IoT Security Architecture and Policy for the Enterprise - a Hub Based Approach

Release 1

Contents

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

Notices

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

Terms of Use

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

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

Disclaimer

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

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

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

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

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

Copyright, Trade Marks and Licensing

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

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this version of the document

John Moor, IoT Security Foundation
Richard Marshall, Xitex Ltd
Stacie Walsh, Oxford Information Labs

Peer reviewers:
Chris Shire, Infineon Technologies Ltd
Jeff Day, BT
Paul Dorey, IoTSF Chairman
Robert Dobson, Device Authority Ltd
Steve Babbage, Vodafone
Plus others – you know who you are!

1 Introduction

1.1 Executive Summary

The opportunities and benefits that exist for businesses to use IoT-class products and systems are many and varied. These may include improving the customer and employee experience, streamlining operations, improving productivity or even creating new avenues of business. With a wide range of procurement, installation, configuration and operating options, a common challenge is how to manage and maintain a complex system. This is especially important when it comes to security as the benefits of IoT could be overshadowed by the risk of adoption.

The IoT Security Foundation is publishing a series of architecture proposal documents with the following intentions:

- Reduce/manage complexity of IoT systems by simplifying implementation options
- Demonstrate what a good security regime looks like, by example
- Explain the benefits of a hub-based approach including achieving security goals, maintaining system hygiene and resilience, managing extensions and life-cycle provisioning

A hub-based architecture may not be a single device/interface solution, but a collection of security and trust tools. For small enterprises, the architecture may comprise a single device; for larger enterprises, it will likely consist of a number of hubs, both for scalability and redundancy. Related devices and solutions that may act as the hub in this architecture include a router, network management and security tools such as a firewall or gateway, network access controls, a protocol bridge or any other device that naturally lends itself to a management role within a network. In practice, a hub architecture provides selected points for IoT device and network management that can make use of existing infrastructure, as well as provide flexible bespoke solutions for individual IoT deployments.

This document is intended to illustrate a solution for enterprise environments where businesses are looking for operational and productivity benefits of using IoT. It is intended for chief officers or managers – such as those tasked with overseeing IoT adoption, information security, or digital transformation – as well as staff with responsibilities for architecting, designing, planning, procuring and operating an IoT-class system – i.e. system architects, technical managers and systems integrators. It may also be of use to companies designing smart hubs as 'the Hub' is a key element of the architecture. Security is not static, it requires a series of on-going processes that need to be managed over the combined life-cycles of system elements including services, devices and networks. The architecture described by this document supports a layered approach to the security challenge and lifecycle management tools in the Enterprise IoT deployment. It presents a relatively user-friendly IoT management solution that supports key principles of security assurance and good practice including network management, connecting devices securely, software maintenance and end-of-life considerations. As a result, it may also support a number of specific compliance requirements or best practice standards. For example, a hub-based architecture can help mitigate risk associated with cyber security and data protection regulations such as the European General Data Protection Regulation (GDPR) [ref 13] and Network and Information Systems (NIS) Directive [ref 14] or support adoption of the USA's Cybersecurity Information Sharing Act (CISA) [ref 15].

Whilst perfect security is likely to remain elusive, this architecture is considered to be a good approach to support the management of common security goals of confidentiality, integrity and availability. Interoperability between IoT devices is a key aspect of hub architectures, like the one described here, and assists with security management across the IoT ecosystem. While this document does not specifically address the issues related to interoperability, it is worth highlighting the work that should be done in this area to support IoT security and ease of adoption.

Similarly, this document proposes an ideal Enterprise hub architecture which is not yet in the marketplace. This is with the intention of stimulating and informing future product design, development and implementation.

Further work can be done to apply hub thinking to existing implementation approaches and identification and adoption of key industry standards to support a hub architecture. Before standards solutions are available, Enterprises should be able to identify the primary IoT and security management needs for their organization by using this Hub architecture in conjunction with a comprehensive risk assessment. With this information, Enterprises may then identify those available market solutions that are best suited for their own IoT deployment.

