IoT Security Foundation
Security Assurance Framework

Docs

Table Of Contents:

IoT Security Assurance Framework

Release 3.0, November 2021

Notices, Disclaimer, Terms Of Use, Copyright And Trademarks 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 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, Trademarks And Licensing

Acknowledgements

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this document:

- Abhay Soorya, Gemserv Ltd
- Alex Margulis, Intel Corp
- Andrew Bott, Secure Thingz Ltd
- Arun Sambordaran, Gemserv Ltd
- Chris Hills, Phaedrus Systems Ltd
- Chris Shire, Infineon Technologies Ltd
- Graham Markall, Embecosm Ltd
- Ian Phillips, Roke Manor Research Ltd
- Ian Poyner, IoTSF
- Isaac Dangana, Red Alert Labs Ltd
- Jan Krueger, Intel Corp
- Jeremy Bennett, Embecosm Ltd
- John Moor, IoT Security Foundation
- Lokesh Johri, Tantiv 4
- Mark Beaumont, Roke Manor Research Ltd
- Michael Richardson, Sandelman Software Works
- Nick Hayes, Thinkstream Ltd
- Pamela Gupta, Outsecure Inc
- Peter Burgers, DisplayLink Ltd
- Richard Marshall, Xitex Ltd
- Richard Storer, MathEmbedded Ltd
- Robert Dobson, Device Authority Ltd
- Roger Shepherd, Chipless Ltd
- Sean Gulliford, Gemserv Ltd
- Trevor Hall, Synaptics / DisplayLink Ltd

Peer Reviewers

- Andrew Bott, Secure Thingz Ltd
- Jeff Day, BT Plc
- James Willison, Unified Security Ltd
- Plus others – you know who you are!

Editors

- Trevor Hall, Synaptics Chair Assurance Framework WG
- Ian Poyner, IoTSF
- Amyas Phillips, Ambotec Ltd - Chair Supply Chain WG
- Richard Marshall, Xitex Ltd
- Graham Markall

Introduction

1.1 Introduction

The IoT Security Foundation (IoTSF) was established to address the challenges of IoT security in an increasingly connected world. It has a specific mission ***"to help secure the Internet of Things, in order to aid its adoption and maximise its benefits. To do this IoTSF will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems"***.

In more concise terms for vendors, operators, and end-users: ***"Build Secure, Buy Secure, Be Secure"***.

This IoT Security Assurance Framework ('Framework') leads its user through a structured process of questioning and evidence gathering. This ensures suitable security mechanisms and practices are implemented. It was previously published as the IoT Security Compliance Framework up until Release 2.1, and this version remains fully backward compatible with the same sections and requirement numbering. The terminology better reflects the risk-based system and is better aligned with how governments and international bodies are approaching IoT security.

The Framework is intended to help all companies make high-quality, informed security choices by guiding them through a comprehensive requirement checklist and evidence gathering process. The evidence gathered during the process can be used to declare conformance with best practice to customers and other stakeholders.

Providing good security capability requires decisions upfront in design and use – often referred to as ***secure by design***. In most cases, addressing the security of a product at the design stage is proven to be lower cost, and requiring less effort than trying to "put security" into or around a product after it has been created (which may not even be possible). Decisions need to be made to address use-case, business model, liability level and risk management in addition to technical concerns such as architecture, design features, implementation, testing, configuration and maintenance.

Throughout this document, and others published by the IoTSF, reference is made to "best practice" or "best practice security engineering". These best practices are derived from the combined expertise of the IoTSF members, used and tested within their own companies, and from the publications and guidance of other relevant organisations. Wherever possible, reference is made to existing standards and best practice materials to avoid unnecessary duplication. A list of external reference materials and related bodies is included at the end of this document in the section References and Abbreviations.

Intended-Audience

1.2 Intended Audience

The Framework can be used internally in an organisation as a pre-compliance tool to self-assess or self-certify against, or by a third-party auditor. It can also be used 'in part', as a procurement mechanism to help specify security requirements of a supplier contract. The Framework is aimed at the following stakeholders:

- For **Managers** in organisations that provide IoT products, technology and or services. It gives a comprehensive overview of the management process needed to adopt best practice. It will be useful for executive, programme, and project managers, by enabling them to ask the right questions and assess the answers.
- For **Developers and Engineers, Logistics and Manufacturing Staff**, it provides detailed requirements 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.). Documentary evidence may be assembled using this Framework as a guide or by completing the Assurance Questionnaire (see below 1.4 IoTSF Resources That Support The Framework). In this way, documentary evidence will be compiled to demonstrate assurance both at development gates, and with third parties such as auditors or customers.
- For **Supply Chain Managers**, the structure can be used to guide the auditing of security practices. It may therefore be applied within a producer organisation (as described above); and inspected by a customer of the producer.
- For **Trusted Third Parties** as part of an audit or certification process.

Scope

1.3 Scope

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

- Business processes
- The “Things” in IoT, i.e. network connected products and/or devices
- Aggregation points such as gateways and hubs that form part of the connectivity
- Networking including wired, and radio connections, cloud and server elements

1.3.1 Key Issues For IoT Security

The key compliance requirements can be summarised as follows:

Security Requirements

The following table outlines key security requirements and associated actions:

Key Requirement	Action Required	Framework Reference
Management governance	There must be a named executive responsible for product security, and privacy of customer information.	2.4.3, 2.4.11
Engineered for security	The hardware and software must be designed with attention to security threats.	2.4.4, 2.4.5, 2.4.6, 2.4.7
Fit for purpose cryptography	These functions should be from the best practice industry standards.	2.4.8, 2.4.9
Secure network framework and applications	Precautions have been taken to secure Apps, web interfaces, and server software.	2.4.12, 2.4.13
Secure production processes and supply chain	Making sure the security of the product is not compromised in the manufacturing process or in the end customer delivery and installation.	2.4.10, 2.4.12, 2.4.13
Safe and secure for the customer	The product is safe and secure "out of the box" and in its day-to-day use. The configuration and control should guide the person managing the device into maintaining security and provide for software updates, vulnerability disclosure policy, and life cycle management.	2.4.14

1.3.2 The Supply Chain Of Trust

All end-use products are constructed using a set of component parts, typically sourced from a variety of suppliers. These parts may be electronic or mechanical components, software modules or packages, including open source. Many of these parts will be procured from third party suppliers. It is important that all parts, together with the supply chain logistics, be subject to a security review/audit.

The final IoT product can then be provided with its own evidence of security assessment, together with the component parts documents, as a complete package of auditable evidence. This will help users to assess how the product conforms to the overall ***"supply chain of trust"*** [ref 36][1].

Footnotes

1. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), an approach for managing information security risks. [https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51546] ↩

IoTSF-Resources-That-Support-The-Framework

1.4 IoTSF Resources That Support The Framework

The IoTSF provides a number of resources to foster security best practice:

- **This Framework** document [ref 19][1] is a structured list of security requirements intended to aid the evidence gathering process to guide an organisation through assurance.
- The **Assurance Questionnaire** is a companion audit and assessment tool to the Framework to aid the setting of security objectives and thereafter the collection of documentation and evidence. The Assurance Questionnaire is available to IoTSF members only for free.
- Additional **Best Practice Guidelines** are provided by the Foundation to help understanding of the most important topics [ref 45][2].
- Further resources including guides, documents, articles and blogs can be found on the IoTSF website.

All IoTSF publications are maintained and reviewed on a regular basis to keep them current – which is a crucial attribute, given the dynamic nature of cyber security.

This is the latest public release and user feedback is welcome as part of its maintenance and evolution for addressing new security threats. You can send feedback and suggestions to improve the Framework by emailing contact@iotsecurityfoundation.org with a subject line of **"Assurance Framework Feedback"**.

1.4.1 Changes From Release 2.1 Of The Framework

Release 2.1 of the Framework was restricted to consumer class products. This Release 3.0 of the Framework includes expanded mapping to standards that have emerged since release 2.1 was published and introduced additional sub sections. New items for this release:

- Change of name from "Compliance Framework" to "Assurance Framework"
- Updated requirements mapping to ETSI standard EN 303 645
- Added new requirements mapping for NIST standard 8259A
- Expanded the Supply Chain section's requirements

The Assurance Applicability (requirements) elements detailed in section 2.4 and the numbering have been maintained where possible from prior releases of the Framework to maintain consistency.

Footnotes

1. IoTSF Vulnerability Disclosure Guidelines can be found [https://iotsecurityfoundation.org/best-practice-guidelines] ↩

2. IoTSF Best Practice Guidelines for Connected Consumer Products V1.1 includes at time of publication individual guidelines for the following topics: A. Classification of data

   B. Physical security

   C. Device secure boot

   D. Secure operating system

   E. Application security

   F. Credential management

   G. Encryption

   H. Network connections

   J. Securing software updates

   K. Logging

   L. Software update policy [https://www.iotsecurityfoundation.org/best-practice-guidelines/#ConnectedConsumerProducts] ↩

The-Process

2.1 The Process

The Framework sets out a comprehensive set of security requirements for aspects of the organisation and product. A response to each requirement needs to be recorded, with supporting statements or evidence. The Assurance Questionnaire is available to IoTSF Members to facilitate evidence collation. For requirements deemed "not applicable", an explanation must be provided as to why. Any alternative countermeasures to reduce any security risk should also be listed.

The assurance process breaks down into a number of steps:

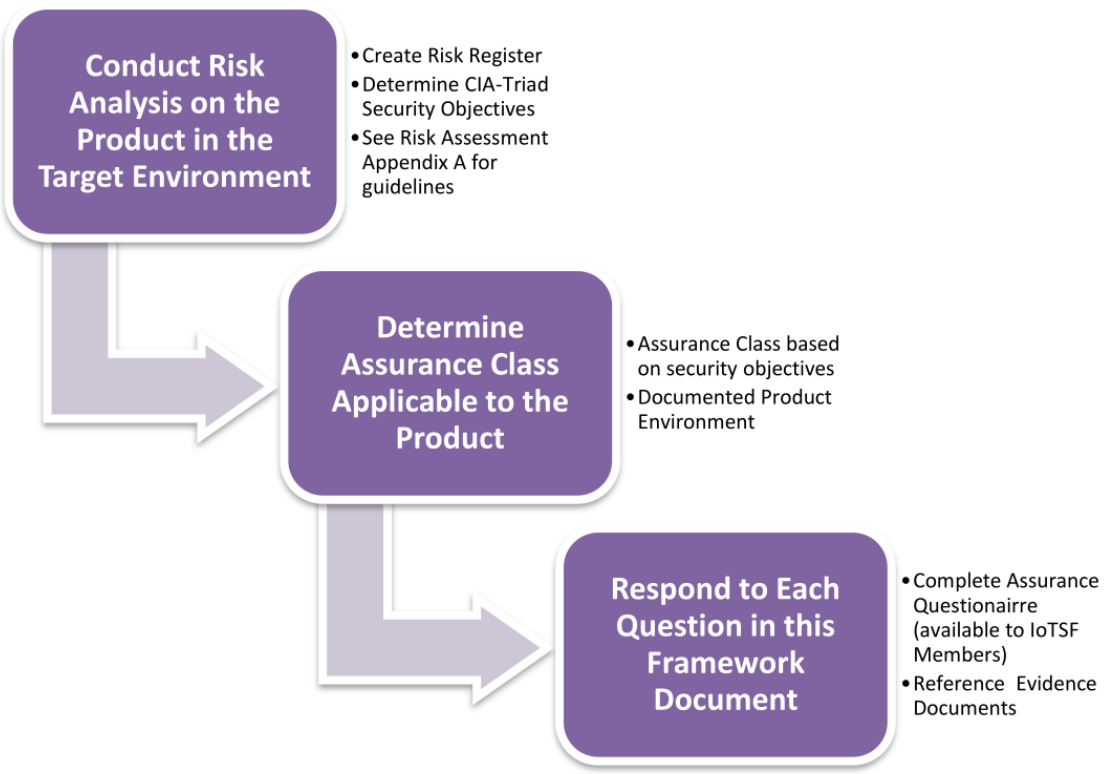

Figure 1 Assurance process steps

2.1.1 Risk Assessment

In security terms, ***context is everything*** - each application differs in use-case and operating environment. It is the responsibility of the Framework user to determine their risk appetite within their stated usage environment and therefore the specific assurance class (section 2.2) of the security measures applied.

To achieve this, **a comprehensive risk assessment is a pre-requisite to using the Framework**. The risk assessment process will help determine the assurance class for the product/service. Section 2.2 has more details on assurance classes and how they relate to the Confidentiality, Integrity and Availability, otherwise known as the CIA Triad [ref 46][1] model, commonly used by security professionals. Generally, the highest possible assurance class should be adopted, considering not just the immediate context of the product, but also the potential hazards to the system(s) that the product/service may eventually be used in.

A basic outline of the risk assessment process can be found in Appendix A. Risk management techniques can also be found in publications from organisations such as NCSC, ENISA and NIST [ref 40, 41 and 42][2][3][4].

Footnotes

1. CIA Triad has no original source, but for more info visit: [https://www.techrepublic.com/blog/it-security/the-cia-triad] ↩

2. UK Government Cyber security risk assessment guidance [https://www.ncsc.gov.uk/guidance/risk-management-collection] ↩

3. NIST Special Publication 800-30 guidance for conducting risk assessments [https://www.nist.gov/publications/guide-conducting-risk-assessments] ↩

4. EU ENISA guidance of Cyber Security Risk Management [https://www.enisa.europa.eu/topics/threat-risk-management/risk-management] ↩

Assurance-Class

2.2 Assurance Class

Determining the security objectives across the full diversity of IoT-class applications is a subjective endeavour. Even within vertical sectors such as consumer and enterprise, the security measures and strength of controls will vary depending on the actual use case. In making the Framework more practical across a range of applications, this version has adopted a risk-based approach derived from the commonly used CIA Triad [ref 46][1]. Whilst it is not a perfect model, its simplicity is its strength, and good security practice can be derived from the core principles.

