IoT Security Foundation

IoT Security Compliance Framework

Release 1.0

Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing

Notices

Documents published by the IoT Security Foundation ("IoTSF") are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org/

Terms of Use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organisation which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF's membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high quality guidance, IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, Trade Marks and Licensing

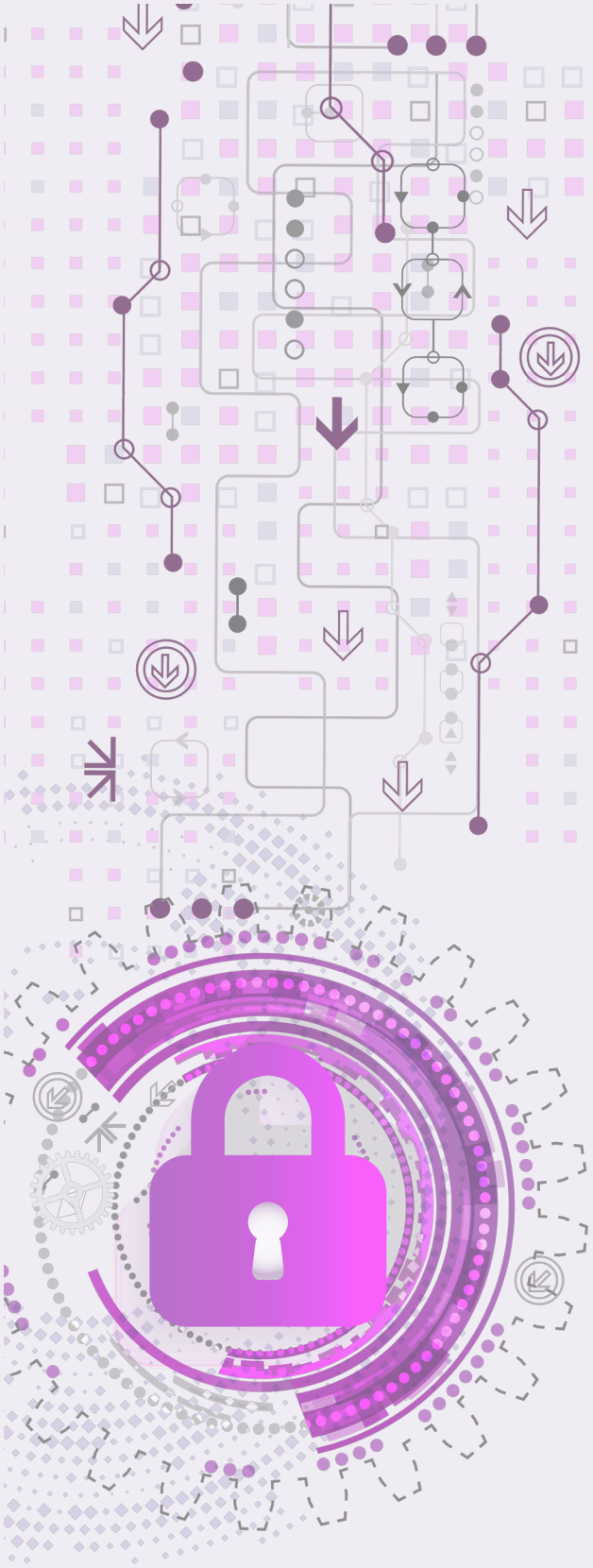
All product names are trade marks, registered trade marks, or service marks of their respective owners.

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members and external reviewers.

- Roland Atoui, Red Alert Labs
- Jeremy Bennett, Embecosm Ltd
- Simon Cook, Embecosm Ltd
- Paul Galwas, Digital Catapult Ltd
- Pamela Gupta, Outsecure Inc
- John Haine, University of Bristol
- Trevor Hall, DisplayLink Ltd
- Chris Hills, Phaedrus Systems Ltd
- Richard Marshall, Xitex Ltd
- John Moor, IoT Security Foundation
- Ken Munro, Pen Test Partners LLP
- Ian Phillips, Roke Manor Research Ltd
- Duncan Purves, Connect2 Systems Ltd
- Colin Robbins, Nexor Ltd
- David Rogers, Copper Horse Solutions Ltd
- Carl Shaw, MathEmbedded Ltd
- Roger Shepherd, Lujam Security Ltd
- Chris Shire, Infineon Technologies Ltd

- Colin Blanchard
- John Cowburn
- Thomas Detert



Contents

1 Intent and Purpose

In a hyper-connected digital world, insecurity is not an option. There is a wide spectrum of known and unknown consequences of poor security including personal inconvenience, financial fraud, industrial espionage and sabotage, national and physical security.

The mission of the IoT Security Foundation (IoTSF) ***"is to help secure the Internet of Things, in order to aid its adoption and maximise its benefits. To do this we will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems."*** The IoTSF is providing the tools for the industry to build an ***"a supply chain of trust".***

IoTSF advocates the core security values of ***security first, fitness of purpose and resilience*** to meet and maintain the necessary levels of trust for IoT system adoption and use.

The Executive Steering Board of IoTSF determined that the consumer and domestic IoT application domains presented acute security concerns, and there is a pressing and immediate need for best practice guidance – this is the sector targeted by "Release 1" of this document. This need is especially important for companies new to the connected product and service markets as they perceive a need to move quickly to gain market share. This is often accompanied with limited experience or awareness of the wider implications of weak security.

The IoT Security Compliance Framework is intended to help companies make high-quality, informed security choices by guiding users through a robust checklist and evidence gathering process. The evidence gathered during the process can be used to demonstrate conformance with best practice to customers and other organisations. Each use-case and intended operating environment will be different and so it is the responsibility of the company to determine the level of security measures applied to make their products fit-for-purpose.
Organisations that follow this process are exercising and demonstrating a duty of care towards their customers and other stakeholders in the IoT eco-system. It is generally agreed that by encouraging more organisations to adopt security best practices, a higher level of assurance and integrity benefits will be accrued. IoTSF therefore also advocates that customers of connected products, technologies and/or services specify security requirements consistent with contemporary best practice.

1.1 Overview

In this first release, The Internet of Things Security Foundation provides pragmatic guidance to businesses that are moving from standalone products, goods, and services; to devices and services that have network connectivity to enhance their functionality.

Businesses making the transition from standalone, self-contained devices and services to those that are network aware and network connected need to consider many technical and business process challenges. One of the imperatives is to make sure that their and their customer's security and privacy are not compromised.

Security best practice requires choices in design, features, implementation, testing, configuration and maintenance. There are a great many considerations including protocols, encryption, technology, software, API's, platforms and more. IoTSF is supplier and technology neutral; it provides guidance built upon security principles and the significant body of knowledge and standards that either already exist or are emerging. This Framework therefore guides the user by referencing existing materials where possible to accelerate the user's progress and understanding and to avoid unnecessary duplication. This Framework takes users through a structured line of question and evidence gathering to ensure the user derives suitable security mechanisms and practices which are appropriate for their business and/or application domain.

1.2 About the Framework

The Foundation provides a number of resources:

- **This document** is a checklist to guide an organisation through the assurance process and gather structured evidence to demonstrate conformance with best practice.
- Additional **Best Practice Guidelines** are provided by the Foundation to help understanding.
- Further background information is contained in linked **reference documents on the IoTSF website.**

The Framework has utility in a number of scenarios including:

1. Within a single organisation it can be used to plan, manage, review and document security practice during the development of products, systems or services. An organisation which uses the Framework may elect to declare so in its marketing to signal professional integrity and a "duty of care" to customers. IoTSF provides a user mark for organisations which follow its guidelines which can be used without cost at their discretion.
2. As part of the product/technology/service development process, an organisation may also apply the framework to assess the security posture of its own suppliers.
3. An organisation procuring products, systems and services from a supplier which declares it has used the Framework may audit the evidence assembled, using either internal resources or a Trusted Third Party ("T3P"). A T3P might be used in situations where the documented evidence would expose sensitive information such as intellectual property or commercial aspects.
4. In future, it is also envisaged that an audit process could lead to the Framework-user being permitted to use a "Trust Mark" as a qualified public symbol of conformance to best practice.