1.2 Scope

The focus of this document is the definition of a Hub-based architecture for IoT devices and solutions implemented and managed by the Enterprise.

We do not make assumptions about the business models of enterprises or IoT solution providers. For this particular reference architecture, it is assumed that IoT devices will not be wholly owned, controlled and operated by the IoT provider – as is the case in some business models. Instead it is assumed the relevant devices will have some level of ownership, control and management by the enterprise itself.

Below is a more detailed list of IoT and related issues considered in scope of this proposed Hub architecture:

- Consumer, in addition to Enterprise-focused, IoT solutions
- Devices that connect to and/or provide information via the Enterprise's network
- Devices with security features that are managed by the Enterprise (e.g. authentication, roots of trust, password control, update)
- Devices with configuration options managed by the Enterprise

The scope of the Enterprise IoT category could be very broad. Explicitly we do not include details regarding specific deployments of IoT, such as Enterprise building fabric solutions like Building Information Modelling (BIM). A deployment such as BIM could warrant its own architecture and special considerations. Instead, the architecture focuses on more general and common uses of IoT solutions such as smart office applications (defined broadly, ranging from connected printers to smart whiteboards), operational efficiency (such as IoT telemetry) and/or smart manufacturing systems. This is to focus effort on covering the majority of enterprise use cases and to concentrate on the IoT devices available for sale today or those widely anticipated, as most enterprises will be looking at the current and future markets for their technology solutions.

Below is a more detailed list of IoT and related issues considered out of scope for this proposed Hub architecture:

- The specific requirements for the following sectors are not in scope
    - Building management
    - Building information modelling
    - The adaptation or augmenting of legacy IoT device capacities
    - BYOD devices broadly (such as personally owned smart fitness devices)
    - Fleet vehicles and mobile assets
- Other Considerations not in scope
    - Existing BYOD devices that IT departments already provide for, such as visitor's laptops
    - Consideration for sector-specific requirements and regulations – such as security and data protection requirements for the finance, healthcare, or critical national infrastructure sectors
    - Sub architectures for this and other IoT reference models: the specific IoT sub architecture within the Hub ecosystem is unique to each deployment. This Hub-based architecture does not specify or make assumptions about sub architecture characteristics such as how and when devices are connected, traffic routing, or implementation of multiple Hub solutions
    - Procurement language and model contracts for the procurement of such hub equipment

1.3 Intended Audience

The intended audience for this document is for people with the following roles or responsibilities:

- CxOs and IoT purchasers – to better inform purchasing decisions, particularly:
    - Section 1: Purpose
    - Section 2: Overview
- IT departments – to better inform security-focused Enterprise IoT management and architecture, particularly
    - Section 2: Overview
    - Section 3: Hub-Based Reference Architecture
- Developers – to better understand IoT management and security needs of Enterprises and gaps in the market, particularly:
    - Section 3: Hub-Based Reference Architecture
- OEM Product Management – to better understand IoT management and security needs of Enterprises and gaps in the market, particularly:
    - Section 3: Hub-Based Reference Architecture

1.4 Taxonomy

In the requirements sections, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119 [ref 2].

The following terms are used in this document:

- Public Roots of Trust: A publicly trusted root is one whether the root of trust is publically accessible, typically where the trust anchor is publically published by one of the public Certificate Authorities
- Private Roots of Trust: A private root differs from a public root because roots of trust aren't publically accessible. The root(s) of trust will need to be published by the organization whose Certificate Authority created the root of trust, to those entities which need to validate the chain of trust anchored by the private root

2 Overview

There are two key elements to the proposed architecture: the Hub device and the flexible Hub networking model. The Hub device acts as a central point for trust and network management. It also adds an additional layer of security to the IoT environment. The Hub device supports flexible networking by allowing IoT devices and sub-architectures to be deployed in the IoT environment as preferred by the Enterprise. Thus, it does not propose particular network architectures beyond separating IoT[1] and business networks.[2]

Unlike other IoT architectures, this Hub architecture provides a centralized point for IoT device and network management utilizing existing security features and offering flexible solutions for the Enterprise. The Hub supports IoT managers by aggregating information and communicating with relevant network elements such as routers and IoT devices. It may also adopt additional functions, for instance acting as a gateway. This enables information sharing between the local IoT environment and other networks or entities, such as the IoT smart coffee machine provider.