Depending on the market and application into which the product is intended to be used, a risk assessment may require a higher assurance class to mitigate the determined level of risk. Consider the following example: a fictional case of a Wi-Fi relay box used in a remote monitoring station, where the threat to the enterprise operation is considered low, could be assessed under Assurance Class 1 requirements. However, when deployed into a hospital, with higher threat dependencies, it could be assessed to be under Assurance Class 4 requirements. A further example is provided in section 2.2.1.

In order to apply an appropriate level of security assurance to a product, the requirements in the Framework are classified using the following assurance classes:

- *Class 0: where compromise to the data generated or loss of control is likely to result in little discernible impact on an individual or organisation*
- *Class 1: where compromise to the data generated or loss of control is likely to result in no more than limited impact on an individual or organisation (requirements in ETSI. DCMS, NCSC CoP demand Class 1 at a minimum)*
- *Class 2: in addition to class 1, the device is designed to resist attacks on availability that would have significant impact on 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 Personally identifiable information (PII)*
- *Class 4: in addition to class 3, where compromise to the data generated or loss of control have the potential to affect critical infrastructure or cause personal injury*

For each assurance class, indicative levels of confidentiality, integrity and availability are shown in **Table 1** below.

Security Objective

Assurance Class	Confidentiality	Integrity	Availability
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

Table 1: Assurance Class Security Objectives

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

- Confidentiality
    - Basic – devices or services processing public information
    - Medium – devices or services processing sensitive information, including Personally Identifiable Information, whose compromise would have limited impact on an individual or organisation
    - High – devices or services processing very sensitive information, including sensitive personal data whose compromise would have significant impact on an individual or organisation
- Integrity
    - Basic – devices or services whose compromise could have a minor or negligible impact on an individual or organisation
    - Medium – devices or services whose compromise could have limited impact on an individual or organisation

    - High – devices or services whose compromise could have a significant or catastrophic impact on an individual or organisation

- Availability
    - Basic – devices or services whose lack of availability would cause minor disruption
    - Medium – devices or services whose lack of availability would have limited impact on an individual or organisation
    - High – devices or services whose lack of availability would have significant impact to an individual or organisation, or impacts many individuals

  [ref 11, 12, 13 & 14 were used as the basis of the above definitions]

Please Note: The Framework Assurance Class is provided for guidance only. A supplier may know of application specific concerns that would change the class values. Requirements deemed "not applicable" must be supported by credible evidence to explain the case.

2.2.1 Determining Security Goals – An Example

To illustrate via a practical example, consider the security features required by a connected thermostat used in a commercial greenhouse. The Assurance Class selection for the device might be determined in the following way:

- Confidentiality is Basic: the underlying assumption is that the thermostat does not store sensitive, confidential, or personally identifiable information
- Integrity is Medium: for a thermostat in a commercial greenhouse, poor data integrity could have a business/financial impact
- Availability is Medium: the thermostat in a commercial greenhouse setting is likely to be part of an environmental control system. As such an individual sensor failure will have little impact, yet a denial- of-service attack across multiple sensors carries a greater commercial risk

In this case, the thermostat may be classified in the following way:

Security Objective

Assurance Class	Confidentiality	Integrity	Availability
Class 1	Basic	Medium	Medium

Table 2: Example of Assurance Class Security Objectives

Footnotes

1. CIA Triad has no original source, but for more info visit: [https://www.techrepublic.com/blog/it-security/the-cia-triad] ↩

Using-The-Assurance-Questionare

2.3 Using The Assurance Questionnaire

It is anticipated that assurance with the Framework will become an integral part of an organisation's security process and will provide the supporting evidence for business assurance. An accompanying audit and assessment tool (available to IoTSF Members), the Assurance Questionnaire, may be used at various stages in the product lifecycle. Firstly, by identifying the need for security at the concept stage; secondly listing evidence gathered; to finally signing off security requirements for production release.

The evidence gathering process can only commence after establishing the Assurance Class described in section 2.2. This is done using a risk assessment (see Appendix A).

Once the Assurance Class is determined, the applicable requirements are automatically derived by the accompanying Assurance Questionnaire tool as either mandatory (M) or advisory (A). The Assurance Questionnaire could also be used to optimise the product design and establish if a change would allow a lower Assurance Class to be selected. For example, by not collecting or processing sensitive personal data or perhaps providing automatic failover to alternative services for customers to maintain service availability.

2.3.1 Assessment Methodology

The assessment method is determined by the context i.e. Business (process) or System (technical) and the Class.This determines both the type of assessment e.g. physical testing or document review, along with the degree of rigour from Self-Assessment for lower Classes to full third-party audit for high classes.

2.3.2 Keywords

To improve the usability of this document the requirements in sections 2.4.3 to 2.4.16 have been categorised using the keywords defined in the **Table 3** below.

Primary Keyword	Description	Secondary keyword	Description
System	The requirement is applicable to the technical elements of the device/ product or service	Software	The requirement is directly applicable to the software of the device or service
		Hardware	The requirement is directly applicable to the electronics of the device/service hardware (PCB, processor, components etc.)
		Physical	The requirement is directly applicable to mechanical aspects of the device such as the casing, form factor etc.
Business	A business requirement not directly related to the operational function of the device/ product or service	Process	A flow of activities that indirectly contributes to the security characteristics of a device or service
		Policy	The instructions and guidelines that indirectly contribute to the security characteristics of a device or service
		Responsibility	A role or responsibility that indirectly contributes to the security characteristics of a device or service

Table 3: Keyword Categories

Please Note: the terms Device and Product are interchangeable in this document

2.3.3 Assurance Requirements Completion Responsibilities

The Assurance requirements completion will be addressed by a variety of roles in an organisation. These roles cannot be prescribed exactly as every organisation is different, but each section of requirements may require the attention of Managers and other specialist staff as suggested in **Table 4** below. Responsibility for any individual requirement may be determined by use of the associated keywords, which can be selected by filter, for users of the Assurance Questionnaire.

Section	Topic	Topic Audience & Typical Responsibilities
2.4.3	Business Security Processes, Policies and Responsibilities	Management responsible for governance of a business developing and deploying IoT Devices.
2.4.4	Device Hardware & Physical Security	Design and Production staff responsible for hardware and mechanical quality.
2.4.5	Device Software	Device application quality management by Software Architects, Product Owners and Release Managers.
2.4.6	Device Operating System	Management and Design staff responsible for selection of a third- party operating system or assessing the quality of 'in-house' developed software.
2.4.7	Device Wired and Wireless Interfaces	Design and Production staff responsible for device communications security.
2.4.8	Authentication and Authorisation	Design and Production staff responsible for security of the IoT systems interfaces and foundations of authentication.
2.4.9	Encryption and Key Management for Hardware	Design and Production staff responsible for security of the IoT systems hardware key management and encryption.
2.4.10	Web User Interface	Design and Production staff responsible for security of the IoT Product or Services' Web Systems.
2.4.11	Mobile Application	Design and Production staff responsible for security of the IoT Product or Services' Mobile Application.
2.4.12	Privacy	Management and staff responsible for Data Protection and Privacy regulatory compliance.
2.4.13	Cloud and Network Elements	Design and Production staff responsible for security of the IoT Product or Services' Cloud or Network Systems.
2.4.14	Secure Supply Chain and Production	Management, Design and Production staff responsible for security of the IoT Product or Services' Supply Chain.
2.4.15	Configuration	Design and Production staff responsible for security of the device and IoT Services configurations.
2.4.16	Device Ownership Transfer	Management, Design and Production staff responsible for a products and services' Supply Chain.

Table 4: Assurance Responsibilities

Relevant requirements should be shown as "addressed" and a reference made to the applicable evidence for the product design.

The accompanying Assurance Questionnaire allows for entries, against each relevant requirement, of either the evidence gathered to prove assurance or a link to that evidence. The evidence may be compiled from a number of sources and people. Evidence should be verified by the person responsible for completion of the Framework and such verification should be recorded.

An example of completed Assurance Questionnaire fragment on Business Processes for a high-risk Class 3 device is shown Figure 1 below.

ReqNo	Requirement	Required Assessment Method	Evidence Type	Pre-Assurance	Evidence	Responsability
2.4.3.1	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 and makes and monitors the security policy	SA Document review + TP Inquiry	Organisation al Chart and Job role description/documentation and Proof of Competence (certification/attestation)		URL or reference to document with Third party attestation	CIO name
2.4.3.2	There is a person or role, who takes ownership for adherence to this compliance framework process.	SA Document review + TP Inquiry	Organisation al Chart and Job role description/documentation and Proof of Competence (certification/attestation)		URL or reference to document with Third party attestation	CIO name
2.4.3.4	The company follows industry standard cyber security recommenda tions (e.g. UK Cyber Essentials, NIST Cyber Security Framework, ISO27000 etc.).	SA Document review + TP Inquiry	Organisation al Chart and Job role description/documentation and Proof of Competence (certification/attestation)		URL or reference to document with Third party attestation	CIO name

Figure 2: Assurance Questionnaire Partially Completed Example

2.3.4 Evidence

This Framework offers a comprehensive set of security requirements (see section 2.4 under Assurance Applicability) and should be used with the products or services design documentation including the Risk Register. Evidence of the mitigations made to address each risk line item must also be recorded. Users of the Framework should therefore create their own records and IoTSF members are encouraged to use the Assurance Questionnaire for the recording process.

Such records should be kept safe and secure, we recommend having back-up copies. They could be useful in the case of real-world threats to the product, but also as evidence for any business assurance regimes used in the organisation. The record keeper should enable access, for auditing, to any referenced evidence and supporting documents. URLs especially should be checked to ensure they will remain accessible at least for the life of the product plus any warranty period. Attention should also be paid to maintaining any tools or applications needed to view the evidence material.

An organisation procuring products, systems and services from a supplier, which declares it has used the Framework, may request an audit of 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.

Assurance-Terminology-And-Applicability

2.4 Assurance Terminology And Applicability

2.4.1 Terminology

The following terms "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may" and "optional" are used in accordance with the definitions in RFC2119 [ref 25][1].

2.4.2 Level Of Assurance

The applicability levels are defined as follows

Mandatory	This requirement shall be met, as it is vital to meet the security objectives of the product.
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 and alternative countermeasures to reduce any security risk should be documented.

For example in the following tables, where it shows “M of 2 and above” assurance class, this means that the requirement is mandatory for the stated level and all higher levels i.e. 2, 3 & 4.

Footnotes

1. IETF – RFC2119 “Key words for use in RFCs to Indicate Requirement Levels” [https://www.ietf.org/rfc/rfc2119.txt] ↩

2.4.3 Business Processes

Go to Detailed Requirements

This section's intended audience is those personnel who are responsible for governance of a business developing and deploying IoT Devices. There must be named executive(s) responsible for product security, and privacy of customer information. There are several classes of requirements, which have been identified by a keyword. Each class should be allocated to a specified person or persons for the product being assessed. Further guidance is available from the IoTSF Best Practice Guidelines [ref 44][1]. The applicability of each requirement is defined as Advisory or Mandatory for the assessed risk level of any device, the default is Advisory.

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.3.1	There is a person or role, accountable to the Board, who takes ownership of and is responsible for product, service and business level security, and mandates and monitors the security policy.	Mandatory for all classes	Business	Responsibility
2.4.3.2	There is a person or role, who takes ownership for adherence to this compliance framework process.	Mandatory for all classes	Business	Responsibility
2.4.3.3	Intentionally left blank to maintain requirement numbering	-		
2.4.3.4	The company follows industry standard cyber security recommendations.	Mandatory for all classes	Business	Policy
2.4.3.5	A policy has been established for interacting with both internal and third party security researcher(s) on the products or services.	Mandatory for all classes	Business	Policy
2.4.3.5.1	The third party policy shall be publicly available and include contact information for reporting issues and information on timelines to acknowledge and provide status updates.	Mandatory for all classes	Business	Policy
2.4.3.6	A policy has been established for addressing risks that could impact security and affect or involve technology or components incorporated into the product or service provided. At a minimum this should include a threat model, risk analysis and security requirements for the product and its supply chain through its whole stated supported life. This should be maintained, communicated, prioritised and addressed internally as part of product development throughout the product support period.	Mandatory for Class 2 and above	Business	Policy
2.4.3.7	Processes and plans are in place based upon the IoTSF "Vulnerability Disclosure Guidelines" [ref 19][2], or a similar recognised process, to deal with the identification of a security vulnerability or compromise when they occur.	Mandatory for all classes	Business	Process
2.4.3.8	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 executives who may deal with the media or make public announcements.	Mandatory for all classes	Business	process
2.4.3.9	There is a secure notification process based upon the IoTSF "Vulnerability Disclosure Guidelines" [ref 19][2], ISO/IEC 29147, or a similar recognised process, for notifying partners/users of any security updates, and what vulnerability is addressed by the update.	Mandatory for all classes	Business	Process