1.3 Intended audience

Most functions in a company making, producing and supplying IoT products or services play a role in and have a measure of responsibility for security. An executive board member, for example the CISO if there is one, should have overall authority for establishing and maintaining security.

This document is aimed at the following readers:

- For Managers in organisations that provide IoT products, technology and or services; it gives a comprehensive overview of the management process needed to follow best practice. As such it will be useful for executive, programme and project managers, enabling them to ask the right questions and judge the answers.
- For Developers and Engineers, Logistics and Manufacturing Staff, it provides a detailed checklist to use in their daily work and in project reviews to validate the use of best practice by different functions (e.g. hardware and software development, logistics etc.). In completing the checklist, documentary evidence will be compiled that can be used to demonstrate compliance both at product gates and with third parties such as customers.
- For Supply Chain Managers, the structure can be used to guide the auditing of security practices. It may therefore be applied within the producer organisation (as described above); by a customer of the producer; or a Trusted Third Party auditor.

1.4 Scope

Security in IoT is constantly changing. To accommodate changes and additions to the Framework, IoTSF operates a system based on releases to meet evolving application needs.

The compliance scheme is based on risk profiles [ref 12], and these will vary by system and intended operational environment. The most stringent risk profile should be adopted wherever possible, considering not just the immediate context of the product but extend to the use of the data that the device generates and to other system(s) the product may eventually be connected to.

The scope of this document includes (but is not limited to):

- Business processes
- Devices and aggregation points such as related gateways/hubs that form part of the connectivity
- Networking including wired, and radio connections using both short-range, LPWA and cellular
- Cloud and server elements as specific to IoT.

1.4.1 Open Items and Release Status

This "Release 1" of the Framework is limited to commercial products intended to be owned/used/operated by the consumer in a domestic setting. This release is the first public release and whilst intended for adoption, feedback is welcome on this Framework as part of its evolution and dealing with new security threats. Future releases will to cover additional product categories, with the next release is expected to be made during the 1st half of 2017.

Open Items for this release:

- Testing – future releases will cover penetration testing
- Transfer of ownership for IoT devices and sensitive data lifecycle management
- Reporting in the event of the detection of any hacking attempts being made on a device and any resultant management actions
- Expansion of the sections on web user interfaces and mobile applications to include requirements for such attacks as cross site scripting and SQL injection etc.

1.4.2 Application/Domain/Product Categorisation

The security requirements may vary according to the context in which a given product is used. Products and services are typically designed for a primary application use and intended market and operating environment. However, products and services may, intentionally or unintentionally, get used in different application environments by their users. When used outside the expected context, the security may not be adequate. This challenges the notion of best practice as the intended use case influences the appropriate security mechanisms[1].

The following application and product categories and their compliance requirements are currently defined.

A	Consumer (Domestic)
B	Enterprise
C	Industrial
D	Medical
E	Automotive
F	Public Agency
G	Critical National Infrastructure

Release 1 of this document is limited to Category A.

1 To illustrate this point, a connected thermostat designed for use in a domestic dwelling may end up being used to monitor and control temperature in a horticultural glasshouse where the economic consequences of a security breach to the grower may be significantly more adverse.

1.5 Roles and Responsibilities

The Executive Management of a company is responsible for oversight of Security in its products and operations, and therefore for adoption of this document. It needs to endorse the mission, charter and authority of a Security function which is responsible for security compliance. If there is no formal Information Security role in the Executive, a board member should be assigned the role. A director or board member should sign off conformance with the Compliance Framework.

2 Using the Checklist

2.1 The Process

The compliance process is guided by determining the category of product and the class of compliance applicable to the product in this section and then the responses captured in the questionnaire in Section 3.

The questionnaire elicits a set of responses to security requirements for aspects of the organisation and product. Each question needs to be confirmed, with evidence to support compliance with the requirement. Alternatively, if the requirement is deemed to be not applicable, an explanation must be provided as to why.

The documented requirements checklist and evidence file must be retained.

2.2 Compliance Class

In order to apply an appropriate level of security compliance to a product, the requirements that are listed in the questionnaire have their applicability determined from being classified into one of the following compliance classes:

Class 0: where compromise to the data generated or level of control provided is likely to result in little discernible impact on an individual or organisation.

Class 1: where compromise to the data generated or level of control provided is likely to result in no more than limited impact on an individual or organisation.

Class 2: in addition to class 1, the device is designed to resist attacks on availability that would have significant impact an individual or organisation, or impact many individuals, for example by limiting operations of an infrastructure to which it is connected.

Class 3: in addition to class 2, the device is designed to protect sensitive data including sensitive personal data.

Class 4: in addition to class 3, where the data generated or level of control provided or in the event of a security breach have the potential to affect critical infrastructure or cause personal injury.

For each compliance class, the levels of integrity, availability and confidentiality are shown in the Table 1 below.

Compliance Class	Security Objective		
	Integrity	Availability	Confidentiality
Class 0	Basic	Basic	Basic
Class 1	Medium	Medium	Basic
Class 2	Medium	High	Medium
Class 3	Medium	High	High
Class 4	High	High	High

Table 1: Compliance Class Security Objectives

Where the definitions of the levels of integrity, availability and confidentiality are as follows:

- Integrity
  - Basic - devices resist low level threat sources that have very little capability and priority
  - Medium - devices resist medium level threat sources that have from very little, focussed capability, through to researchers with significant capability
  - High - devices resist substantial level threat sources
- Availability
  - Basic - devices whose lack of availability would cause minor disruption
  - Medium – devices whose lack of availability would have limited impact on an individual or organisation
  - High – devices whose lack of availability would have significant impact to an individual or organisation, or impacts many individuals
- Confidentiality
  - Basic – devices processing public information
  - Medium – devices processing sensitive information, including Personally Identifiable Information, whose compromise would have limited impact on an individual or organisation
  - High - devices processing very sensitive information, including sensitive personal data whose compromise would have significant impact on an individual or organisation.

References 11, 12, 13, 14 & 15 were used as the basis of the definitions above.

2.3 Category Compliance Applicability

For each product category (only Category A in this release), a column defines the level of recommended compliance with the class of the requirement of the corresponding row. The applicability levels are defined as follows.

Mandatory	This requirement shall be met as it is vital to secure the product category.
Advisory	This requirement should be met unless there are sound product reasons (e.g. economic viability, hardware complexity). The reasons for deviating from the requirement should be documented.

In the following tables, the category applicability applies to all level 1 compliance classes. However, where table shows a “2 and above” compliance class, this means that the requirement is mandatory for all other levels i.e. 2, 3 & 4.

2.3.1 Compliance Applicability - Business Security Processes and Responsibility

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.1.1	There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	1 and above	M	TBD in future release
2.3.1.2	There is a person or role, who takes ownership for adherence to this compliance checklist process.	1 and above	M	TBD in future release
2.3.1.3	There are documented business processes in place for security.	1 and above	M	TBD in future release
2.3.1.4	The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework etc.).	2 and above	A	TBD in future release
2.3.1.5	A policy has been established for dealing with both internal and third party security research on the products or services.	1 and above	M	TBD in future release
2.3.1.6	A security policy has been established for addressing changes, such as vulnerabilities, that could impact security and affect or involve technology or components incorporated into the product or service provided.	2 and above	A	TBD in future release
2.3.1.7	Processes and plans are in place based upon the IoTSF "Vulnerability Disclosure Guidelines" or similar recognised process to deal with the identification of a security vulnerability or compromise when they occur.	1 and above	M	TBD in future release
2.3.1.8	A process is in place for consistent briefing of senior executives in the event of the identification of a vulnerability or a security breach, especially those who may deal with the media or make public announcements. In particular that any public statements made in the event of a security breach, should give as full and accurate account of the facts as possible.	1 and above	M	TBD in future release
2.3.1.9	There is a secure notification process based upon the IoTSF "Vulnerability Disclosure Guidelines" or similar recognised process, for notifying partners/ users of any security updates.	1 and above	M	TBD in future release
2.3.1.10	A security threat and risk assessment shall have been carried out using a standard methodology such as Octave, NIST RMF or NCSC [ref12] to determine the risks and evolving threats.	2 and above	A	TBD in future release