For added security, it is recommended that Enterprise IoT devices connect via a dedicated IoT network and not via the business network. The aim is to minimize the Enterprise and IoT network attack surfaces by protecting business operations from IoT devices which may be used as an attack vector.

It is believed that, compared to other architectures, this Hub architecture offers a more secure and easy to manage Enterprise IoT ecosystem. The Hub architecture is also intended to be a flexible solution to fit any size or type of Enterprise deployment. Flexibility allows the Enterprise to adopt the best IoT solution to suit its needs while not compromising on security. For example, the ability to choose which data is kept within the organization (e.g. managing sensitive data on the Hub) and when to use cloud solutions.

For more information on the benefits of a Hub architecture, see section *2.2.2 Why a Hub?* and *Table 1: Architecture Characteristics*

2.1 Hub-based Reference Architecture

Enterprises and their IoT deployments differ and the proposed Hub architecture is intended to provide a flexible solution which can accommodate a wide variety of Enterprise environments. It is not intended to address a single device/interface solution. Instead it enables the implementation of a collection of security and trust tools that support IoT deployment and management in different Enterprise environments and IoT solutions. For instance, small enterprises may only require a single Hub while larger enterprises will most likely need a number of Hubs – both for scalability and redundancy. Because of its central role, the Hub provides a point to oversee, monitor, and, to a degree, control the Enterprise's local IoT ecosystem.

The Hub is central to the reference architecture, aggregating information and communicating directly with other devices and network elements in the IoT environment. At the same time, the Hub can be visualized at the edge of a network, providing a secure gateway for communication between networks. The Hub should be user-friendly and support good device management and security practices. It should integrate seamlessly with existing network management tools and cater to IoT managers with a variety of capabilities and backgrounds. In addition, the Hub itself needs to have robust security to protect the information and roots of trust that it manages.

[1] For the purpose of this architecture, an IoT network is a network dedicated to supporting IoT solutions deployed in the enterprise environment. For instance, this may include smart light bulbs, motion detectors, manufacturing equipment, or smart coffee machines.

[2] For the purpose of this architecture, a business network is a network (local or wide area) which enables normal business functioning of the enterprise, such as employee access to servers and document stores, enables internet and email access, and direct communications with vendors or clients.

This Hub architecture provides another layer of security for both the wider network and for those devices that may have minimal or no built-in security features by considering security at every level. As a result, the Hub architecture is proposed as a more robust and secure architecture than others, such as “tree” or “hub-and-spoke”.

As opposed to a tree network, which connects a number of nodes via a direct communication line without a central management point, the Hub provides an information aggregation point for all devices or groups of devices and other Hubs such as gateways deployed within the local IoT network. Additionally, the Hub device itself, not only the network architecture, is a key information aggregation element required to fully implement the proposed architecture.

Unlike a hub-and-spoke model, the devices in the Hub architecture do not rely on the Hub to talk to other devices or execute its functions. But the Hub does provide a management point where requests or actions can be taken, communicating from one to many and vice versa.

2.2 Aim of Hub Architecture

This Hub reference architecture aims at providing a user-friendly centralized management solution for Enterprises deploying IoT devices and solutions – from one or multiple vendors. Importantly, the architecture considers security a primary objective and provides a way forward with this in mind. The desired result is a more secure IoT ecosystem within Enterprise environments that is user-friendly, easy to deploy and manage. Enterprises should be able to adopt this Hub architecture as well as use it as part of proof of compliance. It is also intended to highlight where security solutions currently available on the market fulfil as well as lack these desired features.

