely store sensitive security parameters
6) Data protection provisions for consumer IoT
5.8) Ensure that personal data is secure
5.7) Ensure software integrity
5.6) Minimise exposed attack surfaces
5.5) Communicate securely
Annex B) Implementation conformance statement pro forma

America’s National Institute of Standards and Technology (NIST) is also working on guidance about IoT cybersecurity, focusing on ensuring that IoT devices meet the security and privacy needs of federal information systems. The work lays out a process that could be used to enhance IoT cybersecurity in other contexts, and also addresses many non-technical issues.

NIST has recently published four documents:

- SP 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements
- NISTIR 8259B, IoT Non-technical Supporting Capability Core Baseline
- NISTIR 8259C, Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline
- NISTIR 8259D, Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

They build on work in two other documents:

- NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers
- NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline

SP 800-213 offers recommendations to help federal agencies think about how to integrate IoT devices into federal information systems, especially the abilities and actions that an agency should expect from an IoT device and its manufacturer.

The NISTIR 8259 documents then provide tools to implement SP 800-213's guidance to develop specific security requirements.

NISTIRs 8259A and 8259B are a pair. NISTIR 8259A focuses on defining baseline requirements for device cybersecurity. NISTIR 8259B details the non-technical support typically needed from manufacturers, such as documentation, training, and customer feedback.

NISTIR 8259C describes a process for applying the baselines defined in NISTIR 8259A and 8259B in an organisation, to develop an IoT cybersecurity profile suitable for specific IoT device customers or applications.

NISTIR 8259D details the results of applying the NISTIR 8259C process in federal government, providing a device-centric, cybersecurity-oriented profile of the core baselines. NIST says that organisations with needs that aren't addressed by the federal profile contained in NISTIR 8259D should apply the guidance in SP 800-213 to define their security requirements, and then use the NISTIR 8259C process to develop an IoT cybersecurity requirements profile for their needs.

In other words, NIST has done a lot of careful work on using IoT devices securely, and that work is available for anyone else to take advantage of – if they have the resources and rigour to work through its recommendations and processes.

Putting the ETSI standard to work

A standard becomes valuable when it is put to work. Finland was an early adopter of the ETSI work on IoT security, launching a voluntary Cybersecurity Label for secure smart devices in November 2019, based on the emerging standard.

Speaking when EN 303 645 launched in June 2020, Juhani Eronen, chief specialist at Traficom, the Finnish National Cyber Security Centre at the Finnish Transport and Communications Agency, said: “Our labels are awarded to networking smart devices that meet certification criteria based on EN 303 645; this help consumers identify IoT devices that are sufficiently secure. Being involved in the development of the ETSI standard from the start helped us a lot in building up our certification scheme.”

Many others are incorporating EN 303 645 into their work on improving the security of consumer IoT devices. Singapore has developed a national Cybersecurity Labelling Scheme based on EN 303 645. Test and accreditation houses TÜV Süd and VDE are offering testing to EN 303 645, while TÜV Rheinland is offering certification to the standard. The Global Certification Forum, an industry body that promotes the testing and certification of mobile and IoT products to reassure network operators that it is safe to allow them onto their networks, is offering accreditation to EN 303 645.

Even as some organisations adopt EN 303 645 on an ad-hoc basis for testing, labelling, certification and assurance schemes, ETSI is pressing ahead with work to bring some rigour to these processes as well.

For example, it is developing an assessment specification, under the nomenclature of TS 103 701, which will define a set of mandatory and recommended tests for assessing the conformance of consumer IoT products to EN 303 645. The idea is to help standardise the work of testing labs and certifying bodies. The specification may also become an input to a future EU cybersecurity certification scheme, as proposed in the EU Cybersecurity Act.

ETSI is also working on an implementation guide, under the nomenclature TR 103 621, which will help manufacturers meet the requirements of EN 303 645. It will include example implementations of popular IoT devices, designed to meet the provisions of the EN standard. ETSI's TC CYBER group is also working on using EN 303 645 as a basis for sector-specific standards: the first target is a standard for smart door locks.