2.3.2 Compliance Applicability - Device Hardware & Physical Security

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.2.1	The product's processor system has an irrevocable hardware secure boot process.	2 and above	A	TBD in future release
2.3.2.2	The secure boot process is enabled by default.	2 and above	A	TBD in future release
2.3.2.3	Any debug interface, for example related I/O port(s) such as JTAG, is secured on the production devices.	2 and above	A	TBD in future release
2.3.2.4	The hardware incorporates physical protection against tampering and reverse engineering and this has been enabled.	2 and above	A	TBD in future release
2.3.2.5	All communications port(s), such as USB, RS232 etc., which are not used as part of the product's normal operation are not physically accessible or are secured on the production devices.	2 and above	A	TBD in future release
2.3.2.6	After manufacture all the product's test points are secured so that they cannot be used to breach the integrity and/or confidentiality of the product.	2 and above	A	TBD in future release
2.3.2.7	Tamper Evident measures have been used to identify any interference to the assembly.	2 and above	A	TBD in future release
2.3.2.8	Tamper Resistant measures have been used to reduce the attack surface.	3 and above	A	TBD in future release

2.3.3 Compliance Applicability - Device Application

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.3.1	The product has measures to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/or sandbox.	1 and above	M	TBD in future release
2.3.3.2	Where remote software upgrade can be supported by the device, when vulnerabilities are discovered, the software fix for the device is promptly made available.	2 and above	A	TBD in future release
2.3.3.3	Where remote software upgrade can be supported by the device, the software images are digitally signed by an authorised trust entity.	1 and above	M	TBD in future release

2.3.3.4	A software update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.	1 and above	M	TBD in future release
2.3.3.5	If remote software upgrade is supported by a device, software images shall be encrypted whilst being transferred to it.	2 and above	A	TBD in future release
2.3.3.6	If the product has any port(s) that are not required for normal operation, they are securely disabled when shipped. Where a port is used for field diagnostics, the port input is deactivated and the output provides no information which could compromise the device.	2 and above	A	TBD in future release
2.3.3.7	To prevent the stalling or disruption of the devices software operation any watchdog timers for this purpose cannot be disabled.	2 and above	A	TBD in future release
2.3.3.8	The product's software signing root of trust is stored in tamper-resistant memory.	1 and above	M	TBD in future release
2.3.3.9	The product has protection against reverting the software to an earlier and potentially less secure version.	2 and above	A	TBD in future release
2.3.3.10	The cryptographic key chain used for signing production software is different from that used for any other test, development or other software images, to prevent the installation of non-production software onto production devices.	2 and above	A	TBD in future release
2.3.3.11	All functionality used only in development (e.g. debug data or complier information etc.) is securely disabled or removed from production software images.	2 and above	A	TBD in future release
2.3.3.12	Development software versions have any debug functionality switched off if the software is operated on the product outside of the product vendors' trusted environment.	2 and above	A	TBD in future release
2.3.3.13	Steps have been taken to protect the products' software from information leakage and side-channel attacks.	2 and above	A	TBD in future release
2.3.3.14	The product's software source code follows the basic good practice of a Language subset (e.g. MISRA-C) coding standard.	2 and above	A	TBD in future release
2.3.3.15	The product's software source code follows the basic good practice of static vulnerability analysis.	2 and above	A	TBD in future release
2.3.3.16	Sensitive software components such as cryptographic processes are isolated or of higher privilege than other software components.	1 and above	M	TBD in future release
2.3.3.17	Software source code is developed, tested and maintained following defined repeatable processes.	2 and above	A	TBD in future release

2.3.3.18	The build environment and toolchain used to compile the application is run on a build system with controlled and auditable access.	2 and above	A	TBD in future release
2.3.3.19	The build environment and toolchain used to create the software is under configuration management and version control, and its integrity is validated regularly.	2 and above	A	TBD in future release
2.3.3.20	The production software signing keys are under access control.	1 and above	M	TBD in future release
2.3.3.21	The production software signing keys are stored and secured in a storage device compliant to FIPS-140 level 2, or equivalent or higher standard.	2 and above	A	TBD in future release
2.3.3.22	Where the device software communicates with a product related webserver or application over TCP/IP or UDP/IP, the device software uses certificate pinning or public/private key equivalent, where appropriate.	2 and above	M	TBD in future release
2.3.3.23	The device remains secure and maintains state during a side channel attack.	2 and above	A	TBD in future release
2.3.3.24	All inputs and outputs are checked for validity.	2 and above	M	TBD in future release
2.3.3.25	The software has been designed to fail safely.	2 and above	A	TBD in future release

2.3.4 Compliance Applicability - Device Operating System

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.4.1	The operating system is implemented with the most current patches prior to release.	2 and above	A	TBD in future release
2.3.4.2	Where remote update is supported, there is an established process/plan for validating and updating patches on an on-going or remedial basis.	2 and above	A	TBD in future release
2.3.4.3	All interactive operating system accounts or logins have been disabled or eliminated from the software.	2 and above	A	TBD in future release
2.3.4.4	Files and directories are set to appropriate access privileges on a need to access basis.	2 and above	A	TBD in future release

2.3.4.5	Passwords file(s) are owned by and are only accessible to and writable by the most privileged account.	1 and above	M	TBD in future release
2.3.4.6	All OS non-essential services have been removed from the products' software image or file systems.	2 and above	A	TBD in future release
2.3.4.7	All OS command line access to the most privileged accounts has been removed from the operating system.	2 and above	A	TBD in future release
2.3.4.8	The product's OS kernel and its functions are prevented from being called by external product level interfaces and unauthorised applications.	1 and above	M	TBD in future release
2.3.4.9	Applications are operated at the lowest privilege level possible.	2 and above	A	TBD in future release
2.3.4.10	All the applicable security features supported by the OS are enabled.	1 and above	M	TBD in future release
2.3.4.11	The OS is separated from the application(s) and is only accessible via defined secure interfaces.	2 and above	A	TBD in future release

2.3.5 Compliance Applicability - Device Wired and Wireless Interfaces

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.5.1	The product prevents unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.	1 and above	M	TBD in future release
2.3.5.2	For products with multiple network interfaces, the uncontrolled ability to forward IP packets between the interfaces is disabled.	1 and above	M	TBD in future release
2.3.5.3	IP Traffic uses only secure protocols with no publically known vulnerabilities, such as TLS or (D)TLS. Insecure and plaintext application layer protocols (such as ICMPv4, TELNET, FTP, HTTP, SMTP and NTP) are not used.	1 and above	M	TBD in future release
2.3.5.4	All the products' unused ports are closed and the minimal required number of ports are active.	1 and above	M	TBD in future release
2.3.5.5	If a connection requires a password or passcode or passkey for connection authentication, the default password or factory reset password is unique to each device. Examples are WiFi access passwords and Bluetooth PINS.	1 and above	M	TBD in future release

2.3.5.6	Where a wireless interface has an initial pairing process, the passkeys are changed from the default prior to providing normal service.	1 and above	M	TBD in future release
2.3.5.7	For any WiFi connection, WPA2 with AES or a similar strength encryption has been used and insecure protocols such as WPA and TKIP are disabled.	1 and above	M	TBD in future release
2.3.5.8	Where WPA2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	1 and above	M	TBD in future release
2.3.5.9	All network communications keys are stored securely.	1 and above	M	TBD in future release
2.3.5.10	Where the MQTT protocol is used, it is protected by a TLS connection with no known cipher vulnerabilities.	1 and above	M	TBD in future release
2.3.5.11	Where the CoAP protocol is used, it is protected by a DTLS connection with no known cipher vulnerabilities.	1 and above	M	TBD in future release
2.3.5.12	Where cryptographic suites are used such as TLS, all cipher suites shall be listed and validated against the current security recommendations such as NIST 800-131A [ref 2] or OWASP, for example using ephemeral key generation and authenticating encrypting ciphers such as AES-GCM. Where insecure ciphers suites are identified they shall be removed from the product.	1 and above	M	TBD in future release
2.3.5.13	All use of cryptography by the product, such as TLS cipher suites, shall be listed and validated against the import/export requirements for the territories where the product is to be sold and/or shipped.	1 and above	M	TBD in future release
2.3.5.14	Where there is a loss of communications it shall not compromise the integrity of the device.	2 and above	A	TBD in future release
2.3.5.15	The product only enables the protocols necessary for the products' normal operation.	1 and above	M	TBD in future release