2.2.1 Main Hub Functions

In this Hub-based reference architecture, the Hub is a centralized IoT management point with the ultimate aim of supporting trust and security within the Enterprise’s IoT deployment. The Hub provides a central point to oversee and monitor – but not necessarily directly control – every aspect of the IoT ecosystem. This is done by providing a device and user interface that can act as a repository of information for monitoring, audit and reporting capabilities, provide alerts and notifications, act as a certificate manager and/or cache, provide access controls, and possibly device control functionalities. In essence, the Hub functions as an IT manager resource.

To enable the Hub’s flexible management of a unique Enterprise IoT ecosystem, it supports three basic IoT device “classes”. Of the three classes listed below, most IoT devices will fall in Class 2, where the Enterprise may centralize as much of the device management as possible within the Hub architecture, but some aspects of management may rest with the service provider.

- **Class 1: Fully controlled and connected** – where interfaces such as IoT device control, data collection and management are fully integrated and controlled by the Hub device and kept within the Enterprise
- **Class 2: Partially controlled and/or connected** – where the Hub device may execute some but not all interfaces with the device, such as pushing updates and managing traffic but not collecting sensor data
- **Class 3: Information sharing** – the most basic type of interaction, the Hub would not control or manage the IoT device functions such as updating or data collection, but instead will log basic information such as device status or installed updates

For the purpose of this architecture, the main Hub functions or support capabilities include network management, connecting devices securely, and lifecycle management. Below are examples of how each of these Hub functions support Enterprise IoT security:

- **Network Management and Security Tools**
  - **Local IoT Network**: Implementing a local IoT Network to separate traffic, minimize attack surface and protect business operations [see section 3.2.1]
  - **Separation of Testing, Staging and Live Systems**: Separating systems to reduce the risk of new devices reducing the security of the IoT ecosystem [see section 3.2.2]
  - **Gateways and Firewalls:** Implementing gateways and firewalls to protect networks and data, and manage traffic [see section 3.2.3]
- **Connecting Devices Securely**
  - **Authentication and Authorization**: Using authentication and authorization to ensure only verified and permitted devices are on the network [see section 3.3.1]
  - **Secure Boot**: Using secure boot to validate the integrity of IoT software [see section 3.3.2]
  - **Roots of Trust**: Implementing roots of trust to support security foundation [see section 3.3.3]
- **Lifecycle Management**
  - **Monitoring and Audit**: Using monitoring, discovery and audit tools to oversee the IoT ecosystem, take action based on informed decisions, and prove compliance [see section 3.4.1]
  - **Update and Patch**: Managing update and patch processes and history to support security best practice throughout the device lifecycle [see section 3.4.2]
  - **Manage Device Identity and Authorization:** Using device identity to manage and improve security of devices, including end-of-life provisioning [see section 3.4.3]
  - **Managing End-Of-Life**: Managing device end-of-life securely for scenarios including device end-of-support, replacement, and ownership transfer [see section 3.4.4]

2.2.2 Why a Hub?

This paper proposes a Hub-based architecture as a robust foundation for IoT security and management for several reasons, including:

- **Centralized Management** – A Hub is characterized as the focal point in a network, with connectivity to all groups/devices, network management tools or other Hubs. Ideally, this Hub would enable IoT ecosystem lifecycle management by supporting network and end-device security. It provides an easy one-stop-shop to manage roots of trust, monitor network traffic, devices on the network, and updates and patches
- **Software Update and Patch** – The failure or inability to update connected devices is a now well-known security risk [see ref 11]. A Hub would enable the management and implementation of software updates within the Enterprise IoT ecosystem and offer high-level update-able management Hub to protect those devices without update capabilities. It would also facilitate an additional layer of security by providing an easy update point particularly for those devices which do not support endpoint solutions such as updating and patching
- **Security Compliance** – A Hub architecture provides a central place to manage layered security and ensure a minimum level of security that protects all IoT devices across the Enterprise. In addition, it could assist with regulatory compliance. For instance, the Hub could act as a firewall and/or provide a simple update and patch mechanism. The Hub can enable, log, and report on security features or statuses, providing a repository of information that may be used to prove compliance with standards or regulations as needed
- **Troubleshooting** – A Hub would also provide an easy troubleshoot mechanism for the Enterprise IoT ecosystem. The ability to manage, audit and monitor traffic and connected devices in one central