2.4.3.9.1	There is a minimum support period during which security updates will be made available to all stakeholders.	Mandatory for all classes	Business	Process
2.4.3.10	A security threat and risk assessment shall have been carried out using a standard methodology appropriate to IoT products and services, to determine the risks and evolving threats before a design is started -this should cover the entire system being assessed.	Mandatory for Class 1 and above	Business	Process
2.4.3.11	As part of the Security Policy, include a specific contact and web page for Vulnerability Disclosure reporting.	Mandatory for all classes	Business	Policy
2.4.3.12	As part of the Security Policy, provide a dedicated security email address and/or secure online page for Vulnerability Disclosure communications.	Mandatory for all classes	Business	Policy
2.4.3.13	As part of the Security Policy, develop a conflict resolution process for Vulnerability Disclosures.	Mandatory for all classes	Business	Process
2.4.3.14	As part of the Security Policy, publish the organisation's conflict resolution process for Vulnerability Disclosures.	Mandatory for Class 1 and above	Business	Process
2.4.3.16	As part of the Security Policy, develop security advisory notification steps.	Mandatory for all classes	Business	Process
2.4.3.17	The Security Policy shall be compliant with ISO 30111 or similar standard.	Mandatory for Class 3 and above	Business	Policy
2.4.3.18	Where the a device may be used in real-time or high-availability systems, a procedure must be defined for notifying operators of connected components and system management of impending downtime for updates. In such real time or high availability system the end user should be able to decide whether to automatically install updates or to chose to manually install an update at a time of their choosing (or to ignore an update).	Mandatory for Class 2 and above	Business	Process
2.4.3.19	Whilst overall accountability for the product or service remains with the person in 2.4.3.1, responsibility can be delegated for each domain involved in any system or device update process, e.g. new binary code to add features or correct vulnerabilities.	Mandatory for Class 2 and above	Business	Responsibility
2.4.3.20	Responsibility is allocated for control, logging and auditing of the update process.	Mandatory for Class 2 and above	Business	Process
2.4.3.21	There is a point of contact for third party suppliers and open source communities to raise security issues.	Mandatory for Class 1 and	Business	Process

		above		
2.4.3.22	Where remote update is supported, there is an established process/plan for validating "updates" and updating devices on an on-going or remedial basis.	Mandatory for Class 2 and above	Business	Process
2.4.3.22.1	Users must have the ability to disable updating.	Mandatory for Class 1 and above	Business	Process
2.4.3.23	The security update policy for devices with a constrained power source shall be assessed to balance the needs of maintaining the integrity and availability of the device.	Mandatory for Class 2 and above	Business	Policy
2.4.3.24	There is a named owner responsible for assessing third party (including open-sourced) supplied components (hardware and software) used in the product	Mandatory for Class 2 and above	Business	Responsibility
2.4.3.25	Where a remote software upgrade can be supported by the device, there should be a transparent and auditable policy with a schedule of actions of an appropriate priority, to fix any vulnerabilities in a timely manner.	Mandatory for Class 2 and above	Business	Policy
2.4.3.26	As part of the security policy, define a process for maintaining a central inventory of third party components and services, and their suppliers, for each product.	Mandatory for all classes	Business	Policy
2.4.3.27	As part of the security policy, define how security requirements on third party components and services (including open-source) will be established and assessed.	Mandatory for all classes	Business	Policy
2.4.3.28	As part of the procurement policy, a supplier should be awarded a higher score where they demonstrate that they implement secure design in accordance with industry implementation standards or guidelines.	Mandatory for all classes	Business	Policy
2.4.3.29	The organisation retains an enduring competency to revisit and act upon such information during product upgrades or in the event of a potential vulnerability being identified. (Key security design information and risk analysis is retained over the whole lifecycle of the product or service.)	Mandatory for all classes	Business	process

Footnotes

1. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 [https://www.iso.org/standard/57018.html] ↩

2. IoTSF Vulnerability Disclosure Guidelines can be found [https://iotsecurityfoundation.org/best-practice-guidelines] ↩ ↩[2]

2.4.4 Device Hardware

Go to Detailed Requirements

This section's intended audience is those personnel who are responsible for hardware and mechanical quality. Guidance is available from the IoTSF [ref 44][1] regarding Physical Security (part B) Secure Boot (part C) and Secure Operating Systems (part D).

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.4.1	The product's processor system has an irrevocable hardware Secure Boot process.	Mandatory for all classes	System	Hardware
2.4.4.2	The product's processor system has an irrevocable "Trusted Root Hardware Secure Boot".	Mandatory for Class 2 and above	System	Hardware
2.4.4.3	The product's processor boot process provides an appropriate level of trustworthiness by using a hardware root of trust to verify trusted boot or measured boot methods. This may be referred to as 'secure boot', but absolute security cannot be assured.	Mandatory for Class 3 and above	System	Hardware
2.4.4.4	The Secure Boot process is enabled by default.	Mandatory for all classes	System	Hardware
2.4.4.5	Any debug interface only communicates with authorised and authenticated entities on the production devices.(note: 2.4.4.6-8 should be considered as advisory) The functionality of any interface should be minimised to its essential task(s).	Mandatory for Class 1 and above	System	Hardware Software
2.4.4.6	The hardware incorporates protection against tampering and this has been enabled. The level of tamper protection must be determined by the risk assessment.	Mandatory for Class 1 and above	System	Hardware
2.4.4.7	The hardware incorporates physical, electrical and logical protection against tampering to reduce the attack surface. The level of protection must be determined by the risk assessment.	Mandatory for Class 2 and above	System	Hardware Physical
2.4.4.8	The hardware incorporates physical, electrical & logical protection against reverse engineering. The level of protection must be determined by the risk assessment.	Mandatory for Class 3 and above	System	Hardware
2.4.4.9	All communications port(s) which are not used as part of the product's normal operation are not physically accessible or only communicate with authorised and authenticated entities.	Mandatory for Class 1 and above	System	Hardware Physical Software
2.4.4.10	All the product's development test points are securely disabled or removed wherever possible in production devices.	Mandatory for Class 2 and above	System	Hardware Physical
2.4.4.11	Tamper Evident measures have been used to identify any interference to the assembly to the end user.	Mandatory for Class 2 and above	System	Hardware
2.4.4.12	Intentionally left blank to maintain requirement numbering	-		

2.4.4.12	Intentionally left blank to maintain requirement numbering			
2.4.4.13	In production devices the microcontroller/ microprocessor(s) shall not allow the firmware to be read out of the products non-volatile [FLASH] memory. Where a separate non-volatile memory device is used the contents shall be encrypted.	Mandatory for Class 1 and above	System	Hardware
2.4.4.14	Where the product's credential/key storage is external to its processor, the storage and processor shall be cryptographically paired to prevent the credential/key storage being used by unauthorised software.	Mandatory for Class 1 and above	System	Hardware
2.4.4.15	Where a production device has a CPU watchdog, it is enabled and will reset the device in the event of any unauthorised attempts to pause or suspend the CPU's execution.	Mandatory for Class 1 and above	System	Hardware
2.4.4.16	Where the product has a hardware source for generating true random numbers, it is used for all relevant cryptographic operations including nonce, initialisation vector and key generation algorithms.	Mandatory for Class 1 and above	System	Hardware Software
2.4.4.17	The product shall have a hardware source for generating true random numbers.	Mandatory for Class 2 and above	System	Hardware

Footnotes

1. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 [https://www.iso.org/standard/57018.html] ↩

2.4.5 Device Software

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for device application quality e.g. Software Architects, Product Owners, and Release Managers. Guidance is available from the IoTSF [ref 44][1] regarding Secure Operating Systems (part D), Credential Management (part F), and Software Updates (part J).

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.5.1	The product has measures to prevent unauthorised and unauthenticated software, configurations and files being loaded onto it. If the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/or sandbox.	Mandatory for all classes	System	Software
2.4.5.2	Where remote software updates can be supported by the device, the software images must be digitally signed by an appropriate signing authority - e.g. manufacturer/supplier or public. The Signing Authority should be clearly identified.	Mandatory for all classes	System	Software
2.4.5.3	Where updates are supported, the software update package has its digital signature, signing certificate and signing certificate chain verified by the device before the update process begins.	Mandatory for all classes	System	Software
2.4.5.4	If remote software upgrade is supported by a device, software images shall be encrypted or transferred over an encrypted channel.	Mandatory for Class 2 and above	System	Software
2.4.5.5	If the product has any virtual port(s) that are not required for normal operation, they are only allowed to communicate with authorised and authenticated entities or are securely disabled when shipped. When a port is initialised or used for field diagnostics, the port input commands are deactivated and the output provides no information which could compromise the device, such as credentials, memory address or function names.	Mandatory for Class 2 and above	System	Software
2.4.5.6	To prevent the stalling or disruption of the device's software operation, watchdog timers are present, and cannot be disabled.	Mandatory for Class 1 and above	System	Hardware Software
2.4.5.7	The product's software signing root of trust is stored in tamper-resistant memory.	Mandatory for Class 1 and above	System	Hardware
2.4.5.8	The product has protection against unauthorised reversion of the software to an earlier and potentially less secure version. Only authorised entities can restore the software to an earlier secure version.	Mandatory for Class 2 and above	System	Software
2.4.5.9	There are measures to prevent the installation of non-production (e.g. development or debug) software onto production devices.	Mandatory for Class 1 and above	Business	Process
2.4.5.10	Production software images shall be compiled in such a way that all unnecessary debug and symbolic information is removed, to prevent accidental release of superfluous data	Mandatory for Class 1 and above	Business	Process

	accidental release of superfluous data.	above		
2.4.5.11	Development software versions have any debug functionality switched off if the software is operated on the product outside of the product vendor's trusted environment.	Mandatory for Class 2 and above	Business	Process
2.4.5.12	Steps have been taken to protect the product's software from sensitive information leakage, including at network interfaces during initialisation, and side-channel attacks.	Mandatory for Class 3 and above	System	Hardware
2.4.5.13	The product's software source code follows the basic good practice of a Language subset coding standard.	Mandatory for Class 2 and above	Business	Policy
2.4.5.14	The product's software source code follows the basic good practice of static vulnerability analysis [ref 37][2] by the developer.	Mandatory for Class 2 and above	Business	Process
2.4.5.15	The software must be architected to identify and ring fence sensitive software components, including cryptographic processes, to aid inspection, review and test. The access from other software components must be controlled and restricted to known and acceptable operations. For example security related processes should be executed at higher privilege levels in the application processor hardware.	Mandatory for Class 1 and above	Business	Process
2.4.5.16	Software source code is developed, tested and maintained following defined repeatable processes.	Mandatory for Class 1 and above	Business	Process
2.4.5.17	The build environment and toolchain used to compile the application is run on a build system with controlled and auditable access.	Mandatory for Class 2 and above	Business	Process
2.4.5.18	The build environment and toolchain used to create the software is under configuration management and version control, and its integrity is validated regularly.	Mandatory for Class 2 and above	Business	Process
2.4.5.19	Where present, production software signing keys are under access control.	Mandatory for all classes	Business	Policy
2.4.5.20	The production software signing keys are stored and secured in a storage device compliant to FIPS-140-2/FIPS-140-3 level 2, or equivalent or higher standard.	Mandatory for Class 1 and above	Business	Policy
2.4.5.21	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.	Mandatory for Class 2 and above	System	Software
	For a device with no possibility of a software update, the conditions			

2.4.5.22	For a device with no possibility of a software update, the conditions for and period of replacement support should be clear. A replacement strategy must be communicated to the user, including a schedule for when the device should be replaced or isolated.	Mandatory for all classes	Business	Policy
2.4.5.23	All inputs and outputs are checked for validity e.g. use “Fuzzing” tests to check for acceptable responses or output for both expected (valid) and unexpected (invalid) input stimuli.	Mandatory for Class 2 and above	Business	Process
2.4.5.24	The software has been designed to meet the safety requirements identified in the risk assessment; for example in the case of unexpected invalid inputs, or erroneous software operation, the product does not become dangerous, or compromise security of other connected systems.	Mandatory for Class 2 and above	System	Software
2.4.5.25	Support for partially installing updates is provided for devices whose on-time is insufficient for the complete installation of a whole update (constrained devices).	Advisory for all classes	System	Software
2.4.5.26	Support for partially downloading updates is provided for devices whose network access is limited or sporadic.	Advisory for all classes	System	Software
2.4.5.27	Where real-time expectations of performance are present, update mechanisms must not interfere with meeting these expectations (e.g. by running update processes at low priority, or notifying the user of the priority and duration of the update and with the option of postponing or disabling the update).	Mandatory for all classes	System	Software
2.4.5.28	Where a device doesn’t support secure boot, upon a firmware update the user data and credentials should be re-initialised.	Mandatory for all classes	System	Hardware Software
2.4.5.29	Where a device cannot verify authenticity of updates itself (e.g. due to no cryptographic capabilities), only a local update by a physically present user is permitted and is their responsibility.	Mandatory for all classes	System	Software
2.4.5.30	An update to a device must be authenticated before it is installed. Where the update fails authentication, the device should, if possible, revert to the last known good (current stable) configuration/software image which was stored on the device.	Mandatory for all classes	System	Software
2.4.5.31	Withdrawn as duplicate requirement			
2.4.5.32	There is secure provisioning of cryptographic keys for updates during manufacture in accordance with industry standards.	Mandatory for Class 1 and above	Business	Policy
2.4.5.33	Memory locations used to store sensitive material (e.g. cryptographic keys, passwords/passphrases, etc.) are sanitised as soon as possible after they are no longer needed. These can include but are not limited to locations on the heap, the stack, and statically-allocated storage [ref 47][3]	Mandatory for Class 2 and above	System	Software

	allocated storage [ref 47] .			
2.4.5.34	Any caches which potentially store sensitive material are cleared flushed after memory locations containing sensitive material have been sanitised.	Mandatory for Class 3 and above	System	Hardware Software
2.4.5.35	An end-of-life policy shall be published which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to users and an update should be easy to implement. At the end of the support period, the device should reduce the risk of a latent vulnerability being exploited. This could be by indicating an error condition to the user or curtailing functionality. This action should be clearly communicated to the user during the procurement stage.	Mandatory for all classes	Business	Policy
2.4.5.36	Updates should be provided for a period appropriate to the device, and this period shall be made clear to a user when supplying the device. Updates should, where possible, be configurable to be automatically or manually installed. The supply chain partners should inform the user that an update is required.	Mandatory for all classes	Business	Policy
2.4.5.37	The device manufacturer should ensure that shared libraries (e.g. Clib or Crypto libraries) that deliver network and security functionalities have been reviewed or evaluated (note that the actual review or evaluation does not have to be conducted by the manufacturer if it has been conducted by another reputable organisation or government entity). Cryptography libraries should be re-reviewed for known security vulnerabilities on each update of the device.	Mandatory for Class 2 and above	Business	Policy
2.4.5.38	Maintenance changes should trigger full security regression testing.	Mandatory for Class 2 and above	Business	Policy
2.4.5.39	IoT devices must allow software updates to maintain security over the product lifetime.	Mandatory for Class 2 and above	Business	Policy
2.4.5.40	Hard-coded critical/ security parameters in device software source code shall not be used; if needed these should be injected in a separate (secure) process.	Mandatory for all classes	Business	Policy
2.4.5.41	Where the device is capable, it should check after initialization, and then periodically, whether security updates are available, either autonomously or as part of the support service. Otherwise, the support service should push updates to the device.	Mandatory for Class 1 and above	Business	Policy

Footnotes

1. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 [https://www.iso.org/standard/57018.html] ↩

2. Supply Chain of Trust by Hayden Povey of Secure Thingz and the IoTSF [http://www.newelectronics.co.uk/article-images/152099/P18-19.pdf] ↩

3. Examples of security vulnerability advisory programs: [https://www.us-cert.gov/report https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy] ↩

2.4.6 Device OS

Go to Detailed Requirements

This section's intended audience are the personnel responsible for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers quality. The term Operating System (OS) is below used for sake of brevity to imply all such options. Guidance is available from the IoTSF [ref 44][1] regarding Secure Operating Systems (part D).