2.3.6 Compliance Applicability - Authentication and Authorisation

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.6.1	The product contains a unique and tamperproof hardware identifier (e.g. such as the chip serial number or other unique silicon identifier) which is used for binding code and data to a specific device hardware.	2 and above	A	TBD in future release

2.3.6.2	Where the product includes a real time clock, it has a method of validating its integrity, if it is necessary for the security of the product.	2 and above	A	TBD in future release
2.3.6.3	Where a user interface password is used for login authentication, the default password or factory reset password is unique to each device in the product family.	1 and above	M	TBD in future release
2.3.6.4	The product does not accept the use of null or blank passwords.	1 and above	M	TBD in future release
2.3.6.5	The product will not allow new passwords containing the user account name with which the user account is associated.	1 and above	M	TBD in future release
2.3.6.6	The product/system enforces passwords to be compliant with CPNI Password Guidance [ref 10] or similar recommendations on: password length, characters from the groupings and special characters.	1 and above	M	TBD in future release
2.3.6.7	The product has defence against brute force repeated login attempts.	1 and above	M	TBD in future release
2.3.6.8	The product securely stores any passwords using an industry standard cryptographic algorithm.	1 and above	M	TBD in future release
2.3.6.9	The product supports access control measures to the root account to restrict access to sensitive information or system processes.	1 and above	M	TBD in future release
2.3.6.10	The access control privileges are defined, justified and documented.	2 and above	A	TBD in future release
2.3.6.11	The product only allows controlled user account access; access using anonymous or guest user accounts are not supported without justification.	1 and above	M	TBD in future release
2.3.6.12	The product allows the factory default or OEM login accounts to be disabled or erased or renamed.	2 and above	A	TBD in future release
2.3.6.13	The product supports having any or all of the factory default user login passwords, altered prior to installation.	1 and above	M	TBD in future release
2.3.6.14	If the product has a password recovery or reset mechanism, an assessment has been made to confirm that this mechanism cannot readily be abused by an unauthorised party.	1 and above	M	TBD in future release
2.3.6.15	Where passwords are entered on a user interface, the actual pass phrase is obscured by default.	1 and above	M	TBD in future release
2.3.6.16	The product allows an authorised factory reset of the device's authorisation information.	2 and above	A	TBD in future release

2.3.7 Compliance Applicability - Encryption and Key Management for Hardware

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.7.1	A true random number generator source is exclusively used for all relevant cryptographic operations including nonce, initialisation vector and key generation algorithms.	2 and above	A	TBD in future release
2.3.7.2	The true random number generator source has been validated for true randomness using an NIST SP800-22 [ref 4], FIPS 140-2 [ref 5] or similar compliance process.	2 and above	A	TBD in future release
2.3.7.3	There is a process for secure provisioning of keys that includes generation, distribution, revocation and destruction. For example in compliance with FIPS140-2 [ref 5] or similar process.	2 and above	A	TBD in future release
2.3.7.4	There is a secure method of key insertion that protects keys against copying.	1 and above	M	TBD in future release
2.3.7.5	All the product related cryptographic functions have no publicly known weaknesses, for example MD5 and SHA-1 are not used, e.g. those stipulated in NIST SP800-131A [ref 2].	1 and above	M	TBD in future release
2.3.7.6	The product stores all sensitive unencrypted parameters, e.g. keys, in a secure, tamper proof location.	1 and above	M	TBD in future release
2.3.7.7	The cryptographic key chain used for signing production software is different from that used for any other test, development or other software images, to prevent the installation of non-production software into production devices.	2 and above	A	TBD in future release
2.3.7.8	In device manufacture all asymmetric encryption private keys that are unique to each device are either securely and truly randomly internally generated or securely programmed into each device.	2 and above	A	TBD in future release

2.3.8 Compliance Applicability - Web User Interface

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.8.1	Where the product or service provides a web based interface, strong user authentication is used.	2 and above	A	TBD in future release
2.3.8.2	Where the product or service provides a web based management interface, strong mutual authentication is used.	2 and above	A	TBD in future release

2.3.8.3	Where a web user interface password is used for login authentication, the default password or factory reset password is unique to each device in the product family.	1 and above	M	TBD in future release
2.3.8.4	The web user interface is protected by automatic session/logout timeout function.	1 and above	M	TBD in future release
2.3.8.5	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	1 and above	M	TBD in future release
2.3.8.6	The web user interface shall follow good practice guidelines, such as those listed in the OWASP top 10 attacks (https://www.owasp.org).	1 and above	M	TBD in future release
2.3.8.7	A vulnerability assessment has been performed before deployment and on an ongoing basis afterwards.	1 and above	M	TBD in future release
2.3.8.8	All inputs and outputs are validated using for example a whitelist.	1 and above	M	TBD in future release

2.3.9 Compliance Applicability - Mobile Application

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.9.1	Where an application's user interface password is used for login authentication, the default password or factory reset password is unique to each device in the product family.	1 and above	M	TBD in future release
2.3.9.2	Password entry follows the recommendations of 3GPP TS33.117.	2 and above	A	TBD in future release
2.3.9.3	The mobile application stores the minimum required amount of personal information from users.	2 and above	A	TBD in future release
2.3.9.4	The mobile application ensures that all personal user data is encrypted at rest and in transit.	2 and above	A	TBD in future release
2.3.9.5	The mobile application ensures that any related databases or files are either tamper resistant or restricted in their access. Upon detection of tampering of the databases or files they are re-initialised.	1 and above	M	TBD in future release
2.3.9.6	Where the application communicates with a product related remote server(s) or device it does so over a secure connection such as a TLS connection using certificate pinning.	1 and above	M	TBD in future release
2.3.9.7	The product securely stores any passwords using an industry standard cryptographic algorithm.	1 and above	M	TBD in future release

2.3.10 Compliance Applicability – Privacy

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.10.1	The product/service stores the minimum amount of personal information from users.	1 and above	M	TBD in future release
2.3.10.2	The product/service ensures that all personal user data is encrypted at rest and in transit.	1 and above	M	TBD in future release
2.3.10.3	The product/service ensures that only authorised personnel have access to personal data of users.	1 and above	M	TBD in future release
2.3.10.4	The product/service ensures that personal data is anonymised whenever possible and in particular in any reporting.	1 and above	M	TBD in future release
2.3.10.5	The product/service ensures the controlling organisation has a data retention policy in place.	1 and above	M	TBD in future release
2.3.10.6	There is a method or methods for the product owner to be informed about what data is collected, why, where it will be stored.	1 and above	M	TBD in future release
2.3.10.7	There is a method or methods for the product owner to check/verify what data is collected and deleted.	1 and above	M	TBD in future release
2.3.10.8	The product/service can be made compliant with the local and/or regional data protection legislation where the product is to be sold.	1 and above	M	TBD in future release

2.3.11 Compliance Applicability – Cloud and Network Elements

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.11.1	All the product related cloud and network elements have the latest operating system(s) security patches implemented and processes are in place to keep them updated.	2 and above	A	TBD in future release
2.3.11.2	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.	1 and above	M	TBD in future release
2.3.11.3	All product related web servers have their webserver HTTP trace and trace methods disabled.	1 and above	M	TBD in future release