place supports IoT security management. This not only helps manage devices, but also provide real-time notifications of malicious devices, network anomalies and pinch-points

In addition to the security and management attributes, a Hub-based architecture is also considered highly flexible to accommodate a variety of Enterprise implementations. A quick comparison of network architecture characteristics (below) highlights the security functions and flexibility that the Hub architecture offers.

Architecture Characteristics	Hub Architecture	Tree Network	Hub-and-Spoke or Star Networks	Mesh Network	Ring Network
Supports a centralized network management tool	X	X	X		
Supports hybrid network sub-architectures	X	X	X		
Supports direct communication with management tool (does not require information to travel through unneeded nodes or pathways)	X	X	Sometimes		
Information must be shared in a hierarchical manner		X	X		
Network management tool is resilient to device and network disruptions	X	X		X	
In the event of management point failure, networks and devices can continue functioning	X			X	
Central management and information aggregation point	X				
Management tool supports IoT device identity, access and authorization resources	X				
Management tool supports minimization of attack surface	X		X		
Dedicated device for network and IoT device management	X				

Table 1: Architecture Characteristics

2.3 Assumptions

2.3.1 Device Ownership

We assume devices will have a mix of privilege and variety of ownership, by visitors and employees of the enterprise and the enterprise itself. Devices may be used by many people and require trust properties to reflect this, but without imparting administrative privileges to all users of that device.

2.3.2 Network Security

We assume a relatively static size of network, but one that might be expanded to incorporate new technologies as they are rolled out. The need to manage such a diversity of devices is recognized, with an emphasis on clarity of device statuses across the network, and simplicity in the process for improving and updating network security.

2.3.3 Visitor Access

In addition, each enterprise should have strong and established trust policies for devices and groups of devices, such as visitor or guest devices, including levels of trust. This includes temporary Enterprise devices which may be connected to the business as opposed to the guest network. In cases such as these, it assumed that the Enterprise will manage access and device privileges in alignment with Enterprise policy. Whilst specific recommendations on such policies are outside the scope of this document – they will be individual to the needs and security requirements of each enterprise – we do assume that an enterprise will offer open connectivity to visitor devices, so that they will have access to connectivity, but no administrative privileges.

2.3.4 Privileges

We assume that a variety of device/service access and administrative privileges will be managed by the enterprise. Administrative privileges will be influenced by a variety of factors such as the device class (as specified in section 2.2.1), IoT solution business model, handling of business critical and sensitive data, and technical capacity within the organization. We also assume that general users will not be restricted from using the device's full functionality, yet at the same time they do not have administrative privileges. For example, a person should be able to make full use of a smart coffee machine and its services – for example save their regular coffee order and gift coffees to others – whilst not being able to access free test coffee drinks.

2.3.5 Sector-Specific Requirements

Enterprises in certain industry sectors will have more regulation constraints than others, and so there will be a variance in security and audit requirements between enterprises. We assume that the enterprise will adhere to sector-specific requirements including regulations and best practices.

2.3.6 Technologically Neutral

This proposed Hub architecture is intended to be technology agnostic, and therefore should be flexible and broadly applicable to IoT deployments. It is important to keep in mind that the business models of IoT solutions, particular enterprise structures, and unique deployments will all impact implementation of this architecture. Therefore, the following is provided as an example and not a rigid implementation of the architecture described here. Where existing protocols or standards are referenced for illustration and are in not intended to be prescriptive references.