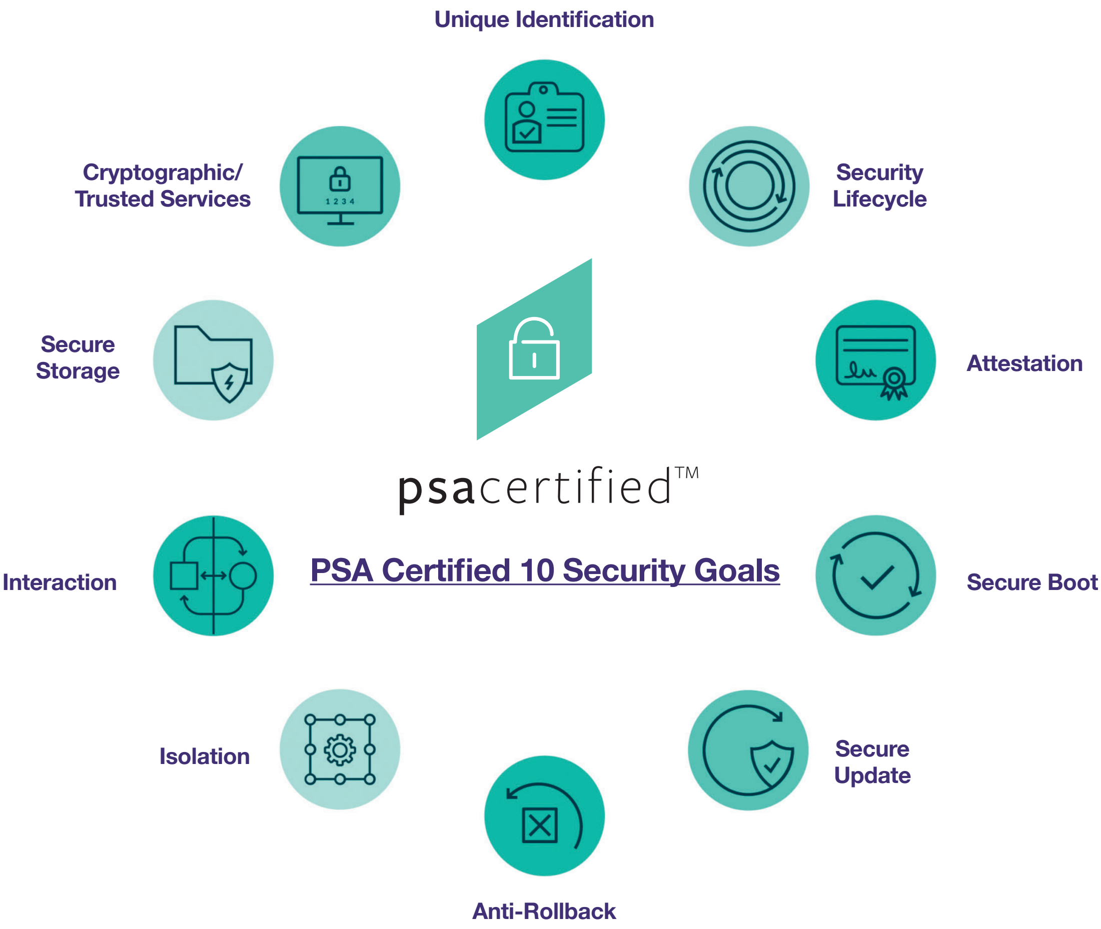
Standards need cheerleaders

ETSI's work is backed by two other significant organisations, which are both trying to take a leading role in ensuring the security of consumer IoT devices.

The PSA Certified organisation promotes a security framework and IoT assurance scheme that is designed to align with industry standards, government regulation, and regional markets, to give device vendors better insights into their security coverage. This, in turn, will enable them to prove the quality of their security protection, hence allowing them to lower product costs.

The framework has four phases. In the analysis phase, users develop a threat model to determine their security needs. In the 'architect' phase, they apply an established security architecture to meeting those needs. In the implementation phase, users create a high-quality implementation. And in the certification phase, users get an independent, unbiased security evaluation of their device, software platform and chip.

PSA Certified promotes ten security goals to guide IoT device design and inform the certification program, as shown in the graphic below.



IoT security is particularly challenging because devices are widely distributed into arbitrary locations, making it easier to manipulate them to, for example, take over other devices' identities. The PSA Certified approach to this challenge is to suggest the use of a hardware Root of Trust (RoT), an immutable, uncopiable element in the device's silicon which can be used to prove the unique identity of an IoT device. The PSA-RoT specification enables nine key security functions, including trusted boot, cryptography, secure storage, and attestation. The PSA Certified framework then defines three levels of PSA-RoT.

Given the importance of the RoT in protecting an IoT device, the IoT ecosystem it forms a part of, and the value chain that it enables, PSA Certified labs can independently test the silicon implementation of a RoT for its ability to deliver the protection functions defined in the Certification level it is claiming to implement. At the same time as PSA Certified has been developing its platform, framework and certification-based approach to IoT device security, another organisation has been developing along parallel lines.

