IASME CONSORTIUM

Certifying IoT device security: What have we learned?

IASME's findings from the pilot of the *IoT Security Assured* connected-device certification scheme

January 2021

Overview

This document is a summary of the learnings from the pilot of IASME's *IoT Security Assured* internet-connected device certification scheme. It aims to assist understanding of the impact on security of device certification schemes and support the discussion about the most successful way to operate them.

About the IASME Consortium

The IASME Consortium is the UKs leading information assurance organisation for SMEs.

The organisation was established in 2010 following a government funded project to develop an alternative to ISO 27001 for small organisations. The IASME Consortium works to ensure that SMEs have access to good quality cyber security advice and certification at an accessible cost.

The IASME Consortium certifies more than 1,500 companies each month through its 260 UK-based Certification Bodies.

IASME is expanding its range of certifications to include specialised certifications for IoT devices and working with partners to offer certifications that help meet anti-fraud requirements for financial services organisations.

Executive Summary

IASME Consortium has piloted *IoT Security Assured,* a new security certification for Internet of Things (IoT) devices, with ten device manufacturers of different sizes across a variety of product sectors.

The pilot found that around 60 percent of manufacturers made positive changes to improve the security of their devices in order to achieve certification. The most common change made was the implementation of a vulnerability disclosure policy and associated processes, in addition to changes to the manufacturers approach to privacy and data protection. Pilot participants found the support and guidance from a skilled assessor useful to implement the changes needed. Also, assessors provided feedback that pilot participants needed targeted guidance particularly for those that lacked a technical understanding of security

Pilot participants gave positive feedback about the question set and the assessment process but found that scoping for certification could be complex. It was also observed that to complete the assessment manufacturers needed to involve people from across the business, including those with knowledge of company processes and data protection, as well as product engineering. Pilot participants were also very interested in placing the IoT Security Assured badge on their product and marketing material.

There was some interest in certification from manufacturers who sell to businesses rather than consumers. These manufacturers were not part of the pilot, but they may be important for the initial commercial viability of IoT device certification schemes before consumer legislation is implemented.

There was interest from pilot participants in continuing their security journey, with around 50 percent of participants who achieved certification wanting to certify additional devices and many interested in certifying to an additional level of assurance beyond the verified self-assessment. IASME is developing a "hands-on" audited version of the scheme to provide this option.

IASME would like to talk to manufacturers, industry organisations, universities, government and any other interested parties about our experience of running the pilot scheme and to work together to encourage as many manufacturers as possible to improve their device security.

The *IoT Security Assured* certification and the pilot project

IASME operate information security assurance schemes which provide practical and accessible security certification for small and medium sized enterprises (SMEs), as well as larger organisations.

In 2019, we identified a need in the marketplace for an inexpensive security certification for internet-connected (IoT) devices. Using our experience of operating our existing schemes, and with guidance from the Internet of Things Security Foundation (IoTSF), we developed an initial version of the *IoT Security Assured* certification as a verified self-assessment.

In 2020, we updated and improved the IoT Security Assured certification to ensure its continued alignment with ETSI EN 303 645. We also initiated a pilot rollout of the scheme with ten manufacturers of consumer IoT devices. The aim was to incorporate the learnings from the pilot into our certification and launch the scheme commercially.

This document provides details of the pilot scheme and contains a summary of the top ten learnings from its operation.

Details of the pilot project

The pilot project involved 10 manufacturers of connected consumer devices who sell into the UK market. The manufacturers were picked from responses to a call from volunteers that was shared through IASME's Certification Bodies across the UK, through social media and through members of various industry organisations including MakeUK, TechUK, CENSIS and IoTSF

The table below provides some information about the consumer manufacturers who were participants. The information used in this report has been anonymised, so the manufacturers names are not provided. Some manufacturers have agreed to be involved in publicity about the pilot scheme and have done so separately from this document

Size of company	Type of device	Sells to UK market?
Micro	Building/home sensors	Yes
Micro	Online learning device	Yes
Micro	Lighting sensor	Yes
Micro	Personal health sensor and service	Yes
Small	Building/home monitoring sensor	Yes
Small	Modules for consumer IoT products	Yes
Small	Connected power sockets	Yes
Small	House alarm system	Yes
Large	Home security camera	Yes
Large	Home-office equipment	Yes

The manufacturers were each allocated one of IASME's IoT assessors to work with. The assessor provided to the manufacturer the following package, free of charge:

- A remote session of up to three hours to understand the product and provide customised security guidance to meet the standard
- Assessment to the IoT Security Assured certification using our IASME's online platform (which was customised specifically for the new standard)
- Marking of the assessment by the assessor with detailed feedback provided on how to improve device security
- A second remote session of up to three hours to offer further guidance on how to improve security
- Second attempt at certification (if necessary)

At each stage in the process, the assessor provided detailed feedback to IASME. In addition, on completing the process, the manufacturer provided feedback. This feedback was tracked and additional anecdotal feedback from operating the project such as phone calls and emails was added to the tracked feedback. This body of information then formed the basis for this report.