2.3.11.4	All the product related web servers' TLS certificate(s) are signed by trusted certificate authorities; are within their validity period; and processes are in place for their renewal.	1 and above	M	TBD in future release
2.3.11.5	All the product related web servers use protocols with no publicly known weaknesses.	1 and above	M	TBD in future release
2.3.11.6	The product related web servers have low and medium strength TLS ciphers disabled.	2 and above	A	TBD in future release
2.3.11.7	The product related web servers have repeated renegotiation of TLS connections disabled.	1 and above	M	TBD in future release
2.3.11.8	The related servers have unused IP ports disabled.	1 and above	M	TBD in future release
2.3.11.9	Where a product related to a webserver encrypts communications using TLS and requests a client certificate, the server(s) only establishes a connection if the client certificate and its chain of trust are valid.	2 and above	A	TBD in future release
2.3.11.10	Where a product related to a webserver encrypts communications using TLS, certificate pinning is implemented. For example, using OWASP https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning or similar organisations' certificate and public key pinning guidance.	2 and above	A	TBD in future release
2.3.11.11	All the related servers and network elements prevent the use of null or blank passwords.	1 and above	M	TBD in future release
2.3.11.12	The cloud and network elements follow the password requirements of section 2.3.6.	1 and above	A	TBD in future release
2.3.11.13	All the related servers and network elements prevent new passwords from containing the user account name, with which the user account is associated.	1 and above	M	TBD in future release
2.3.11.14	All the related servers and network elements enforce passwords to include: at least eight characters in length; characters from the groupings: alpha, numeric, and special characters and shall not be vulnerable to dictionary attack.	1 and above	M	TBD in future release
2.3.11.15	The maximum permissible number of consecutive failed user account login attempts follows the recommendations of 3GPP TS33.117.	2 and above	M	TBD in future release
2.3.11.16	All the related servers and network elements store any passwords using a cryptographic implementation using industry standard cryptographic algorithms.	1 and above	M	TBD in future release

2.3.11.17	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	1 and above	M	TBD in future release
2.3.11.18	All the related and network elements servers prevent anonymous/guest access except for read only access to public information.	1 and above	M	TBD in future release
2.3.11.19	If run as a cloud service, the service meets industry standard Cloud Security principles such as the Cloud Security Alliance, NIST or UK Government Cloud Security Principles.	2 and above	A	TBD in future release

2.3.12 Compliance Applicability – Secure Supply Chain and Production

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.12.1	The product has all of the test and calibration software used during manufacture erased or removed before the product is dispatched from the factory.	2 and above	A	TBD in future release
2.3.12.2	In manufacture, all encryption keys that are unique to each device are either securely and truly randomly internally generated or securely programmed into each device. Any secret key programmed into a product at manufacture is unique to that individual device, i.e. no global secret key is shared between multiple devices.	2 and above	A	TBD in future release
2.3.12.3	In manufacture, all the devices are logged by the product vendor, so that cloned or duplicated devices can be identified and either disabled or prevented from being used with the system.	1 and above	M	TBD in future release
2.3.12.4	The production system for a device has a process to detect any devices with duplicate serial numbers to ensure that any devices with duplicate serial numbers are not shipped and are either reprogrammed or destroyed.	1 and above	M	TBD in future release
2.3.12.5	Where a product includes a trusted secure boot process, the entire production test and any related calibration is executed with the processor system operating in its secured boot, authenticated software mode.	2 and above	A	TBD in future release
2.3.12.6	A securely controlled area is used for device provisioning when the production facility is untrusted.	2 and above	A	TBD in future release

2.3.13 Compliance Applicability – Configuration

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.3.13.1	The configuration of the implementation or the device and any related web services is tamper resistant.	1 and above	M	TBD in future release

3 Certification Questionnaire

3.1 Business Security Processes and Responsibility

Please confirm and verify with evidence (to be supplied) that the business processes and responsibility supporting the product/service comply with the following requirements. Each response should be selected from the following: “Compliant” [C]; “Partially Compliant” [P]; “Non-compliant” [N]:

Req. No	Requirement	Compliance Class	Response	Evidence
3.1.1	There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	1 and above	C/ PC/ N	<link to evidence>
3.1.2	There is a person or role, who takes ownership for adherence to this compliance checklist process.	1 and above	C/ PC/ N	<link to evidence>
3.1.3	There are documented business processes in place for security.	1 and above	C/ PC/ N	<link to evidence>
3.1.4	The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework etc.).	2 and above	C/ PC/ N	<link to evidence>
3.1.5	A policy has been established for dealing with both internal and third party security research on the products or services.	1 and above	C/ PC/ N	<link to evidence>
3.1.6	A security policy has been established for addressing changes, such as vulnerabilities, that could impact security and affect or involve technology or components incorporated into the product or service provided.	2 and above	C/ PC/ N	<link to evidence>
3.1.7	Processes and plans are in place based upon the IoTSF “Vulnerability Disclosure Guidelines” or similar recognised process to deal with the identification of a security vulnerability or compromise when they occur.	1 and above	C/ PC/ N	<link to evidence>

3.1.8	A process is in place for consistent briefing of senior executives in the event of the identification of a vulnerability or a security breach, especially those who may deal with the media or make public announcements.	1 and above	C/ PC/ N	<link to evidence>
3.1.9	There is a secure notification process based upon the IoTSF "Vulnerability Disclosure Guidelines" or similar recognised process, for notifying partners/users of any security updates.	1 and above	C/ PC/ N	<link to evidence>
3.1.10	A security threat and risk assessment shall have been carried out using a standard methodology such as Octave, NIST RMF or NCSC [ref12] to determine the risks and evolving threats.	2 and above	C/ PC/ N	<link to evidence>

3.2 Device Hardware & Physical Security

Please confirm and verify with evidence (to be supplied) that the physical elements of the product/ system meet the following requirements:

Req. No	Requirement	Compliance Class	Response	Evidence
3.2.1	The product's processor system has an irrevocable hardware secure boot process.	2 and above	C/ PC/ N	<link to evidence>
3.2.2	The secure boot process is enabled by default.	2 and above	C/ PC/ N	<link to evidence>
3.2.3	Any debug interface, for example related I/O port(s) such as JTAG, is secured on the production devices.	2 and above	C/ PC/ N	<link to evidence>
3.2.4	The hardware incorporates physical protection against tampering and reverse engineering and this has been enabled.	2 and above	C/ PC/ N	<link to evidence>
3.2.5	All communications port(s), such as USB, RS232 etc., which are not used as part of the product's normal operation are not physically accessible or are secured on the production devices.	2 and above	C/ PC/ N	<link to evidence>
3.2.6	After manufacture, all the product's test points are secured so that they cannot be used to breach the integrity and/or confidentiality of the product.	2 and above	C/ PC/ N	<link to evidence>
3.2.7	Tamper evident measures have been used to identify any interference to the assembly.	2 and above	C/ PC/ N	<link to evidence>
3.2.8	Tamper resistant measures have been used to reduce the attack surface.	3 and above	C/ PC/ N	<link to evidence>

3.3 Device Software

Please confirm and verify with evidence (to be supplied) that the software elements of the product meet the following requirements:

3.3.1 Device Application

Req. No	Requirement	Compliance Class	Response	Evidence
3.3.1.1	The product has measures to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/or sandbox.	1 and above	C/ PC/ N	<link to evidence>
3.3.1.2	Where remote software upgrade can be supported by the device, when vulnerabilities are discovered, the software fix for the device is promptly made available.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.3	Where remote software upgrade can be supported by the device, the software images are digitally signed by an authorised trust entity.	1 and above	C/ PC/ N	<link to evidence>
3.3.1.4	A software update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.	1 and above	C/ PC/ N	<link to evidence>
3.3.1.5	If remote software upgrade is supported by a device, software images shall be encrypted whilst being transferred to it.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.6	If the product has any port(s) that are not required for normal operation, they are securely disabled when shipped. Where a port is used for field diagnostics, the port input is deactivated and the output provides no information which could compromise the device.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.7	To prevent the stalling or disruption of the devices software operation, any watchdog timer for this purpose cannot be disabled.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.8	The product's software signing root of trust is stored in tamper-resistant memory.	1 and above	C/ PC/ N	<link to evidence>
3.3.1.9	The product has protection against reverting the software to an earlier and potentially less secure version.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.10	The cryptographic key chain used for signing production software is different from that used for any other test, development or other software images, to prevent the installation of non-production software onto production devices.	2 and above	C/ PC/ N	<link to evidence>