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.6.1	The OS is implemented with relevant security updates prior to release.	Mandatory for Class 2 and above	Business	Process
2.4.6.2	Intentionally left blank to maintain requirement numbering	-		
2.4.6.3	All unnecessary accounts or logins have been disabled or eliminated from the software at the end of the software development process, e.g. development or debug accounts and tools.	Mandatory for Class 1 and above	System	Software
2.4.6.4	Files, directories and persistent data are set to minimum access privileges required to correctly function.	Mandatory for Class 1 and above	System	Software
2.4.6.5	Security parameters and passwords should not be hard-coded into source code or stored in a local file. If passwords absolutely must be stored in a local file, then the password file(s) are owned by, and are only accessible to and writable by, the Device's OS most privileged account and are obfuscated.	Mandatory for Class 1 and above	System	Software
2.4.6.6	All OS non-essential services have been removed from the product's software, image or file systems.	Mandatory for Class 1 and above	System	Software
2.4.6.7	All OS command line access to the most privileged accounts has been removed from the OS.	Mandatory for Class 1 and above	System	Software
2.4.6.8	All of the product's OS kernel and services or functions are disabled by default unless specifically required. Essential kernel, services or functions are prevented from being called by unauthorised external product level interfaces and applications.	Mandatory for Class 1 and above	System	Software
2.4.6.9	All software is operated at the least privilege level possible and only has access to the resources needed as controlled through appropriate access control mechanisms.	Mandatory for Class 1 and above	System	Software
2.4.6.10	All the applicable security features supported by the OS are enabled.	Mandatory for Class 1 and above	System	Software
2.4.6.11	The OS is separated from the application(s) and is only accessible via defined secure interfaces.	Mandatory for Class 1 and above	System	Software

2.4.6.12	The OS implements a separation architecture to separate trusted from untrusted applications.	Mandatory for Class 2 and above	System	Software
2.4.6.13	The product's OS kernel is designed such that each component runs with the least security privilege required (e.g. a microkernel architecture), and the minimum functionality needed (2.4.6.6 - 2.4.6.8 requires non-essential components are disabled or removed).	Mandatory for Class 2 and above	System	Software
2.4.6.14	The Product OS should be reviewed for known security vulnerabilities particularly in the field of cryptography prior to each update and after release. Cryptographic algorithms, primitives, libraries and protocols should be updateable to address any vulnerabilities.	Mandatory for Class 1 and above	System	Software
2.4.6.15	As per 2.4.10.5, the user interface is protected by an automatic session idle logout timeout function.	Mandatory for Class 1 and above	System	Software

Footnotes

1. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 [https://www.iso.org/standard/57018.html] ↩

2.4.7 Device Interfaces

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for device security. Guidance is available from the IoTSF Best Practice Guidelines [ref 44][1] regarding Credential Management (part F) and Network Connections (part H).

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.7.1	The product prevents unauthorised connections to it or other devices the product is connected to.	Mandatory for Class 1 and above	System	Software
2.4.7.2	The network component and firewall (if applicable) configuration has been reviewed and documented for the required/defined secure behaviour.	Mandatory for Class 1 and above	Business	Process
2.4.7.3	To prevent bridging of security domains within products with network interfaces, forwarding functions should be blocked by default.	Mandatory for Class 1 and above	System	Software
2.4.7.4	Devices support only the versions of application layer protocols that have been reviewed and evaluated against publicly known vulnerabilities.	Mandatory for Class 1 and above	Business	Process
2.4.7.5	If a potential unauthorised change is detected (e.g.: an access fails authentication or integrity checks), the device should alert the user/administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function. Failed attempts should be logged, but without providing any information about the failure to the initiator.	Mandatory for Class 1 and above	System	Software
2.4.7.6	All the product's unused ports (or interfaces) are closed and only the necessary ones are active.	Mandatory for Class 1 and above	Business	Process
2.4.7.7	If a connection requires a password or passcode or passkey for connection authentication, the factory issued or reset password is unique to each device.	Mandatory for all classes	Business	Process
2.4.7.8	Where using initial pairing process, a Strong Authentication shall be used, requiring physical interaction with the device or possession of a shared secret.	Mandatory for Class 1 and above	System	Software
2.4.7.9	Where a wireless interface has an initial pairing process, the passkeys are changed from the factory issued, or reset password prior to providing normal service.	Mandatory for all classes	Business	Policy
2.4.7.10	For any Wi-Fi connection, WPA-2 AES [ref 51][2] or a similar strength encryption has been used. Migration to the latest standard should be planned.(e.g. WPA3). Older insecure protocols such as WEP, WPA/WPA2 (Auto), WPA-TKIP and WPA-2 TKIP/AES (Mixed Mode) are disabled.	Mandatory for Class 1 and above	System	Software

2.4.7.11	Where WPA-2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	Mandatory for Class 1 and above	System	Software
2.4.7.12	All network communications keys are stored securely, in accordance with industry standards.	Mandatory for Class 1 and above	System	Software
2.4.7.13	Where a TCP protocol, such as MQTT, is used, it is protected by a TLS connection with no known vulnerabilities.	Mandatory for Class 1 and above	System	Software
2.4.7.14	Where a UDP protocol is used, such as CoAP, it is protected by a DTLS connection with no known vulnerabilities.	Mandatory for Class 1 and above	System	Software
2.4.7.15	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][3] or OWASP. Where insecure ciphers suites are identified they shall be removed from the product.	Mandatory for Class 1 and above	Business	Process
2.4.7.16	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.	Mandatory for Class 1 and above	Business	Process
2.4.7.17	Where there is a loss of communications or availability it shall not compromise the local integrity of the device.	Mandatory for Class 1 and above	System	Software
2.4.7.18	The product only initialises and enables the communications interfaces, network protocols, application protocols and network services necessary for the product's operation.	Mandatory for Class 1 and above	System	Software
2.4.7.19	Communications protocols should be latest versions with no publicly known vulnerabilities and/or appropriate for the product.	Mandatory for Class 1 and above	Business	Policy
2.4.7.20	Post product launch, communications protocols should be reviewed throughout the product life cycle against publicly known vulnerabilities and changed to the most secure versions available if appropriate.	Mandatory for Class 1 and above	Business	Policy
2.4.7.21	If a factory reset is made, the device should warn that secure operation may be compromised until updated.	Mandatory for Class 1 and above	System	Software
2.4.7.22	Where RF communications are enabled (e.g., ZigBee, etc.) antenna power is configured to limit ability of mapping assets to	Advisory for all classes	System	Software

	limit attacks such as WAR-Driving.			
2.4.7.23	Protocol anonymity features are enabled in protocols (e.g., Bluetooth) to limit location tracking capabilities.	Advisory for all classes	System	Software
2.4.7.24	As far as reasonably possible, devices should remain operating and locally functional in the case of a loss of network connection.	Mandatory for Class 1 and above	System	Software
2.4.7.25	Following restoration of power or network connection, devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect, which collectively could overwhelm a network.	Mandatory for Class 1 and above	System	Software

Footnotes

1. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 [https://www.iso.org/standard/57018.html] ↩

2. NCSC guidance on TLS management [https://www.ncsc.gov.uk/guidance/tls-external-facing-services] ↩

3. NIST Special Publication 800-131A Revision 1 "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" November 2015 ↩

2.4.8 Authentication & Authorisation

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for the security of the IoT systems interfaces and authentication processes. Guidance is available from the IoTSF Best Practice Guides [ref 44][1] regarding Credential Management (part F).

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.8.1	The product contains a unique and tamper-resistant device identifier. E.g.: the chip serial number or other unique silicon identifier, for example to bind code and data to a specific device hardware. This is to mitigate threats from cloning and also to ensure authentication may be done assuredly using the device identifier e.g. using a device certificate containing the device identifier.	Mandatory for all classes	System	Hardware
2.4.8.2	Where the product has a secure source of time there is a method of validating its integrity.	Mandatory for Class 1 and above	System	Software
2.4.8.3	Where a user interface password is used for login authentication, the factory issued or reset password is randomly unique for every device in the product family. If a password-less authentication is used the same principles of uniqueness apply.	Mandatory for all classes	System	Software
2.4.8.4	The product does not accept the use of null or blank passwords.	Mandatory for all classes	System	Software
2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.	Mandatory for all classes	System	Software
2.4.8.6	Password entry follows industry standard practice on password length, characters from the groupings and special characters.	Mandatory for all classes	System	Software
2.4.8.7	The product has defence against brute force repeated login attempts, such as exponentially increasing retry attempt delays.	Mandatory for Class 1 and above	System	Software
2.4.8.8	The product securely stores any passwords using an industry standard cryptographic algorithm, compliant with an industry standard.	Mandatory for Class 1 and above	System	Software
2.4.8.9	The product supports access control measures to the root/highest privilege account to restrict access to sensitive information or system processes.	Mandatory for Class 1 and above	System	Software
2.4.8.10	The access control privileges are defined, justified and documented.	Mandatory for Class 1 and above	Business	Process
2.4.8.11	The product only allows controlled user account access; access using anonymous or guest user accounts is not supported without justification.	Mandatory for Class 1 and above	System	Software

2.4.8.12	The product allows the factory issued or OEM login accounts to be disabled or erased or renamed when installed or commissioned.	Advisory for all classes	System	Software
2.4.8.13	The product supports having any or all of the factory default user login passwords altered when installed or commissioned.	Mandatory for all classes	Business	Process
2.4.8.14	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.	Mandatory for Class 1 and above	Business	Process
2.4.8.15	Where passwords are entered on a user interface, the actual pass phrase is obscured by default.	Mandatory for Class 1 and above	System	Software
2.4.8.16	The product allows an authorised and complete factory reset of all of the device's authorisation information.	Advisory for all classes	System	Software
2.4.8.17	Where the product has the ability to remotely recover from attack, it should rely on a known good state, to enable safe recovery and updating of the device, but should limit access to sensitive assets until the devices is in a known secure condition.	Mandatory for Class 1 and above	System	Software
2.4.8.18	Devices are provided with a RoT-backed unique authenticable logical identity.	Mandatory for Class 1 and above	System	Software

Footnotes

1. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 [https://www.iso.org/standard/57018.html] ↩

2.4.9 Encryption & Key Management

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for the security of the IoT systems hardware key management and encryption. Guidance is available from the IoTSF [ref 44][1] regarding Encryption (Part G).

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.9.1	Intentionally left blank to maintain requirement numbering	-		
2.4.9.2	If present, a true random number generator source has been validated for true randomness.	Mandatory for Class 2 and above	System	Hardware
2.4.9.3	There is a process for secure provisioning of security parameters and keys that includes random and individual (unique) generation, distribution, update, revocation and destruction.	Mandatory for Class 2 and above	Business	Process
2.4.9.4	There is a secure method of key insertion that protects keys against copying.	Mandatory for Class 1 and above	System	Software
2.4.9.5	All the product related cryptographic functions have no publicly known unmitigated weaknesses in the algorithms or implementation, for example MD5 and SHA-1 are not used.	Mandatory for Class 1 and above	Business	Process
2.4.9.6	All the product related cryptographic functions are sufficiently secure for the lifecycle of the product, or cryptographic algorithms and primitives should be updateable ("cryptoagility")".	Mandatory for Class 1 and above	Business	Process
2.4.9.7	The product stores all sensitive unencrypted parameters (e.g. keys) in a secure, tamper-resistant location.	Mandatory for Class 1 and above	System	Hardware
2.4.9.8	The cryptographic key chain used for signing production software is different from that used for any other test, development or other software images or support requirement.	Advisory for all classes	System	Software
2.4.9.9	In device manufacture, all asymmetric encryption private keys that are unique to each device are secured. They must be truly randomly internally generated or securely programmed into each device.	Mandatory for Class 2 and above	Business	Process
2.4.9.10	All key lengths are sufficient for the level of assurance required.	Mandatory for Class 2 and above	Business	Policy
2.4.9.11	In systems with many layered sub devices, key management should follow best practice.	Mandatory for all classes	Business	Policy

Footnotes

1. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 [https://www.iso.org/standard/57018.html] ↩

2.4.10 Web User Interface

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services Web Systems. Guidance is available from the IoTSF [ref 44][1] regarding Application Security (part E), and Credential Management (part F).