2.4 Security Principles

There is a huge variety of devices labelled "IoT" and equal variety in the level of security features supported by those devices and solutions. Enterprises need to be aware of security risks when implementing IoT solutions, and therefore should be aware of common security principles, no matter the deployment environment. The resulting decisions will most likely differ by Enterprise as no IoT deployment is the same. Nevertheless, these principles should be taken into consideration from the outset.

The most modest approach to security focuses on the following three key principles, also included in the "IoT Security Compliance Framework" [ref 1]:

- Confidentiality – ensuring information and systems are protected from unauthorized access
- Integrity – ensuring that information and systems are unaltered and accurate throughout the lifecycle. For instance, information integrity applies to data collection, transfer, use and storage
- Availability – ensuring that information is and services are accessible by users or systems as and when needed

From these principles, a wide variety of questions emerge when considering IoT solutions. Many of these questions are considered in "Make it safe to connect: Establishing principles for Internet of Things Security" [ref 10] by the IoT Security Foundation, replicated here for ease:

- Does the data need to be private?
- Does the data need to be audited?
- Does the data need to be trusted?
- Is the safe / timely arrival of data important?
- Is it necessary to restrict access to, or control of, the device?
- Will the device need to be updated?
- Will ownership of the device need to be managed or transferred?

Developing these points to take into consideration architectures as well as data security, this proposed Hub architecture expands upon the list above. The following architecture-specific questions are incorporated here:

- What is the Hub's relationship with trust management? [see section 3.3.3]
- How does the Hub architecture support layered security? [see section 3.3]
- To what extent is network access managed and when should access be revoked? [see section 3.2.1]
- Where is it safe to make the data transparent for monitoring, updating and auditing? [see section 3.3]
- What permissions are given to a device and does it – and potentially its data – need to be treated differently to other devices? [see section 3.3.1]
- What information about the Enterprise does the data provide, what is the relation to business-critical functions, and where is the data best managed? [see sections 3.3.1, 3.3.3]
- What should be considered when decommissioning devices or transferring device ownership? [see section 3.5]

Good security hygiene should be the foundation of any IoT management process. Therefore, the principles for this architecture are based in ensuring a minimum level of security across the Enterprise IoT ecosystem and understanding where weak points or attack vectors might be located.

2.4.1 Threat Assessments and the Hub Architecture

This Hub architecture focuses on three security management features identified to support these security principles. The security management tools at the core of this architecture are:

- Network Management and Security

- Connecting Devices Securely
- Device lifecycle management

Information security is also an integral part of secure IoT ecosystems, and is supported by security management systems in the Hub architecture. It is assumed that information security best practices will be implemented with IoT deployments, be structured in a way that best meets the needs of the Enterprise, and is in compliance with relevant regulations such as local data protection and privacy regulations. Information security best practice are not the focus of the architecture, but more information on how they relate can be found in Appendix B.

Below is a table with a few examples to highlight the manner in which this reference architecture can help an Enterprise safeguard against some computer security threats and support compliance measures. The examples focus on the exploitation of connected systems and are organized using the widely-known STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) threat classification model along with two additional threats relevant to Enterprise IoT deployment – regulatory compliance and unsupported endpoint management.

However, these are not the only threats to an Enterprise IoT environment, nor is it the only threat or risk model available. Other examples include: PASTA, VAST, Trike, NIST's Cyber Security Framework, NCSC's Risk Management Guidance, ISO/IEC 27000 series (particularly those on information security risk management and auditing), and OWASP (application security). An Enterprise should select the most appropriate model when executing an assessment.

For a more comprehensive sample threat modelling, see Appendix A.