3.3.1.11	All functionality used only in development (e.g. debug data or complier information etc.) is securely disabled or removed from production software images.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.12	Development software versions have any debug functionality switched off if the software is operated on product outside the product vendors' premises.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.13	Steps have been taken to protect the products' software from information leakage and side-channel attacks.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.14	The product's software source code follows the basic good practice of a Language subset (e.g. MISRA-C) coding standard.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.15	The product's software source code follows the basic good practice of static vulnerability analysis.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.16	Sensitive software components such as cryptographic processes are isolated or of higher privilege than other software components.	1 and above	C/ PC/ N	<link to evidence>
3.3.1.17	Software source code is developed, tested and maintained following defined repeatable processes.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.18	The build environment and toolchain used to compile the application is run on a build system with controlled and auditable access.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.19	The build environment and toolchain used to create the software is under configuration management and version control, and its integrity is validated regularly.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.20	The production software signing keys are under access control.	1 and above	C/ PC/ N	<link to evidence>
3.3.1.21	The production software signing keys are stored and secured in a storage device compliant to FIPS-140 level 2, or equivalent or higher standard.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.22	Where the device software communicates with a product related webserver or application over TCP/IP or UDP/IP, the device software uses certificate pinning or public/private key equivalent, where appropriate.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.23	The device remains secure and maintains state during a side channel attack.	2 and above	C/ PC/ N	<link to evidence>
3.3.1.24	All inputs and outputs are checked for validity.	2 and above	C/ PC/ N	<link to evidence>

3.3.1.25	The software has been designed to fail safely.	2 and above	C/ PC/ N	<link to evidence>

3.3.2 Device Operating System

Where an RTOS or operating system has been incorporated into the device firmware, please confirm and verify with evidence (to be supplied) that the operating system of the products' firmware meets the following requirements:

Req. No	Requirement	Compliance Class	Response	Evidence
3.3.2.1	The operating system is implemented with the most current security patches prior to release.	2 and above	C/ PC/ N	<link to evidence>
3.3.2.2	Where remote update is supported, there is an established process/plan for validating and updating patches on an on-going or remedial basis.	2 and above	C/ PC/ N	<link to evidence>
3.3.2.3	All interactive operating system accounts or logins have been disabled or eliminated from the software.	2 and above	C/ PC/ N	<link to evidence>
3.3.2.4	Files and directories are set to appropriate access privileges on a need to access basis.	2 and above	C/ PC/ N	<link to evidence>
3.3.2.5	Passwords file(s) are owned by and are only accessible to and writable by the most privileged account.	1 and above	C/ PC/ N	<link to evidence>
3.3.2.6	All OS non-essential services have been removed from the products' software image or filesystems.	2 and above	C/ PC/ N	<link to evidence>
3.3.2.7	All OS command line access to the most privileged accounts has been removed from the operating system.	2 and above	C/ PC/ N	<link to evidence>
3.3.2.8	The product's OS kernel and its functions are prevented from being called by external product level interfaces and unauthorised applications.	1 and above	C/ PC/ N	<link to evidence>
3.3.2.9	Applications are operated at the lowest privilege level possible.	2 and above	C/ PC/ N	<link to evidence>
3.3.2.10	All the applicable security features supported by the OS are enabled.	1 and above	C/ PC/ N	<link to evidence>
3.3.2.11	The OS is separated from the application(s) and is only accessible via defined secure interfaces.	2 and above	C/ PC/ N	<link to evidence>

3.4 Device Wired & Wireless Network Interfaces

Please confirm and verify with evidence (to be supplied) that the device network interfaces (whether wired or wireless) of the product/service meet the following requirements:

Req. No	Requirement	Compliance Class	Response	Evidence
3.4.1	The product prevents unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.	1 and above	C/ PC/ N	<link to evidence>
3.4.2	For products with multiple network interfaces, the uncontrolled ability to forward IP packets between the interfaces is disabled.	1 and above	C/ PC/ N	<link to evidence>
3.4.3	IP Traffic uses only secure protocols with no publically known vulnerabilities, such as TLS or (D)TLS. Insecure and plaintext application layer protocols (such as ICMPv4, TELNET, FTP, HTTP, SMTP and NTP) are not used.	1 and above	C/ PC/ N	<link to evidence>
3.4.4	All the products' unused ports are closed and the minimal required number of ports are active.	1 and above	C/ PC/ N	<link to evidence>
3.4.5	If a connection requires a password or passcode or passkey for connection authentication, the default password or factory reset password is unique to each device. Examples are WiFi access passwords and Bluetooth PINS.	1 and above	C/ PC/ N	<link to evidence>
3.4.6	Where a wireless interface has an initial pairing process, the passkeys are changed from the default prior to providing normal service.	1 and above	C/ PC/ N	<link to evidence>
3.4.7	For any WiFi connection, WPA2 with AES or a similar strength encryption has been used and insecure protocols such as WPA and TKIP are disabled.	1 and above	C/ PC/ N	<link to evidence>
3.4.8	Where WPA2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	1 and above	C/ PC/ N	<link to evidence>
3.4.9	All network communications keys are stored securely.	1 and above	C/ PC/ N	<link to evidence>
3.4.10	Where the MQTT protocol is used, it is protected by a TLS connection with no known cipher vulnerabilities.	1 and above	C/ PC/ N	<link to evidence>
3.4.11	Where the CoAP protocol is used, it is protected by a DTLS connection with no known cipher vulnerabilities.	1 and above	C/ PC/ N	<link to evidence>

3.4.12	Where cryptographic suites are used such as TLS, all cipher suites shall be listed and validated against the current security recommendations such as NIST 800-131A [ref 2] or OWASP, for example using ephemeral key generation and authenticating encrypting ciphers such as AES-GCM. Where insecure ciphers suites are identified they shall be removed from the product.	1 and above	C/ PC/ N	<link to evidence>
3.4.13	All use of cryptography by the product, such as TLS cipher suites, shall be listed and validated against the import/export requirements for the territories where the product is to be sold and/or shipped.	1 and above	C/ PC/ N	<link to evidence>
3.4.14	Where there is a loss of communications, it shall not compromise the integrity of the device.	2 and above	C/ PC/ N	<link to evidence>
3.4.15	The product only enables the protocols necessary for the products' normal operation.	1 and above	C/ PC/ N	<link to evidence>

3.5 Authentication and Authorisation

Please confirm and verify with evidence (to be supplied) that the authentication and authorisation elements of the product/service meet the following requirements:

Req. No	Requirement	Compliance Class	Response	Evidence
3.5.1	The product contains a unique and tamperproof hardware identifier (e.g. such as the chip serial number or other unique silicon identifier) which is used for binding code and data to a specific device hardware.	2 and above	C/ PC/ N	<link to evidence>
3.5.2	Where the product includes a real time clock, it has a method of validating its integrity, if it is necessary for the security of the product.	2 and above	C/ PC/ N	<link to evidence>
3.5.3	Where a user interface password is used for login authentication, the default password or factory reset password is unique to each device in the product family.	1 and above	C/ PC/ N	<link to evidence>
3.5.4	The product does not accept the use of null or blank passwords.	1 and above	C/ PC/ N	<link to evidence>
3.5.5	The product will not allow new passwords containing the user account name with which the user account is associated.	1 and above	C/ PC/ N	<link to evidence>