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.10.1	Where the product or service provides a web based user interface, Authentication is secured using current best practice cryptography.	Mandatory for Class 1 and above	System	Software
2.4.10.2	Where the product or service provides a web browser based interface, access to any restricted/administrator area or functionality shall require authentication.	Mandatory for Class 1 and above	System	Software
2.4.10.3	Where the product or service provides a web based management interface, Authentication is secured using current best practice cryptography.	Mandatory for Class 1 and above	System	Software
2.4.10.4	Where a web user interface password is used for login authentication, the initial password or factory reset password is unique for every device in the product family.	Mandatory for all classes	System	Software
2.4.10.5	The web user interface is protected by an automatic session idle logout timeout function.	Mandatory for Class 1 and above	System	Software
2.4.10.6	User passwords are not stored in plain text.	Mandatory for all classes	System	Software
2.4.10.6.1	Strong passwords are required, and a random salt value is incorporated with the password.	Mandatory for Class 1 and above	System	Software
2.4.10.7	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	Mandatory for Class 1 and above	System	Software
2.4.10.8	The web user interface shall follow good practice guidelines.	Mandatory for Class 1 and above	Business	Policy
2.4.10.9	A vulnerability assessment has been performed before deployment, and is repeated periodically throughout the lifecycle of the service or product.	Mandatory for Class 1 and above	Business	Process
2.4.10.10	All data being transferred over interfaces should be validated where appropriate. This could include checking the data type, length, format, range, authenticity, origin and frequency.	Mandatory for Class 1 and above	System	Software
2.4.10.11	Sanitize input in Web applications by using URL encoding or HTML encoding to wrap data and treat it as literal text rather than executable script	Mandatory for Class 1 and above	System	Software

	than executable script.	above		
2.4.10.12	All inputs and outputs are validated using for example an allow list (formerly 'whitelist') containing authorised origins of data and valid attributes of such data.	Mandatory for Class 1 and above	System	Software
2.4.10.13	Administration Interfaces are accessible only by authorized operators. Mutual Authentication is used over administration interfaces, for example, by using certificates.	Mandatory for Class 1 and above	System	Software
2.4.10.14	Reduce the lifetime of sessions to mitigate the risk of session hijacking and replay attacks. (For example to reduce the time an attacker has to capture a session cookie and use it to access an application).	Mandatory for Class 1 and above	System	Software
2.4.10.15	All inputs and outputs are checked for validity. Tests to include both expected (valid) and unexpected (invalid) input stimuli.	Mandatory for Class 1 and above	Business	Process
2.4.10.16	Web Interfaces should be developed using best practice secure coding techniques and server frameworks.	Mandatory for Class 1 and above	Business	Process
2.4.10.17	Password entry follows industry standard practice.	Mandatory for all classes	Business	Process
2.4.10.18	Web interface should provide a simple method (one to two clicks) to initiate any security update to the end device	Mandatory for all classes	Business	Process
2.4.10.19	Any personal data communicated between the web interface and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	Mandatory for all classes	Business	Process

Footnotes

1. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 [https://www.iso.org/standard/57018.html] ↩

2.4.11 Mobile Application

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services Mobile Application. Guidance is available from the IoTSF [ref 44][1] regarding Application Security (part E) and Credential Management (part F).

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.11.1	Where an application's user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family.	Mandatory for all classes	System	Software
2.4.11.2	Password entry follows industry standard practice.	Mandatory for all classes	System	Software
2.4.11.3	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.	Mandatory for Class 1 and above	System	Software
2.4.11.4	Where the application communicates with a product related remote server(s), or device, it does so over a secure connection.	Mandatory for Class 1 and above	System	Software
2.4.11.5	The product securely stores any passwords using an industry standard cryptographic algorithm.	Mandatory for Class 1 and above	System	Software
2.4.11.6	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	Mandatory for Class 1 and above	System	Software
2.4.11.7	All data being transferred over interfaces should be validated where appropriate. This could include checking the data type, length, format, range, authenticity, origin and frequency.	Mandatory for Class 1 and above	System	Software
2.4.11.8	Secure Administration Interfaces; It is important that configuration management functionality is accessible only by authorised operators and administrators. Enforce Strong Authentication over administration interfaces, for example, by using certificates.	Mandatory for Class 1 and above	System	Software
2.4.11.9	All application inputs and outputs are validated using for example an allowed-list containing authorised origins of data and valid attributes of such data.	Mandatory for Class 1 and above	System	Software
2.4.11.10	Mobile Apps should be developed using best practice secure coding techniques and server frameworks.	Mandatory for Class 1 and above	System	Software
2.4.11.11	App interface should provide a simple method (one to two clicks) to initiate any security update to the end device.	Mandatory for Class 1 and above	System	Software

2.4.11.12	Access to device functionality via a network/web browser interface in the initialized state should only be permitted after successful Authentication using current best practice secure cryptographic modules.	Mandatory for Class 1 and above	System	Software
2.4.11.13	Any personal data communicated between the mobile app and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	Mandatory for Class 1 and above	System	Software

Footnotes

1. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 [https://www.iso.org/standard/57018.html] ↩

2.4.12 Privacy

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for Data Protection and Privacy regulatory compliance.

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.12.1	The product/service stores the minimum amount of Personal Information from users required for the operation of the service.	Mandatory for Class 1 and above	Business	Policy
2.4.12.2	The product/service ensures that all Personal Information is encrypted for confidentiality (both when stored and if communicated out of the device) and only accessible after successful authentication and authorisation. Note: authentication only proves who you are, but authorisation confirms if you are allowed access to the PI. The cryptography must be of sufficient strength to protect the Personal Information for however long it is expected to be retained (or remain confidential).	Mandatory for Class 3 and above	Business	Policy
2.4.12.3	The product/service ensures that only authorised personnel have access to personal data of users.	Mandatory for Class 1 and above	Business	Policy
2.4.12.4	The product/service ensures that Personal Information is anonymised whenever possible and in particular in any reporting.	Mandatory for Class 1 and above	Business	Policy
2.4.12.5	The Product Manufacturer or Service Provider shall ensure that a data retention policy is in place and documented for users.	Mandatory for Class 1 and above	Business	Policy
2.4.12.6	There is a method or methods for the product owner to be informed about what Personal Information is collected, why, where it will be stored and processed, and by whom and for what purposes. This includes sensing capabilities, such as sound or video recording, biometrics, location, etc.	Mandatory for Class 1 and above	Business	Process
2.4.12.7	There is a method or methods for each user to check/verify what Personal Information is collected.	Mandatory for Class 1 and above	Business	Process
2.4.12.8	The product / service can be made compliant with the local and/or regional Personal Information protection legislation where the product is to be sold. For example GDPR [ref 14][1].	Mandatory for Class 1 and above	Business	Process
2.4.12.9	The supplier or manufacturer of any device shall provide documented information to end users about how the device(s) functions within the end user's network may affect their privacy.	Advisory for all classes	Business	Process
2.4.12.10	The supplier or manufacturer of any devices or devices shall provide clear information about how the device(s) should be set	Mandatory for all classes	Business	Process

	up to maintain the end user's privacy and security.			
2.4.12.11	The supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal or replacement shall be carried out to maintain the end user's privacy and security, including deletion of all personal information from the device and any associated services.	Mandatory for Class 1 and above	Business	Process
2.4.12.12	The supplier or manufacturer of any devices or services shall provide clear information about the end user's responsibilities to maintain the devices and/or services privacy and security.	Mandatory for Class 1 and above	Business	Process
2.4.12.13	Security of devices and services should be designed with usability in mind (reducing user decision points that may have a detrimental impact on privacy and security).	Mandatory for Class 1 and above	System	Software
2.4.12.14	The product or service only records audio/visual/or any other data in accordance with the authorisation of the user (e.g., no passive recording without explicit authorisation).	Mandatory for Class 1 and above	System	Software
2.4.12.15	The supplier or manufacturer performs a privacy impact assessment (PIA) to identify Personally Identifiable Information (PII) and design approaches for safeguarding user privacy compliant with the legal requirements of the user's location (e.g. GDPR). This should extend to data gathered via Web APIs from third party platform suppliers.	Advisory for all classes	Business	Process

Footnotes

1. Overview of the General Data Protection Regulations (GDPR), ICO: [https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr] ↩

2.4.13 Cloud And Network Elements

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services Cloud or Network Systems.

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.13.1	All the product related cloud and network elements have the latest operating system(s) security updates implemented and processes are in place to keep them updated.	Mandatory for Class 2 and above	Business	Process
2.4.13.2	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.	Mandatory for Class 1 and above	System	Software
2.4.13.3	All product related web servers have their webserver HTTP trace and trace methods disabled.	Mandatory for Class 1 and above	System	Software
2.4.13.4	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.	Mandatory for Class 1 and above	System	Software
2.4.13.5	The Product Manufacturer or Service Provider has a process to monitor the relevant security advisories to ensure all the product related web servers use protocols with no publicly known weaknesses.	Mandatory for Class 1 and above	Business	Process
2.4.13.6	The product related web servers support appropriately secure TLS/DTLS ciphers and disable/remove support for deprecated ciphers.	Advisory for all classes	System	Software
2.4.13.7	The product related web servers have repeated renegotiation of TLS connections disabled.	Mandatory for Class 1 and above	System	Software
2.4.13.8	The related servers have unused IP ports disabled.	Mandatory for Class 1 and above	System	Software
2.4.13.9	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.	Mandatory for Class 1 and above	System	Software
2.4.13.10	Where a product related to a webserver encrypts communications using TLS, certificate pinning is implemented.	Advisory for all classes	System	Software
2.4.13.11	All the related servers and network elements prevent the use of null or blank passwords.	Mandatory for Class 1 and above	System	Software
2.4.13.12	Intentionally left blank to maintain requirement numbering	-		
2.4.13.13	Intentionally left blank to maintain requirement numbering	-		
	All the related servers and network elements enforce	Mandatory for		

2.4.13.14	passwords that follows industry good practice.	Class 1 and above	System	Software
2.4.13.15	Brute force attacks are impeded by introducing escalating delays following failed user account login attempts, and/or a maximum permissible number of consecutive failed attempts.	Mandatory for Class 1 and above	System	Software
2.4.13.16	All the related servers and network elements store any passwords using a cryptographic implementation using industry standard cryptographic algorithms.	Mandatory for Class 1 and above	System	Software
2.4.13.17	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	Mandatory for Class 1 and above	System	Software
2.4.13.18	All the related servers and network elements prevent anonymous/guest access except for read only access to public information.	Mandatory for Class 1 and above	System	Software
2.4.13.19	If run as a cloud service, the service meets industry standard cloud security principles.	Advisory for all classes	System	Software
2.4.13.20	Where a Product or Services includes any safety critical or life-impacting functionality, the services infrastructure shall incorporate protection against DDOS attacks, such as dropping of traffic or sink-holing.	Mandatory for Class 2 and above	System	Software
2.4.13.21	Where a Product or Service includes any safety critical or life-impacting functionality, the services infrastructure shall incorporate redundancy to ensure service continuity and availability.	Mandatory for Class 1 and above	System	Software
2.4.13.22	Input data validation should be maintained in accordance with industry best practice methods.	Mandatory for Class 1 and above	System	Software
2.4.13.23	If run as a cloud service, the cloud service TCP based communications (such as MQTT connections) are encrypted and authenticated using the latest TLS standard.	Mandatory for Class 1 and above	System	Software
2.4.13.24	If run as a cloud service, UDP-based communications are encrypted using the latest Datagram Transport Layer Security (DTLS).	Mandatory for Class 1 and above	System	Software
2.4.13.25	Where device identity and/or configuration registries (e.g., "thing shadows") are implemented to "on-board" devices within a cloud service, the registries are configured to restrict access to only authorized administrators.	Mandatory for Class 1 and above	System	Software
2.4.13.26	Product-related cloud services bind API keys to specific IoT applications and are not installed on non-authorised devices.	Mandatory for Class 2 and above	System	Software

2.4.13.27	Product-related cloud services API keys are not hard-coded into devices or applications.	Mandatory for all classes	System	Software
2.4.13.28	If run as a cloud service, privileged roles are defined and implemented for any gateway/service that can configure devices.	Mandatory for Class 2 and above	System	Software
2.4.13.29	Product-related cloud service databases are encrypted during storage.	Mandatory for Class 1 and above	System	Software
2.4.13.30	Product-related cloud service databases restrict read/write access to only authorized individuals, devices and services.	Mandatory for Class 1 and above	System	Software
2.4.13.31	Product-related cloud services are designed using a defence-in-depth architecture consisting of Virtual Private Clouds (VPCs), firewalled access, and cloud-based monitoring.	Mandatory for Class 1 and above	System	Software
2.4.13.32	When implemented as a cloud service, all remote access to cloud services is via secure means (e.g. SSH).	Mandatory for Class 1 and above	System	Software
2.4.13.33	Product-related cloud services monitor for compliance with connection policies and report out-of-compliance connection attempts.	Mandatory for Class 2 and above	System	Software
2.4.13.34	IoT edge devices should connect to cloud services using secure hardware and services (e.g. TLS using private keys stored in secure hardware).	Mandatory for Class 1 and above	System	Hardware
2.4.13.35	Any personal data communicated between the mobile app and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	Mandatory for Class 2 and above	System	Software
2.4.13.36	Subject to user permission, telemetry data from the device should be analysed for anomalous behaviour to detect malfunctioning or malicious activity.	Mandatory for Class 2 and above	System	Software

2.4.14 Secure Supply Chain Production

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services' Supply Chain and Production.