The Internet of secure things (ioXt) Alliance claims to be ‘the Global Standard for IoT Security”. Its mission is “to build confidence in IoT products through multi-stakeholder, international, harmonised, and standardised security and privacy requirements, product compliance programs, and public transparency of those requirements and programs.”

The IoXt Alliance is backed by companies including Amazon, Facebook, Google, Honeywell, Silicon Labs, T-Mobile, Comcast, and the Zigbee Alliance. It has a certification programme and offers a list of certified products. It even has an IoXt Security Pledge, which promises that ioXt certified devices should have: no universal passwords; secured interfaces; proven cryptography; security by default; verified software; automatic security updates; a vulnerability reporting programme; and a security expiration date. In other words, a lot of features that other IoT security efforts also support.

PSA Certified is now presenting itself.as the organisation that can tackle the fragmentation of IoT security standards and guidelines. In 2020 it updated its PSA Certified Level 1 questionnaire to version 2.0, to align the questions within it more closely with the essential parts of four other documents:

- ETSI EN 303 645, for the European market
- NIST 8259A baseline, for North America
- Californian state law, which is leading on regulating RoT security
- Draft IoT security requirements from the UK government

At the same time, at least at the launch of the EN 303 645 standards back in June 2020, the ioXt Alliance was listed in the launch materials as developing an assurance profile for the European standard.

There was further alignment in IoT security in October 2020, when the ioXt Alliance announced that it had selected PSA Certified as a foundational RoT scheme and would recognise it as such in its product evaluations. The quotes given by the two organisations in their press release reflect their different backgrounds.

Brad Ree, chief technology officer of the ioXt Alliance, said: “Securing IoT devices from inception is one of our core principles at the ioXt Alliance and that mission closely aligns with the great work that PSA Certified – co-founded by Arm – has and continues to accomplish. By working with the organization, we will look to expand our reach into the global silicon industry and strengthen our resources that bake security into all facets of a connected device.”

Andy Rose, chief system architect and fellow at Arm, said: “As the number of connected devices we interact with continues to grow, comprehensive security must be designed in from the ground up and simple to deploy. PSA Certified is an industry-wide initiative focused on certifying a hardware Root of Trust and supported by the world’s leading semiconductor companies. By partnering with the ioXt Alliance, we will unlock even more ways to simplify and enhance device security for the IoT ecosystem.”

Talking security

Why did semiconductor IP vendor Arm invest its time and resources in helping to develop PSA Certified? Anurag Gupta, director of business development for PSA Certified at Arm, told the June panel that PSA Certified was started in order to ease fragmentation in IoT security.

“If we do all this, it will create opportunities and make the whole bigger for all of us,” Gupta said.

Other panellists stressed the importance of developing an IoT security ecosystem. Giuseppe Surace, chief product and marketing officer at Eurotech, pointed out that IoT security impacts the whole of any digital transformation effort in any sector, and so it is vitally important to help customers trust that their data will be secure. He added that some customers are still doing their own security work, taking a “roll your own” approach, when really “it’s an ecosystem game.”

Muenther at ams OSRAM added: “To get a viable result, everyone has to take responsibility for their part. We need an ecosystem so that we lift each other to the level that the customer expects. The loss of customer trust is due to failing to fix the problem: customers expected the industry would use best practices and they didn’t.”

Other panellists pointed out that the IoT security ecosystem needs to be enriched with new players, such as insurers that will trust IoT security standards and certifications deeply enough to risk real money on them.

Muenther pointed out the challenge of insuring IoT ecosystems, given that they often involve niche applications, when cyber insurers are much more familiar with insuring more quantifiable risks such as large IT installations.

“If you want to insure a secure custom device, where do you start?” he said, arguing that in the long term the industry must address the issue by establishing a landscape of security certifications which are actually meaningful, to come up with a trust certification that is good enough for insurers.

Asked what single step would have the most impact on improving IoT security, Muenther pointed to the importance of secure hardware.

“There’s only so much software can do, especially if the hardware is flawed,” he said. “You can’t always software your way out of an issue.”

Surace at Eurotech echoed his statement, adding: “Hardware roots of trust can certainly help. It would be the first building block to boost all the other security features.”

Contact us

For more information please see **www.cryptoquantique.com**
or contact **info@cryptoquantique.com**

CRYPTO
QUANTIQUE