3.5.6	The product/system enforces passwords to be compliant with CPNI Password Guidance [ref 10] or similar recommendations on: password length, characters from the groupings and special characters.	1 and above	C/ PC/ N	<link to evidence>
3.5.7	The product has defence against brute force repeated login attempts.	1 and above	C/ PC/ N	<link to evidence>
3.5.8	The product securely stores any passwords using an industry standard cryptographic algorithm.	1 and above	C/ PC/ N	<link to evidence>
3.5.9	The product supports access control measures, to the root account to restrict access to sensitive information or system processes.	1 and above	C/ PC/ N	<link to evidence>
3.5.10	The access control privileges are defined, justified and documented.	2 and above	C/ PC/ N	<link to evidence>
3.5.11	The product only allows controlled user account access; access using anonymous or guest user accounts are not supported without justification.	1 and above	C/ PC/ N	<link to evidence>
3.5.12	The product allows the factory default or OEM login accounts to be disabled or erased or renamed.	2 and above	C/ PC/ N	<link to evidence>
3.5.13	The product supports having any or all of the factory default user login passwords altered prior to installation.	1 and above	C/ PC/ N	<link to evidence>
3.5.14	If the product has a password recovery or reset mechanism, an assessment has been made to confirm that this mechanism cannot readily be abused by an unauthorised party.	1 and above	C/ PC/ N	<link to evidence>
3.5.15	Where passwords are entered on a user interface, the actual pass phrase is obscured by default.	1 and above	C/ PC/ N	<link to evidence>
3.5.16	The product allows an authorised factory reset of the device's authorisation information.	2 and above	C/ PC/ N	<link to evidence>

3.6 Encryption and Key Management for Hardware

Please confirm and verify with evidence (to be supplied) that the encryption elements of the product/service meet the following requirements:

Req. No	Requirement	Compliance Class	Response	Evidence
3.6.1	A true random number generator source is exclusively used for all relevant cryptographic operations including nonce, initialisation vector and key generation algorithms.	2 and above	C/ PC/ N	<link to evidence>

3.6.2	The true random number generator source has been validated for true randomness using an NIST SP800-22 [ref 4], FIPS 140-2 [ref 5] or similar compliance process.	2 and above	C/ PC/ N	<link to evidence>
3.6.3	There is a process for secure provisioning of keys that includes generation, distribution, revocation and destruction. For example in compliance with FIPS140-2 [ref 5] or similar process.	2 and above	C/ PC/ N	<link to evidence>
3.6.4	There is a secure method of key insertion that protects keys against copying.	1 and above	C/ PC/ N	<link to evidence>
3.6.5	All the product related cryptographic functions have no publicly known weaknesses, for example MD5 and SHA-1 are not used, e.g. those stipulated in NIST SP800-131A [ref 2].	1 and above	C/ PC/ N	<link to evidence>
3.6.6	The product stores all sensitive unencrypted parameters, e.g. keys, in a secure, tamper proof location.	1 and above	C/ PC/ N	<link to evidence>
3.6.7	The cryptographic key chain used for signing production software is different from that used for any other test, development or other software images, to prevent the installation of non-production software into production devices.	2 and above	C/ PC/ N	<link to evidence>
3.6.8	In device manufacture, all asymmetric encryption private keys that are unique to each device are either securely and truly randomly internally generated or securely programmed into each device.	2 and above	C/ PC/ N	<link to evidence>

3.7 Web User Interface

Please confirm and verify with evidence (to be supplied) that the remote web interface(s) of the product/service meet the following requirements.

Req. No	Requirement	Compliance Class	Response	Evidence
3.7.1	Where the product or service provides a web based interface, strong user authentication is used.	2 and above	C/ PC/ N	<link to evidence>
3.7.2	Where the product or service provides a web based management interface, strong mutual authentication is used.	2 and above	C/ PC/ N	<link to evidence>
3.7.3	Where a web user interface password is used for login authentication, the default password or factory reset password is unique to each device in the product family.	1 and above	C/ PC/ N	<link to evidence>

3.7.4	The web user interface is protected by automatic session/logout timeout function.	1 and above	C/ PC/ N	<link to evidence>
3.7.5	Where passwords are entered on a user interface, the actual pass phrase, is obscured by default, to prevent the capture of passwords.	1 and above	C/ PC/ N	<link to evidence>
3.7.6	The web user interface shall follow good practice guidelines, such as those listed in the OWASP top 10 attacks (https://www.owasp.org).	1 and above	C/ PC/ N	<link to evidence>
3.7.7	A vulnerability assessment has been performed before deployment and on an ongoing basis afterwards.	1 and above	C/ PC/ N	<link to evidence>
3.7.8	All inputs and outputs are validated using for example a whitelist.	1 and above	C/ PC/ N	<link to evidence>

3.8 Mobile Application

Please confirm and verify with evidence (to be supplied) that any mobile application associated with the product/service meet the following requirements.

Req. No	Requirement	Compliance Class	Response	Evidence
3.8.1	Where an application's user interface password is used for login authentication, the default password or factory reset password is unique to each device in the product family.	1 and above	C/ PC/ N	<link to evidence>
3.8.2	Password entry follows the recommendations of 3GPP TS33.117.	2 and above	C/ PC/ N	<link to evidence>
3.8.3	The mobile application stores the minimum required amount of personal information from users.	2 and above	C/ PC/ N	<link to evidence>
3.8.4	The mobile application ensures that all personal user data is encrypted at rest and in transit.	2 and above	C/ PC/ N	<link to evidence>
3.8.5	The mobile application ensures that any related databases or files are either tamper resistant or restricted in their access. Upon detection of tampering of the databases or files they are re-initialised.	1 and above	C/ PC/ N	<link to evidence>
3.8.6	Where the application communicates with a product related remote server(s) or device it does so over a secure connection such as a TLS connection using certificate pinning.	1 and above	C/ PC/ N	<link to evidence>
3.8.7	The product securely stores any passwords using an industry standard cryptographic algorithm.	1 and above	C/ PC/ N	<link to evidence>

3.9 Privacy

Please confirm and verify with evidence (to be supplied) that the privacy of the product/service meets the following requirements:

Req. No	Requirement	Compliance Class	Response	Evidence
3.9.1	The product/service stores the minimum amount of personal information from users.	1 and above	C/ PC/ N	<link to evidence>
3.9.2	The product/service ensures that all personal user data is encrypted at rest and in transit.	1 and above	C/ PC/ N	<link to evidence>
3.9.3	The product/service ensures that only authorised personnel have access to personal data of users.	1 and above	C/ PC/ N	<link to evidence>
3.9.4	The product/service ensures that personal data is anonymised whenever possible and in particular in any reporting.	1 and above	C/ PC/ N	<link to evidence>
3.9.5	The product/service ensures the controlling organisation has a data retention policy in place.	1 and above	C/ PC/ N	<link to evidence>
3.9.6	There is a method or methods for the product owner to be informed about what data is collected, why, where it will be stored.	1 and above	C/ PC/ N	<link to evidence>
3.9.7	There is a method or methods for the product owner to check/verify what data is collected and deleted.	1 and above	C/ PC/ N	<link to evidence>
3.9.8	The product/service can be made compliant with the local and/or regional data protection legislation where the product is to be sold.	1 and above	C/ PC/ N	<link to evidence>

3.10 Cloud and Network Elements

Please confirm and verify with evidence (to be supplied) that the cloud and network elements of the product/service shall meet the following requirements:

Req. No	Requirement	Compliance Class	Response	Evidence
3.10.1	All the product related cloud and network elements have the latest operating system(s) security patches implemented and processes are in place to keep them updated.	2 and above	C/ PC/ N	<link to evidence>
3.10.2	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.	1 and above	C/ PC/ N	<link to evidence>
3.10.3	All product related web servers have their webserver HTTP trace and trace methods disabled.	1 and above	C/ PC/ N	<link to evidence>