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.14.1	Ensure the entire production test and calibration software used during manufacture is removed or secured before the product is dispatched from the factory. This is to prevent alteration of the product post manufacture when using authorised production software, for example hacking of the RF characteristics for greater RF ERP. Where such functionality is required in a service centre, it shall be removed upon completion of any servicing activities.	Mandatory for Class 2 and above	System	Software
2.4.14.2	Any hardware design files, software source code and final production software images with full descriptive annotations are stored encrypted in off-site locations or by a 3rd party Escrow service.	Advisory for all classes	Business	Process
2.4.14.3	In manufacture, all the devices are logged by the product vendor, utilizing unique tamper resistant identifiers such as serial number so that cloned or duplicated devices can be identified and either disabled or prevented from being used with the system.	Mandatory for Class 1 and above	Business	Process
2.4.14.4	The production system for a device has a process to ensure that any devices with duplicate serial numbers are not shipped and are either reprogrammed or destroyed.	Mandatory for Class 1 and above	Business	Process
2.4.14.5	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.	Advisory for all classes	Business	Process
2.4.14.6	A securely controlled area and process shall be used for device provisioning where the production facility is untrusted.	Advisory for all classes	Business	Process
2.4.14.7	A cryptographic protected ownership proof shall be transferred along the supply chain and extended if a new owner is added in the chain. This process shall be based on open standards such as Enhanced Privacy ID, Certificates per definition in ISO 20008/20009 [ref 42][1].	Mandatory for Class 1 and above	Business	Process
2.4.14.8	An auditable manifest of all libraries used within the product (open source, etc.) is maintained to inform vulnerability management throughout the device lifecycle and whole of the support period.	Advisory for all classes	Business	Process
2.4.14.9	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 in accordance with industry standard FIPS140-2 [ref 5][2] or equivalent. Any secret key programmed into a product at manufacture is unique to that	Mandatory for Class 2 and above	Business	Process

	individual device, i.e. no global secret key is shared between multiple devices, unless this is required by a licensing authority.			
2.4.14.10	An authorised actor in physical possession of a device can discover and authenticate its ROT-backed logical identity e.g. for inspection, verification of devices being onboarded (this may need electrical connection).	Mandatory for Class 2 and above	Business	Process
2.4.14.11	Devices are shipped with readily-accessible physical identifiers derived from their ROT-backed IDs. This is to facilitate both tracking through the supply chain and for the user to identify the device-type/model and SKU throughout the support period.	Mandatory for Class 1 and above	Business	Process
2.4.14.12	IoT devices' RoT-backed logical identity is used to identify them in logs of their physical chain of custody. This is to facilitate tracking through the supply chain.	Mandatory for Class 2 and above	Business	Process
2.4.14.13	Products ship with information (documents or URL) about their operations and normal behaviour e.g. domains contacted, volume of messaging, Manufacturer Usage Description (MUD).	Mandatory for Class 2 and above	Business	Process
2.4.14.14	Procedures for proper disposal of scrap product exist at manufacturing facilities, and compliance is monitored. This to prevent scrap entering grey markets.	Mandatory for Class 2 and above	Business	Process
2.4.14.15	Production assets are encrypted during transport to the intended production facility, area or system, or delivered via private channel. Examples of production assets include firmware images, device certificate CA keys, onboarding credentials, production tools and manufacturing files.	Mandatory for Class 2 and above	Business	Process
2.4.14.16	Device firmware images and configuration data are secured against unauthorised modification in manufacturing environments, including during programming. If IP protection is required then the images and data need to be protected against unauthorised access.	Mandatory for Class 2 and above	Business	Process
2.4.14.17	Steps have been taken to prevent inauthentic devices from being programmed with confidential firmware images and configuration data. This is to prevent IP theft and reverse engineering.	Mandatory for Class 2 and above	Business	Process
2.4.14.18	Steps have been taken to prevent inauthentic devices from being signed into certificate chains of trust or otherwise onboarded. For example, a policy or checklist describing which devices may be onboarded exists and is followed.	Mandatory for Class 2 and above	Business	Process
2.4.14.19	Device certificate signing keys and other onboarding credentials are secured against unauthorised access. For example, they may be stored encrypted and managed or created by an HSM and delivered by the secure signing process.	Mandatory for Class 2 and above	Business	Process

2.4.14.20	If time critical delivery of products is needed, availability of production resources accessed in real time over the Internet is assured, by providing them with alternative access channels not susceptible to DOS attacks.	Mandatory for all classes	Business	Process
2.4.14.21	Operators of production servers, computers and network equipment keep their software up to date and monitor them for signs of compromise e.g. unusual activity.	Mandatory for Class 2 and above	Business	Process
2.4.14.22	The OEM retains authorisation of secure production control methods to prevent a third party manufacturer (CEM etc.) from producing overproduction and/or unauthorised devices.	Mandatory for Class 2 and above	Business	Process
2.4.14.23	The supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal or replacement shall be carried out to maintain the end user's privacy and security, including deletion of all personal information from the device and any associated services.	Mandatory for Class 2 and above	Business	Process
2.4.14.24	An end of life disposal process shall be provided to ensure that retired devices are permanently disconnected from their cloud services and that any confidential user data is securely erased from both the device and the cloud services.	Mandatory for Class 1 and above	Business	Process
2.4.14.25	Where contractual supply arrangements and software licence agreements allow, a software bill of materials (SBOM) shall be available and notified (URL) to customers with product documentation.	Mandatory for Class 2 and above	Business	Process

Footnotes

1. EU ENISA guidance of Cyber Security Risk Management [https://www.enisa.europa.eu/topics/threat-risk-management/risk-management] ↩

2. FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001. [http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf] ↩

2.4.15 Configuration

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for the security of the device and IoT Services configurations.

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.15.1	The configuration of the device and any related web services is secure and tamper resistant i.e. sensitive configuration parameters should only be changeable by authorised people (evidence should list the parameters and who is authorised to change e.g. Owners / Guests). Sensitive parameters include cryptographic configuration settings.	Mandatory for Class 1 and above	Business	Process
2.4.15.2	Updates to configuration should be provisioned securely and just-in-time, maintaining consistency . Irrelevant components of the configuration must be removed at the same time.	Mandatory for Class 1 and above	Business	Process
2.4.15.3	The manufacturer should provide users with guidance on how to check whether their device is securely set up.	Mandatory for Class 1 and above	Business	Process

2.4.16 Device Ownership Transfer

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for Data Protection and Device Ownership management.

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.16.1	Where a device may have its ownership transferred to a different owner, the supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal or replacement shall be carried out to maintain the end user's privacy and security, including deletion of all Personal Information from the device and any associated services. This option must be available when a transfer of ownership occurs or when an end user wishes to delete their Personal Information from the service or device.	Mandatory for Class 1 and above	Business	Process
2.4.16.2	Where a device User wishes to dispose of the device or end the service, the supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal or replacement shall be carried out to maintain the end user's privacy and security, including secure erasure of all Personal Information from the device and deletion of personal information from any associated services (other than that required for legitimate reasons such as billing). A clear confirmation is provided to the user. Examples of a user include a renter of accommodation, a vehicle or medical aids.	Mandatory for Class 1 and above	Business	Process
2.4.16.3	The Service Provider should not have the ability to do a reverse lookup of device ownership from the device identity.	Mandatory for Class 1 and above	Business	Process
2.4.16.4	If ownership change is required/allowed, the device must have an irrevocable method of decommissioning and recommissioning.	Mandatory for Class 1 and above	System	Software
2.4.16.5	The device registration with the Service Provider shall use a secure connection.	Mandatory for Class 1 and above	Business	Process
2.4.16.6	The device manufacturer ensures that the exposed identity of the device cannot be linked by unauthorised actors to the end user, to ensure anonymity and comply with relevant local data privacy laws e.g. GDPR [ref 14][1] in the EU.	Mandatory for Class 1 and above	Business	Policy
2.4.16.7	Where transfer of a device to a new end user is supported, user settings and confidential user data on the device should be reliably erasable by triggering a user reset function. This is so the new user can be confident in the device state and also so the previous user can be confident their data has been unrecoverably erased to maintain confidentiality (see alongside 2.4.12.13 and 2.4.12.11).	Mandatory for Class 1 and above	Business	Policy

Footnotes

1. Overview of the General Data Protection Regulations (GDPR), ICO: [https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr] ↩

3.1 References & Standards

The following organisations, publications and/or standards have been used for the source of references in this document:

- 3GPP (3rd Generation Partnership Project)
- CSA (Cloud Security Alliance)
- DoD (US Department of Defense)
- ENISA (European Union Agency for Network and Information Security)
- ETSI (European Telecommunications Standards Institute)
- EU (European Union)
- FIPS (US Federal Information Processing Standard)
- GSMA (GSM Association)
- IETF (Internet Engineering Task Force)
- IoTSF (Internet of Things Security Foundation)
- ISO (International Standard Organisation)
- JTAG (Joint Test Action Group)
- NCSC (UK National Cyber Security Centre)
- NIST (US National Institute of Standards and Technology)
- OWASP (Open Web Application Security Project)

The following references are used in this document:

1. NIST Special Publication 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" January 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf http://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 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

4. Special Publication 800-22 Revision 1a "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" April 2010 https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762

5. FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

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 https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4_marked_changes.pdf

7. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012 Version 3.1 Revision 4 CCMB-2012-09-002 https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf

8. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012 Version 3.1 Revision 4 https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf

9. Draft Framework for Cyber-Physical Systems; NIST; October 2016 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

10. UK Government advice on Password Guidance, Simplifying your approach, CESG and CPNI Sept 2015: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

11. DoDI-8500.2 IA Controls: http://www.dote.osd.mil/tempguide/index.html

12. NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122, NIST, April 2010: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

13. Key definitions of the Data Protection Act, ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions

14. Overview of the General Data Protection Regulations (GDPR), ICO: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr

15. TS-0003 Annex J (normative): List of Privacy Attributes and Clause 11 Privacy Protection Architecture using Privacy Policy Manager (PPM) https://www.onem2m.org/technical/published-specifications

16. Example of IoT application ID registry and possible privacy profile registry https://www.onem2m.org/images/ppt/TP-2017-0200-AppID_Registry_A_Foundation_for_Trusted_Interoperability.pdf

17. 3GPP TS33.117. Catalogue of general security assurance requirements produced by ESTI https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928

18. Cloud Security Alliance, Cloud Security Alliance is a not-for-profit organization promoting best practices for security assurance within Cloud Computing https://cloudsecurityalliance.org

19. IoTSF Vulnerability Disclosure Guidelines can be found https://iotsecurityfoundation.org/best-practice-guidelines

20. NIST National Institute of Standards and Technology www.nist.gov

21. NIST Cyber Security Framework https://www.nist.gov/cyberframework

22. Octave, programming language https://www.gnu.org/software/octave/

23. UK Cyber Essentials: UK government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks https://www.cyberaware.gov.uk/cyberessentials

24. UK Government Cloud Security Principles is for consumers and providers using cloud services https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

25. IETF – RFC2119 "Key words for use in RFCs to Indicate Requirement Levels" https://www.ietf.org/rfc/rfc2119.txt

26. NIST SP800-63b Revision 1" NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management" June 2017 https://pages.nist.gov/800-63-3/sp800-63b.html

27. ENISA "Algorithms, Key Sizes and Parameters Report – 2013" https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report

28. IETF RFC7525 "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" https://tools.ietf.org/html/rfc7525

29. SSL Labs "SSL-and-TLS-Deployment-Best-Practices" 31 March 2017 https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

30. OWASP "Transport Layer Protection Cheat Sheet" https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

31. OWASP Certificate and Public Key Pinning https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

32. NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" – SC-5 Denial of Service Protection https://nvd.nist.gov/800-53/Rev4/control/SC-5

33. NIST 800-53, Revision 4, "Security Controls and Assessment Procedures for Federal Information Systems and Organizations" - SI10 Information Input Validation https://nvd.nist.gov/800-53/Rev4/control/SI-10

34. NIST Special Publication 800–167 "Guide to Application Whitelisting" http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

35. NIST SP 800-37 Rev. 1 "Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach Risk Management Framework" https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final or Octave from ENISA

36. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), an approach for managing information security risks. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51546

37. Supply Chain of Trust by Hayden Povey of Secure Thingz and the IoTSF http://www.newelectronics.co.uk/article-images/152099/P18-19.pdf

38. Static Code Analysis Tools https://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html

39. Bluetooth Numeric Comparison https://csrc.nist.gov/publications/detail/sp/800-121/rev-1/archive/2012-06-11 page 14

40. UK Government Cyber security risk assessment guidance https://www.ncsc.gov.uk/guidance/risk-management-collection

41. NIST Special Publication 800-30 guidance for conducting risk assessments https://www.nist.gov/publications/guide-conducting-risk-assessments

42. EU ENISA guidance of Cyber Security Risk Management https://www.enisa.europa.eu/topics/threat-risk-management/risk-management

43. Security Policy ISO/IEC Standards for Vulnerability Disclosures ISO/IEC 29147 and ISO/IEC 30111 http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip and https://www.iso.org/standard/53231.html

44. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 https://www.iso.org/standard/57018.html

45. IoTSF Best Practice Guidelines for Connected Consumer Products V1.1 https://www.iotsecurityfoundation.org/best-practice-guidelines/#ConnectedConsumerProducts includes at time of publication individual guidelines for the following topics:

A. Classification of data

B. Physical security

C. Device secure boot

D. Secure operating system

E. Application security

F. Credential management

G. Encryption

H. Network connections

J. Securing software updates

K. Logging

L. Software update policy

46. CIA Triad has no original source, but for more info visit: https://www.techrepublic.com/blog/it-security/the-cia-triad

47. Examples of security vulnerability advisory programs: https://www.us-cert.gov/report and https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy

48. Example of memory sanitisation:

SEI CERT C Coding Standard Recommendation MEM03-C: "Clear sensitive information stored in reusable resources" https://wiki.sei.cmu.edu/confluence/display/c/MEM03-C.+Clear+sensitive+information+stored+in+reusable+resources

ISO/IEC TR 24772:2013 "Information technology -- Programming languages -- Guidance to avoiding vulnerabilities in programming languages through language selection and use" "Sensitive Information Uncleared Before Use" https://www.iso.org/standard/61457.html

Other references:

MITRE CWE-226 "Sensitive Information Uncleared Before Release" https://cwe.mitre.org/data/definitions/226.html

CWE-244 "Improper Clearing of Heap Memory Before Release ('Heap Inspection')" https://cwe.mitre.org/data/definitions/244.html

49. NCSC password guidance https://www.ncsc.gov.uk/guidance/password-collection

50. Privacy Impact Assessment advice can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ and https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf

51. NCSC guidance on TLS management https://www.ncsc.gov.uk/guidance/tls-external-facing-services

52. WPA - Wi-Fi Protected Access is the name given to wireless security standard IEEE 802.11i-2004 https://standards.ieee.org/standard/802_11i-2004.html

53. The ETSI Technical Committee on Cybersecurity EN 303 645 version 2.1.1 "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements" June 2020, , a standard for cybersecurity in the Internet of Things that establishes a security baseline for internet-connected consumer products and provides a basis for future IoT certification schemes. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

54. NIST 8259A "IoT Device Cybersecurity Capability Core Baseline" May 2020 https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf

3.2 Definitions And Abbreviations

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

3.2.1 Definitions

Anonymity	In case of market requirements, an anonymous identity is required during ownership transfer. EU data privacy or Privacy Regulations may apply.
Application	Applications (also called end-user programs) are software programs designed to perform a group of coordinated tasks that may vary by installation or model. Examples of IoT applications include a web browser, sensor manag actuator controller. This contrasts with system software, which executes the operating software of the main proc device.
Authentication	Authentication is the process of recognising an identity. It is the mechanism of associating an incoming request v identifying credentials. The credentials provided are checked with those in the device or within an authentication
Authentication	Authentication is the process of recognising an identity. It is the mechanism of associating an incoming request v identifying credentials. The credentials provided are checked with those in the device or within an authentication
Boot	The initial process used by the device when turned on that prepares the system for operation (normally contains Boot steps).
Consumer	An end user, and not necessarily a purchaser, in the distribution chain of a good or service who make personal u and/or service.
Deployment	The placing of the product into customer trial or service.
Encrypted	Data secured using a recognised algorithm and protected keys, so as to be meaningful, only if decoded, and dec those with access to the relevant algorithm and keys.
Enterprise	An organisation in business for commercial or not-for-profit purposes that share information technology resource
Firmware	Computer programs and data stored in hardware – typically in read only memory(ROM) or programmable read-o (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the pr
IoT Product Class	Class of network products that all implement a common set of IoTSF defined functions for that particular IoT pro
Interactive Account	Interactive accounts include non-personal accounts such as root, admin, service, batch, super user or privilege a permit system configuration changes.
Mutual Authentication	Mutual authentication refers to a security process or technology in which two entities in a communications link ve and integrity of each other before any sensitive data is sent over the connection. In a network, the client authenticates the server and vice-versa. It is a default mode of authentication in some pr SSH (see https://tools.ietf.org/html/rfc4250) and optional in others, such as TLS (see https://tools.ietf.org/html/rfc
Nonce	Nonce is an abbreviation of the term "number used once". It is often a random or pseudo-random number issued authentication protocol to ensure that old communications messages cannot be reused in replay attacks.
Operating System	An operating system (OS) is system software that manages device hardware and software resources and provid services for software programs.
On boarding	The method to register a device into its service or solution to enable device registration [ref 16][1], configuration a

Ownership Transfer	In case a device is transferred through a supply chain and changes owner, this method ensures a reliable and se ownership.
Personal Information	Personal Information is defined by the EU General Data Protection Regulation (GDPR): https://ec.europa.eu/info topic/data-protection_en. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). An id person is one who can be identified,directly or indirectly, in particular by reference to an identifier such as a nam identification number, location data, an online identifier or to one or more factors specific to the physical, physiol mental, economic, cultural or social identity of that natural person. Other jurisdictions may have different definitions.
Secure Boot	Process that ensures a device only starts software that is trusted by the OEM.
Secure Protocol	The method of exchanging information that ensures protection and reliability of the data (usually though cryptogr techniques).
Software	Unless otherwise explicitly stated, for the purposes of this document the term software also includes any firmwar product.
Strong Authentication	A procedure based on the use of two or more of the following elements, categorised as knowledge, ownership a i) Something only the user or device knows, e.g. static password, code, personal identification number; ii)Something only the user or device possesses, e.g. token, smart card, mobile phone; iii) Something the user or device is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise th least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as confidentiality of the authentication data defined other examples include NIST Special Publication 800-63B see [European Central Bank: Recommendations For The Security Of Internet Payments http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafter 95e6bba1ef875877ad3c35cf3b12399c
Supply Chain of Trust	Where an IoT system uses device or service components with more than one source, all sources demonstrate a relevant requirements of this framework. This will lead to the Devices and services in an IoT system exhibiting th attributes: - Engender robust Root of Trust and secure identities - Safeguard application code at source Inhibit grey-manufacturing and protect IP - Ensure only valid applications are programmed - Integrate robust key structures for ownership delegation - Enable lifecycle updates and patching
Tamper Evident	The enclosure of the product has measures to ensure that any unauthorised attempt to open it leaves evidence example, labelling across a product's enclosure joint that fragments when the joint is disturbed.
Tamper Resistant	The enclosure of the product has measures to prevent its unauthorised opening. Typically, with specialist fastene features that require the use of specialist tooling, unique to the product.

3.2.2 Acronyms

CoAP Constrained Application Protocol
DDoS Distributed Denial of Service
DTLS Datagram Transport Layer Security
EAL Evaluation Assurance Level
ERP Effective Radiated Power
HTML Hypertext Markup Language
HTTP Hypertext Transfer Protocol
IP Internet Protocol
MD Message Digest
MQTT Message Queue Telemetry Transport - ISO standard ISO/IEC PRF 20922
OEM Original Equipment Manufacturer
PRNG Pseudo Random Number Generator
ROT Root Of Trust
SHA Secure Hash Algorithm
SSH Secure Socket Shell
TRNG True Random Number Generator
TBC To Be Confirmed
TBD To Be Determined
TCP Transmission Control Protocol
TLS Transport Layer Security
T3P Trusted Third Party
UDP User Datagram Protocol
URL Uniform Resource Locator
WPS Wi-Fi Protected Setup

Footnotes

1. Example of IoT application ID registry and possible privacy profile registry ↩

2. NIST SP800-63b Revision 1" NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management" June 2017 [https://pages.nist.gov/800-63-3/sp800-63b.html] ↩

Risk-Assessment-Steps

1 Risk Assessment Steps

The core of the security process is to understand what is being protected and from what or whom. It is also important to identify what is not being protected. There are many ways to accomplish this procedure, but it is recommended to use well-known, best practice, risk management standards [ref 39, 40 and 41][123]. Risk management techniques can also be found in several common business training publications. An outline of the Risk Assessment process used in this document can be seen in the flow diagram and bullet list below:

Figure 3 Outline risk assessment process steps

- Create a list of security risks to the product
  - Use brainstorming techniques, mind mapping or other Group Creativity techniques.
  - Generate a list covering both business and technical threats:
    - E.g. “Brand Image damage due to adverse publicity”, “cost of product recall”, “product exposes users Wi-Fi credentials”
    - Safety aspects of the product that affect users if the security is compromised
    - The Framework can be used to support the creation of the list of risks by considering the Assurance Class criteria
- Assess the “probability” of each item on the Risk List happening
- Assess the “Cost” (impact in terms of the detectability and recovery) of each item on the Risk List – if it happens
- Multiply the Cost by the Probability, this gives a “Risk Factor”
- Order list by “Risk Factor”. This could be a percentage or simply Probability x Impact number

This list becomes the “Risk Register” document and may then be used to guide and justify the work needed to address product security. The aim of the work is to reduce the risk “probability” factor to an acceptable level.

Threat Description	Probability (0-100%)	Impact/Cost to company of threat happening (0-5)	Risk Factor
Compromise of Encryption and Key Management	5%	5	(0.05*5) = 0.25
Web User Interface subversion	90%	4	(0.9*4) =3.6
Mobile Application hacked	15%	2	(0.15*2) = 0.3
Leakage of Private personal data	15%	5	(0.15*5) = 0.75

Table 5

This is showing the biggest risk is the web User Interface, so the priority should be on mitigating this to reduce the probability.

Footnotes

1. Bluetooth Numeric Comparison [https://csrc.nist.gov/publications/detail/sp/800-121/rev-1/archive/2012-06-11] ↩

2. UK Government Cyber security risk assessment guidance [https://www.ncsc.gov.uk/guidance/risk-management-collection] ↩

3. NIST Special Publication 800-30 guidance for conducting risk assessments [https://www.nist.gov/publications/guide-conducting-risk-assessments] ↩

Security-Objectives-And-Requirements

2 Security Objectives And Requirements

The next step is to identify the security objectives and security non-objectives for the product. Items with high risk factors that need mitigation by design are usually considered as security objectives and items with low risk factors for which investment in mitigation is not justified are considered as non-objectives. Each objective must clearly state the asset that needs protection and relevant threats. Any excluded objectives should also be stated and explained, to make clear that they have been considered.

Security requirements are then derived from the security objectives. The main difference between those two is that security objectives specify what needs to be protected and security requirements are the means to achieve the required protection. The Security requirements document is a major milestone in the product development life cycle and should be ready before design is started.

Security-Requirements-Design-And-Implementation

3 Security Requirements Design And Implementation

The Security requirements document feeds the design and validation teams. Design methodology of security features is not different from the general design methodology of regular functional requirements. However, this is not true for validation methodology. The aim of the functional requirements validation is to verify that a system is able to do properly what it was designed to do. Security validation shall also try to simulate illegal or unexpected scenarios (e.g. writing to reserved bits in a register or applying an incorrect power up sequence) and verify that a system behaviour is predictable and security assets are not compromised.

The Risk Register should be maintained throughout the project, and the threat probabilities reassessed given the mitigations put in place to reduce the Risk Factor to an Acceptable level.

What is Acceptable? This is a qualitative assessment that needs to be made by the product owner against risk to reputation, customer expectation and cost of rectification in case of a security failure.

Appendix B Introduction To Supply Chain Security Requirements

The core of the security process is to understand what is being protected and from what or whom. It is also important to identify what is not being protected

B1-Motivation

B1 Motivation

IT systems, including IoT systems, can be compromised by cyber-attacks in their supply chain. Components compromised in the supply chain open the way for a variety of exploits when deployed into operational environments. Supply chain attacks are extremely cost effective from attackers' points of view. IT assets coming from development, manufacturing and distribution environments are often trusted implicitly by downstream users, despite weak or unknown security controls in those environments. Furthermore, a successful compromise of a single well-chosen IT vendor environment can fan out to the vendor's entire customer base as products and software updates are deployed. It is no coincidence that many of the most notorious cyber attacks have been supply chain attacks.

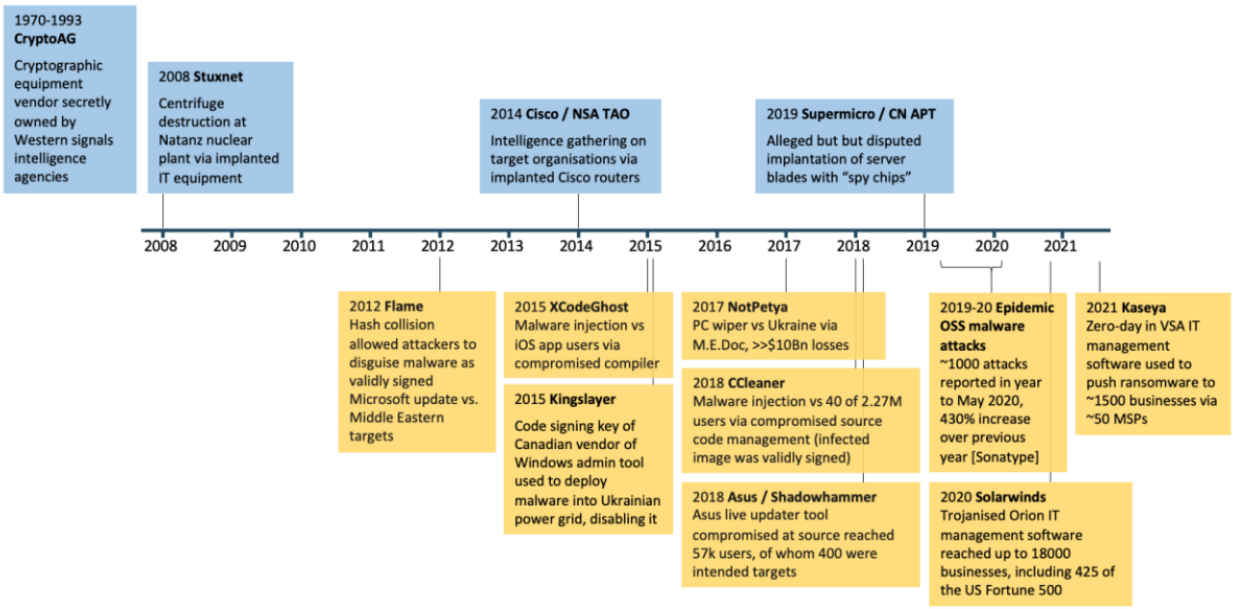

Figure 4 Timeline of well-known supply chain attacks

In recent years the ICT security literature has increasingly recognised the problem of protecting both software and hardware assets in the supply chain and has developed a variety of recommendations in response. However, while many of these recommendations are applicable to IoT devices, interpreting them requires a detailed understanding of the IoT supply chain. There is also a need for IoT-specific security recommendations to accommodate IoT device supply chains' unique characteristics.

An IoTSF working group was formed in April 2020 to supply both these needs with an expanded and updated set of security requirements concerning smart devices' supply chains. The group received contributions from 43 experts representing 34 organisations resulting in 29 specific, implementable recommendations. These have been mapped into this edition of the Framework in 5 pre-existing and 24 new requirements.

B2-Definition-Of-Terms

B2 Definition Of Terms

The job of an IoT device supply chain is to deliver devices into an application in a known, trustworthy, and trusted state. As well as delivering hardware and software, an IoT device supply chain must establish trust relationships. This characteristic is not shared by ICT supply chains in general.