What's next?

IASME has already used the learnings from the pilot scheme to update the existing question set to version 1.2, update associated scheme documents and processes and to improve the assessment platform configuration. We will also use the learnings to help target the scheme to the right audience as we launch it commercially with the aim of ensuring that as many devices get certified as possible to improve the overall security of IoT devices sold in the UK.

We are also developing an audited version of the certification which will involve a hands-on assessment of the device by an assessor to provide an additional level of assurance whilst balancing the cost of assessment, so it remains affordable to smaller manufacturers.

We would very much like to talk to manufacturers, industry organisations, universities, government and any other interested parties about our experience of running the pilot scheme and to work together to encourage as many manufacturers as possible to improve their device security.

If you would like to get in contact to find out more about the scheme and our experience of the pilot, please contact IASME's Head of Technical Strategy, Jamie Randall (jamie.randall@iasme.co.uk).

What we have learned: the top ten findings of the pilot scheme

The pilot scheme produced a number of key findings which are detailed in this section.

❶ Around 60 percent of manufacturers made positive changes to improve the security of their devices in order to achieve certification

The overall aim of any IoT security certification scheme must be to improve the security of the devices that are certified, regardless of any other factors.

The pilot found that approximately 60 percent of the manufacturers involved made positive changes to the security of either their devices or their security processes in order to achieve certification. This should be seen as a significant positive outcome from the certification process. IASME has observed similar actions from participants in the successful Cyber Essentials and IASME Governance security assurance schemes. In both schemes we believe that participants are motivated by the schemes to make security changes and can be empowered by the structure of the question set to understand exactly where changes need to be made.

The most common change made was the implementation of a vulnerability disclosure policy and associated processes, in addition to changes to the manufacturers approach to privacy and data protection. Both of these changes were split across both large and small manufacturers.

Other changes to security made by manufacturers included:

- Implementing a defined support period for devices
- Implementing secure boot and software signing for firmware updates
- Ensuring unique ID generators are secure
- Carrying out a risk review of supply chain
- Improving cryptographic key management
- Changing device recovery processes
- Implementing secure design processes
- Verifying deployed devices

❷ Support and guidance from a skilled assessor makes a positive impact on device security

A significant proportion of the pilot funding was allocated to providing each manufacturer with an IASME IoT assessor who could provide support and guidance about how to understand the scheme requirements and implement changes to become more secure.

We found that the support and guidance was very important for many participants, in what is for many a relatively new subject area. IASME has made it a key element of all the schemes that we operate to allow assessors to have a close relationship with applicants in order to provide help and support rather than encourage a potentially adversarial assessor/client relationship. We have a strong quality control process in place, as well as a strictly enforced assessor code of conduct, which enables this close relationship. We believe that the overall outcome for security is much improved through this approach. It is also particularly helpful for SMEs where specialist knowledge of security may be limited.

Assessors provided feedback to IASME on the topics where participants needed the most support:

- Vulnerability disclosure policy
- Data protection
- Reference industry security standards that could be used to help prepare for assessment
- Encryption key management/governance
- Supplier management
- Risk assessment
- Secure development of software
- Secure configuration
- Device provisioning
- Penetration testing of devices and services
- Physical device protection

❸ Having a badge to put on a product is a strong motivating factor

Pilot participants were strongly motivated to achieve certification in order to be able to place the IoT Security Assured badge on their product and marketing material. One participant was keen to take part on learning that they would be able to apply a badge to their products before their competitors. Two other participants, after having been notified they had passed the assessment, immediately asked for high-resolution image files of the badges so they could put them in marketing and incorporate in the latest packaging for their product.

❹ The IoT Security Assured question-set and online platform is fit for purposes, with some minor tweaks to wording and flow

The IoT Security Assured question set attempts to strike a balance between the necessary complexity of meeting the EN 303 645 requirements and the overriding need to make the questions simple to understand for applicants from manufacturers of all sizes and at all stages of product development.

Pilot participants gave positive feedback about the question set and the assessment process – all applicants rated the process as either easy or very easy overall, despite some describing the assessment as a "searching process".

One participant said that going through the question set helped them during their development stage by providing them with a checklist of the security measures that they needed to embed into their processes

There was minor feedback about the question set in terms of tweaks to question wording and the guidance provided alongside the questions. In some cases, questions were not applicable to a particular manufacturer's situation – for example, some manufacturers devices did not handle personal data and so it needed to be easier for applicants to express this and by-pass the particular questions relating to personal data.

Participants also wanted it to be easier to distinguish basic, silver and gold questions so that they could understand which topics to focus effort on in order to obtain the level of certification they desired. Also, a "not applicable" option with a notes field was needed for some of the yes/no questions to allow applicants to explain their particular situation to the assessor.

Some participants wanted access to an electronic copy of the questions before completing the application, to allow them to prepare for assessment. We have made these available as a spreadsheet and they will also be available as a booklet for the launch date. Both of these will be freely downloadable from the IASME website.