3.10.4	All the product related web servers' TLS certificate(s) are signed by trusted certificate authorities; are within their validity period; and processes are in place for their renewal.	1 and above	C/ PC/ N	<link to evidence>
3.10.5	All the product related web servers use protocols with no publicly known weaknesses.	1 and above	C/ PC/ N	<link to evidence>
3.10.6	The product related web servers have low and medium strength TLS ciphers disabled.	2 and above	C/ PC/ N	<link to evidence>
3.10.7	The product related web servers have repeated renegotiation of TLS connections disabled.	1 and above	C/ PC/ N	<link to evidence>
3.10.8	The related servers have unused IP ports disabled.	1 and above	C/ PC/ N	<link to evidence>
3.10.9	Where a product related to a webserver encrypts communications using TLS and requests a client certificate, the server(s) only establishes a connection if the client certificate and its chain of trust are valid.	2 and above	C/ PC/ N	<link to evidence>
3.10.10	Where a product related to a webserver encrypts communications using TLS, certificate pinning is implemented. For example using OWASP, https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning or similar organisations' certificate and public key pinning guidance.	2 and above	C/ PC/ N	<link to evidence>
3.10.11	All the related servers and network elements prevent the use of null or blank passwords.	1 and above	C/ PC/ N	<link to evidence>
3.10.12	The cloud and network elements follow the password requirements of section 3.5.	1 and above	C/ PC/ N	<link to evidence>
3.10.13	All the related servers and network elements prevent new passwords from containing the user account name, with which the user account is associated.	1 and above	C/ PC/ N	<link to evidence>
3.10.14	All the related servers and network elements enforce passwords to include: at least eight characters in length; characters from the groupings: alpha, numeric, and special characters, and shall not be vulnerable to dictionary attack.	1 and above	C/ PC/ N	<link to evidence>
3.10.15	The maximum permissible number of consecutive failed user account login attempts follows the recommendations of 3GPP TS33.117.	2 and above	C/ PC/ N	<link to evidence>

3.10.16	All the related servers and network elements store any passwords using a cryptographic implementation using industry standard cryptographic algorithms.	1 and above	C/ PC/ N	<link to evidence>
3.10.17	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	1 and above	C/ PC/ N	<link to evidence>
3.10.18	All the related and network elements servers prevent anonymous/guest access except for read only access to public information.	1 and above	C/ PC/ N	<link to evidence>
3.10.19	If run as a cloud service, the service meets industry standard Cloud Security principles such as the Cloud Security Alliance, NIST or UK Government Cloud Security Principles.	2 and above	C/ PC/ N	<link to evidence>

3.11 Secure Supply Chain and Production

Please confirm and verify with evidence (to be supplied) that the device production and supply chain for the product and service shall meet the following requirements:

Req. No	Requirement	Compliance Class	Response	Evidence
3.11.1	The product has all of the test and calibration software used during manufacture erased or removed before the product is dispatched from the factory.	2 and above	C/ PC/ N	<link to evidence>
3.11.2	In manufacture, all encryption keys that are unique to each device are either securely and truly randomly internally generated or securely programmed into each device. Any secret key programmed into a product at manufacture is unique to that individual device, i.e. no global secret key is shared between multiple devices.	2 and above	C/ PC/ N	<link to evidence>
3.11.3	In manufacture, all the devices are logged by the product vendor, so that cloned or duplicated devices can be identified and either disabled or prevented from being used with the system.	1 and above	C/ PC/ N	<link to evidence>
3.11.4	The production system for a device has a process to detect any devices with duplicate serial numbers to ensure that any devices with duplicate serial numbers are not shipped and are either reprogrammed or destroyed.	1 and above	C/ PC/ N	<link to evidence>

3.11.5	Where a product includes a trusted secure boot process, the entire production test and any related calibration is executed with the processor system operating in its secured boot, authenticated software mode.	2 and above	C/ PC/ N	<link to evidence>
3.11.6	A securely controlled area is used for device provisioning when the production facility is untrusted.	2 and above	C/ PC/ N	<link to evidence>

3.12 Configuration

Please confirm and verify with evidence (to be supplied) that the configuration elements of the product/service meet the following requirements:

Req. No	Requirement	Compliance Class	Response	Evidence
3.12.1	The configuration of the implementation, or the device and any related web services, is tamper resistant.	1 and above	C/ PC/ N	<link to evidence>

4 References and Abbreviations

4.1 References & Standards

The following references are used in this document.

1. NIST SP800-57 Part 3 Revision 1" NIST Special Publication 800 – 57 Part 3 Revision 1 Recommendation for Key Management Part 3: Application - Specific Key Management Guidance" http://nvlpubs.nist.gov/nistpubs SpecialPublications/NIST.SP.800-57Pt3r1.pdfhttp://nvlpubs.nist.gov/nistpubs SpecialPublications/NIST.SP.800-57Pt3r1.pdf
2. NIST Special Publication 800-131A Revision 1"Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" November 2015
3. NIST Special Publication 800-90A Revision 1 "Recommendation for Random Number Generation Using Deterministic Random Bit Generators" June 2015
4. Special Publication 800-22 Revision 1a "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" April 2010
5. FIPS PUB 140-2, Security Requirements for Cryptographic Modules
6. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2012 Version 3.1 CCMB-2012-09 001 CCMB-2012-09-003
7. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012 Version 3.1 Revision 4 CCMB-2012 09-002
8. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012 Version 3.1 Revision 4
9. Draft Framework for Cyber-Physical Systems; NIST; October 2016
10. Password Guidance, Simplifying your approach, CPNI: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach
11. DoDI-8500.2 IA Controls: http://www.dote.osd.mil/docs/dote-temp guidebook/DoDI-8500.2.pdf
12. Threat, capability and priority level terminology is taken from HMG IA Standard No. 1 – Technical Risk Assessment: https://www.ncsc.gov.uk/content files/guidance_files/IS1%20%26%202%20Supplement%20-%20Technical%2 Risk%20Assessment%20and%20Risk%20Treatment%20-%20issue%201.0%2 April%202012%20-%20NCSC%20Web.pdf
13. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122, NIST, April 2010: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf
14. Key definition of the Data Protection Act, ICO: https://ico.org.uk/for organisations/guide-to-data-protection/key-definitions
15. Overview of the General Data protection Regulations (GDPR), ICO: https://ico org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
16. Annex J (normative): List of Privacy Attributes and Clause 11 Privacy Protection Architecture using Privacy Policy Manager (PPM) http://www.onem2m.org images/files/deliverables/Release2/TS-0003_Security_Solutions-v2_4_1.pdf
17. Example of IoT application id registry and possible privacy profile registry https: appid.iconectiv.com/appid/#/

4.2 Definitions and Abbreviations

For the purposes of the present document, the following abbreviations apply.

4.2.1 Definitions

Authorised Trust Entity	Trusted third party, such as certification authority (CA) that issues digital certificates. These certify the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. The most commonly encountered public-key infrastructure (PKI) schemes are those used to implement https on the world-wide web.
Application	Applications (also called end-user programs) are software programs designed to perform a group of coordinated functions or tasks that may vary by installation or model. Examples of IoT applications include a web browser, sensor management, or actuator controller. This contrasts with system software, which runs the operating software of the main processor in the device.
Deployment	The placing of the product into customer trial or service.
Encrypted	Is defined as being encrypted using a recognised algorithm and protected keys.
Firmware	Computer programs and data stored in hardware - typically in read only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. SOURCE: CNSSI-4009
Mutual Authentication	Mutual authentication refers to a security process or technology in which two entities in a communications link authenticate each other before any sensitive data is sent over the connection. In a network environment, the client authenticates the server and vice-versa. It is a default mode of authentication in some protocols (IKE, SSH) and optional in others (TLS).
IoT Product Class	Class of network products that all implement a common set of IoTSF defined functions for that particular IOT product.
Software	Unless otherwise explicitly stated, for the purposes of this document the term software also includes any firmware elements in the product.
Trust Mark	A certification mark that indicates that the product and/or service has been through a security compliance process recognised by the IoTSF.

4.2.2 Abbreviations

CPNI	Centre for the Protection of National Infrastructure
FSM	Foundation Security Mark
MNO	Mobile Network Operator
PRNG	Pseudo Random Number Generator
SAM	Security Access Module
TOE	Target of Evaluation
TRNG	True Random Number Generator
TBC	To Be Confirmed
TBD	To Be Determined
TLS	Transport Layer Security

www.iotsecurityfoundation.org