Each component of an IoT device is the product of a preceding design and production process. It is more accurate to think of the supply "chain" as a supply "network". Anyone in the supply network with access to unprotected assets becomes part of the trust base of that device. Producers of key components such as embedded operating systems, cryptographic libraries and ICs carry a significant burden of trust and must demonstrate that they deserve it. But, as the designer of the production process, it is the device OEM who chooses whom to trust and is responsible for securing it overall.

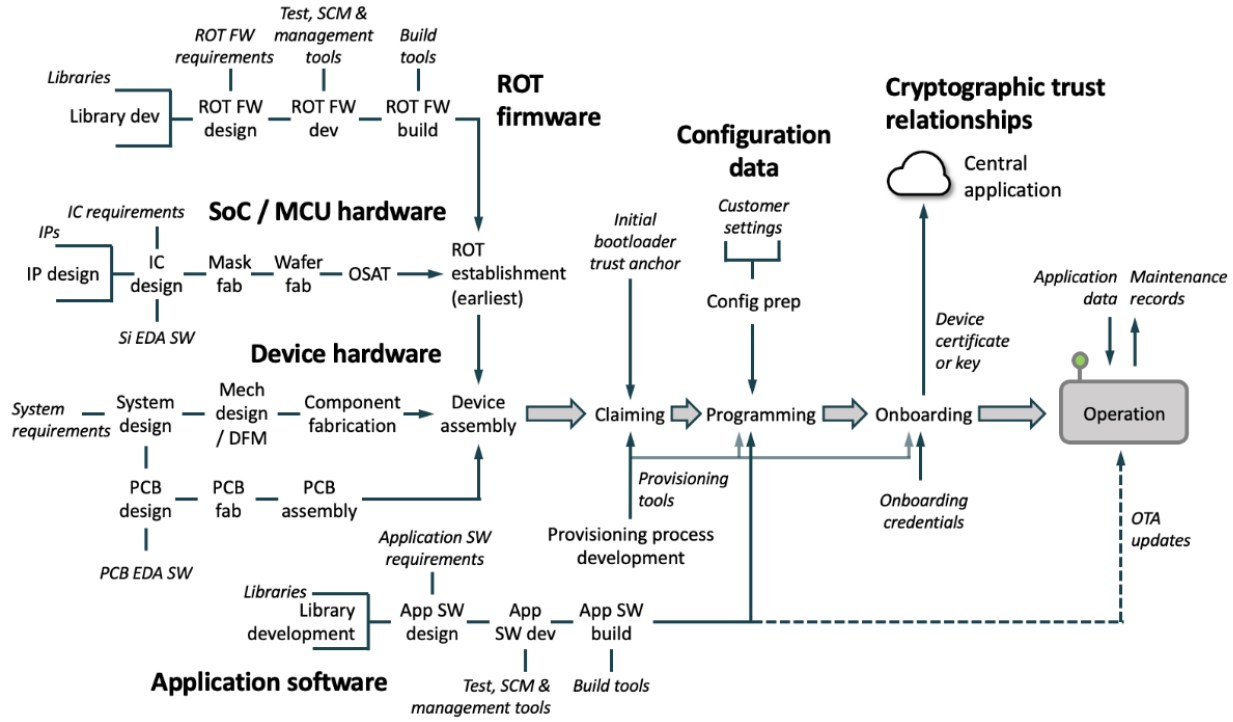

Figure 5 Overview of a typical IoT device supply network

The supply network is comprised of four basic types of operation: hardware assembly, which progressively integrates components and subassemblies into complete devices, programming, which installs logical assets onto those devices, personalisation, which generates a unique identity for each device, and on boarding, which places those devices into trust relationships with other systems. Programming, personalisation and on boarding together comprise the provisioning process, by which hardware is put into a functioning state.

While device hardware is undoubtedly important, it isn't likely to be attacked in the supply chain. In any case by far the biggest hardware determinant of devices' behaviour is the processor IC, the design and manufacture of which is outside of device OEMs' control. For most OEMs the main hardware risk is the use by Contract Electronics Manufacturers (CEMs) of grey market parts, which have been known to include manufacturing discards, recycled parts and counterfeits1. Much more vulnerable to cyber-attacks are the various provisioning operations (Table 6).

Operation	Description
Programming	Programming is always performed via a programming interface exposed by the target. Programming operations place software and configuration assets onto devices. These can include assets such as: - software images and server certificates, which are the same for every device - manufacturing data and customer-specific settings, which change per batch - identity secrets and device certificates, which are individually personalised for each device. Device operators rely on the authenticity and integrity of all these assets - and, in the case of identity secrets, also their confidentiality. Device OEMs and ODMs on their part often have an interest in maintaining the confidentiality of their software IP. Secure programming is rarely as straightforward as installing a binary image. Sometimes binaries are rebuilt per device to check for a specific IC hardware ID, as a defence against cloning. In other cases, configuration data is installed as late as possible in production, or even deferred into distribution. Device identities might be generated externally and programmed individually. Programmed assets must be protected not just in the programming environment but on the target IC. Because of this, ICs entering a secure programming environment must be authentically what they are believed to be, and they must be configured to prevent unauthorised readout or modification of assets before they leave.
RoT Establishment	With no identity or correspondent software already present, ICs fresh off the wafer typically expose a hardware-level programming interface. This channel is necessarily unencrypted and unauthenticated. The first programming step, **RoT establishment**, must therefore take place in a secure facility. RoTs once established can expose secure interfaces for provisioning subsequent assets. Examples of this pattern include secure boot managers which can detect and install new valid software images and secure programming interfaces. Both are often found as features of RoTs installed by IC vendors.
Claiming	An OEM making use of a secure boot manager established by the IC vendor must **claim** it by programming it with a trust anchor with which to validate the next software in the boot chain. Like ROT establishment, this is a special case of programming. Claiming is a key moment in the life of an IoT device because whoever installs that trust anchor chooses what software runs and thereby takes full control of the behaviour of the device.
Personalisation	Every connected device requires a unique, authenticable identity. Ideally devices should generate asymmetric identity key pairs internally, so the private key need never be exposed externally. Most modern microcontroller RoTs are able to generate high quality key pairs. Older or smaller microcontrollers may lack robust sources of high-quality entropy. Their private keys must be generated externally. Ideally this is done as close to the target device as possible to limit the potential exposure of those keys. The provisioning tool is an ideal place to accomplish this. Personalisation can also include serial numbers and other public identifiers.
	IoT devices are useless until they are connected into larger applications. Those applications need to be told which devices to trust and how to authenticate them. There are various ways of doing this, but all involve telling the central application to trust devices which can prove possession of specified secret keys. This is called **on boarding**. The act of on boarding is a major trust decision. When a device operator makes a decision to trust an IoT device they're making a decision to trust it, and the supply chain that delivered it to them, including everyone who has had access to the device and its components. For a device with a RoT those components include **I.** The initial bootloader, on which the operator is relying to ensure only properly signed code runs, **II.** The RoT runtime services, on which they are relying to provide unimpeachable security services, and **III.** The embedded software developed by the device OEM or ODM, which the operator is expecting to

Onboarding	behave exactly according to specification. Device operators unfortunately are not usually in a position to determine for themselves whether an IoT device has been provisioned into a known, trusted, functional initial state. Instead they must rely on someone else's assurances. Someone they trust, often the OEM, needs to assert "this device is in a known trusted state". Where devices are identified using asymmetric (private and public) keys this is accomplished by on boarding the public key to central services. This can be done in several ways. The simplest method is to take a copy of each devices' public key on the production line and upload it to the central service. The copy should be taken when the device is fully provisioned, but before it leaves the trusted manufacturing environment. A more powerful and flexible method is to sign each device's public key into a certificate chain on the production line and load that certificate chain back into the device. The device can later deliver its public key to the central service itself, as part of a TLS handshake. Central services can on board that key on the authority of any Certificate Authority (CA) certificate in the chain. Because this allows large volumes of devices to be on boarded in a single operation it is convenient for device operators to have their devices signed into their own certificate chain of trust. In each case, whether keys are on boarded directly to the central service from the production line or signed into certificate chains of trust, it is essential that only trusted parties perform that operation. The fewer entities involved the better. Signing devices into chains of trust offers a distinct advantage over other on boarding methods in this respect, because the CA keys can be stored in an onsite HSM or secure element, or offsite in a secure facility, where they can be used without ever being exposed in manufacturing environments. It is important to note that the private keys of all the CAs in the chain of trust must be similarly protected, because an attacker gaining the use of any of them gains the ability to on board any device they choose [2].

Table 6: Provisioning operations

To reach a known functional initial state, devices must be provisioned with many software and data assets and into many trust relationships, often in a sequence of provisioning steps that begins with a blank IC and ends with a fully functional and secured device. Each step may be performed by a different actor, each provisioning the device into an intermediate state. The process may begin upstream of the OEM, with IC vendors provisioning naked dies, and it may extend to as late as immediately before devices' live deployment, with installers commissioning devices on site.

IoT OEMs already design provisioning sequences and create or specify provisioning tools (Figure 3) for each step of those sequences, as part of their device development. Because manufacturing environments have generally been assumed secure it has been rare to give further consideration to protecting these tools and processes against deliberate attack. In essence though security is just another design goal. OEMs can use their control of this process to allocate key steps to more-trusted suppliers. Alternatively, they can engineer provisioning tools to keep assets out of harm's way in untrusted environments.

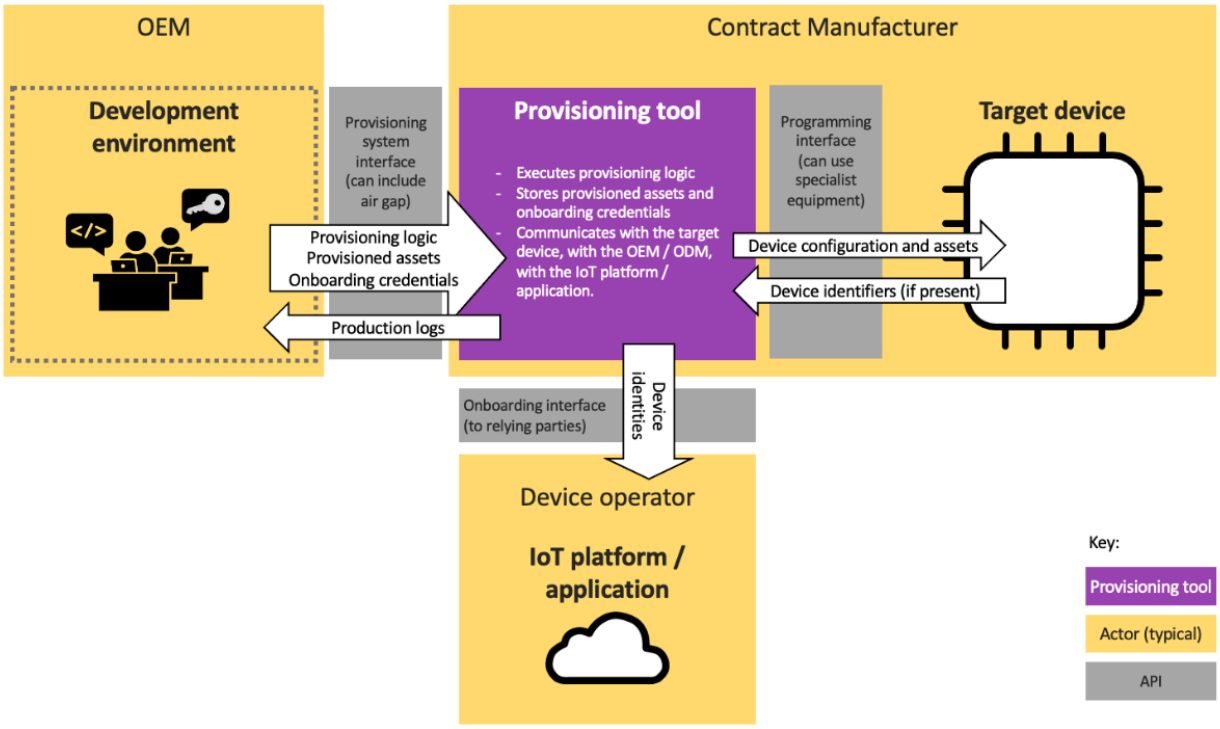

Figure 6 Generic provisioning tool

---

1. 2015, Rob Wood, NCC Group, Secure Device Manufacturing: Supply Chain Security Resilience

2. 2021, Michael Richardson, IETF, A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors

B3-Approach

B2 Approach

Submissions were invited from representatives of IoT users and vendors and categorised into lists of actors, principles, attacks, references, characteristics, assets, objectives, mitigations, and definitions. Using these inputs as an initial guide the working group developed the general characterisation of IoT device supply chains outlined above before proceeding to a threat analysis using the method of attack trees 3 . Security recommendations were developed to address these threats. In parallel, the group surveyed a range of standards and literature for known attacks and existing advice. Both were used to check the completeness of the ab initio analysis4 before the recommendations were mapped into the Framework.

This Appendix (B) was created from a white paper generated by the IoTSF Supply Chain Working Group Our thanks go to

Editor and chair

- Amyas Phillips, Ambotec Consulting

Working group members

- Amit Rao, Trusted Objects
- Anjana Priya, Microchip
- Michael Richardson, Sandelman Software Works
- Prof. Paul Dorey, CSO Confidential
- Rob Brown, Jitsuin

Contributors

- Alagar Gandhi, FCA
- Alexandru Suditu, OMV Petrom
- Andrew Frame, Secure Thingz / IAR Systems
- Angela Mison, University of South Wales

---

3. 1999, Bruce Schneier, Dr Dobb's Journal, Attack Trees (see https://www.schneier.com/academic/archives/1999/12/attack_trees.html)
4. A full bibliography is not provided here, however special attention was given to associating actionable recommendations to the principles proposed in ENISA's 2020 publication "Guidelines for Securing the Internet of Things: Secure Supply Chain for IoT".