❺ Participants find supporting guidance and templates useful to achieve compliance

Participants requested additional help to comply through templates and guidance.

In particular, participants asked for a vulnerability disclosure policy template (which was created and released to them during the pilot), an information asset register template and data protection templates such as a data privacy impact assessment (DPIA) template. We will make these and other templates available to applicants after the launch of the scheme.

Assessors provided feedback that the participants needed targeted guidance particularly for those that lacked a technical understanding of security. In particular, they highlighted the need for guidance that is simple to understand and avoids the usage of technical language. IASME has found from operating other assurance schemes, that simple guidance can make a positive impact on assessment outcomes because it empowers the person applying for certification to ask searching questions of other members of their organisation and suppliers about technical topics.

❻ Defining the scope of certification can be complex

Defining scope is one of the most difficult tasks for all certification schemes and IASME has identified it as a key topic for both the Cyber Essentials and IASME Governance information assurance schemes.

The pilot found that scoping for IoT Security Assured was also complex. In most cases, it is simple to define what counts as "a device". But, the certification also encourages inclusion of device hubs, apps and associated cloud services within the scope. This introduces complexity because the boundaries of these additional areas are often unclear. However, there is likely to be a better outcome for security if a broader scope is encouraged.

❼ Completing the assessment requires both technical knowledge and organisational knowledge

The participants involved a number of people with different roles to complete the assessment.

The smaller companies initially involved their CEO and/or CTO in the initial conversations and then brought in product engineers to assist in the process. The larger companies involved product leads and security engineering teams in completing the assessment.

However, it was observed that there was a need to bring in additional people beyond the engineering and security teams in order to complete the elements of the assessment that related to policies, data protection and company processes.

The new online platform being used by IASME for the IoT Security Assured certification allows specific questions to be assigned to different people within an organisation to answer. We will be incorporating guidance into the scheme when launched to ensure applicants are aware of this option and the need to involve people across business areas in order to complete the assessment successfully.

8 Strong interest in certification from manufacturers who sell to business, as well as those that sell to consumers

The pilot focus was on certifying consumer IoT devices, based on the ETSI definition. This category is actually fairly broad and encompasses many types of connected devices. All of the devices on the pilot either had a consumer use or were targeted at the consumer market. Nonetheless, this did restrict the devices that could take part in the pilot.

When reviewing the responses to our request for volunteers, we found that, beyond consumer manufacturers, there was also strong interest in certification from:

- manufacturers of devices that have are mainly sold to other businesses (particularly those who manufacture devices such as environment and power usage sensors for installation in commercial buildings)
- manufacturers who sell connected devices for industrial usage (sometimes referred to as Industrial IoT or IIoT)

We were unable to include these types of devices in the pilot, but nonetheless we talked to these manufacturers and learned more about their motivation for volunteering, which was to prove the security of their devices to other businesses. This focus was about ensuring that the IoT components in an end-user business supply chain can be proven to be secure.

The current scheme is probably not appropriate for Industrial IoT devices, due to the specialist knowledge needed to assess this equipment and the different risk/threat model that is likely to apply to an industrial environment. However, the IoT Security Assured certification may well be suitable for the first category of manufacturers. In particular, many businesses are using consumer IoT devices within their offices and so many consumer devices are also in reality dual-usage "business IoT" devices too.

We believe that the initial demand for certification may come from business purchasers rather than consumers and this may an important element in the commercial viability of IoT device certification schemes before consumer legislation is implemented.

One of the manufacturers in the pilot produces sensor devices which are components of consumer IoT devices but do not directly handle user data. They have successfully certified to the IoT Security Assured standard, although we have taken on board feedback to make the data protection provisions of the standard flexible enough to encompass such devices that don't directly handle user data.

❾ 50 percent of participants want to certify additional devices

Many of the participants manufacture multiple connected devices and the feedback survey showed that around 50 percent of participants that achieved certification are planning to certify additional devices to the IoT Security Assured certification once it has been launched commercially.

This suggests that the participants found the process and/or the certification to be beneficial and would be prepared to pay for certifying additional devices. Also, many of the participants confirmed that they will renew the certification for the device involved in the pilot in 12 months time.

❿ Interest in a greater level of assurance beyond verified self-assessment

A number of participants asked about the availability of an additional level of assurance beyond the verified self-assessment and wanted to understand the next steps available to them.

IASME is developing a hands-on version of the standard that would allow manufacturers to prove the security of devices with greater confidence to purchasers whilst remaining affordable and accessible. The hands-on certification would require manufacturers to first achieve the verified self-assessment and then upgrade to the hands-on version which would involve additional documentation and a hands-on assessment of the device by the assessor.

Importantly, this level of certification would not involve an in-depth technical assessment, but would see the assessor examining the device from a user-perspective in a typical use environment. This would provide a significant additional level of assurance without a significant additional cost.