Threat	Threat Example	Treatment Examples	Hub Architecture Treatment Correlation
Spoofing	Address resolution protocol (ARP) spoofing used to redirect data traffic to the attacker	Update and patch devices to prevent vulnerability exploitation	Authentication & Authorization [3.3.1] Update and Patch [3.4.2]
Tampering	Tampering with software to modify permissions, install spyware or backdoors	Secure boot and update to ensure software and hardware are only modified by trusted sources Periodic auditing of firmware to check for tampering or unauthorized modification	Secure Boot [3.3.2] Monitor & Audit [3.4.1]
Repudiation	Sensor data is modified in transit to the cloud service and Enterprise metrics are affected	Use of digital certificates to support secure identity of users and devices Public key infrastructure to manage and revoke digital	Authentication & Authorization [3.3.1] Roots of Trust [3.3.3]

		certificates and roots of trust	
Information Disclosure (Data Breach)	Diagnostics information shared with an OEM which discloses proprietary Enterprise information which is not required by the OEM	Traffic monitoring and management (ingoing and outgoing) Separating business and IoT networks	Local IoT Network [3.2.1] Gateway and Firewalls [3.2.3]
Denial of Service	Using exploits in connected devices to execute a DoS or DDoS attack on another IoT device in the Enterprise network	Traffic monitoring, auditing and management (on the IoT network, ingoing and outgoing) Use of gateways and firewalls to monitor and block traffic	Local IoT Network [3.2.1] Monitor and Audit [3.4.1] Update and Patch [3.4.2]
Elevation of Privilege	Unauthorized access of a cloud service provider's system enabling access to the Enterprise business or IoT network	Separation of IoT and business networks to discourage privileged users from accessing non-relevant business information	Local IoT Network [3.2.1] Authentication & Authorization [3.3.1] Monitor and Audit [3.4.1]
Regulatory non-compliance*	Need to prove compliance through metrics after a data breach to show due diligence	Log and report on security features and ecosystem management Enable security best practices Identify, manage, and update regulation compliance measures	*Highly dependent on regulatory requirements. Gateways and Firewalls [3.2.3] Authentication & Authorization [3.3.1] Monitoring and Audit [3.4.1]
Unsupported endpoint management	Inability to encrypt data or assign a root of trust	Create a secure local environment for devices - separate devices from WAN and business networks	Local IoT Network [3.2.1] Gateways and Firewalls [3.2.3] Monitor and Audit [3.4.1]

Table 2: Threat Treatment and Architecture Correlation

3 Hub-Based Reference Architecture

The architecture presented here is meant to be a resource which outlines key security considerations and how a Hub may act as a central information repository, assist IoT deployment and enable long-term management. The extent to which the Hub provides monitoring, audit and controls depends on the relevant IoT solutions, Enterprise structure, and specific implementation of this architecture.

This section presents a high-level Hub architecture design as a reference model for Enterprise IoT managers. Cyber security principles are the foundation of this work, in particular the DCMS "Secure by Design Report" section 4.5 [ref 7] and the IoTSF's "Application Note: Mapping the IoT Security Foundation's Compliance Framework to the DCMS proposed Code of Practice for Security in Consumer IoT" [ref 8]. Supporting these principles and enabling easy implementation and control is a primary aim of the Hub architecture which provides a device management point.

We do not prescribe or presume certain protocols or solutions, but some reasonable assumptions have been made about number of connected devices, their physical constraints and the "character" of such devices and networks (e.g. if one person sets up the network, or many people have admin rights for different parts of the system). This technology-agnostic approach enables the blueprint to be applicable to a wide-range of systems with such constraints.

3.1 Example of Hub-Based Architecture

The Hub architecture is elaborated here through five elements. The first is a visualization of the Hub architecture and illustrates how the Hub is connected to other devices and security features on the network

This is followed by three key processes and their security considerations identified for IoT solution implementation and management, consisting of:

- Network Management and Security Tools
- Connecting Devices
- Lifecycle Management

Lastly, there are security considerations for the Hub itself (section 3.5 Hub Device Security), including device and software security.

3.1.1 Visualization of Hub-Based Architecture

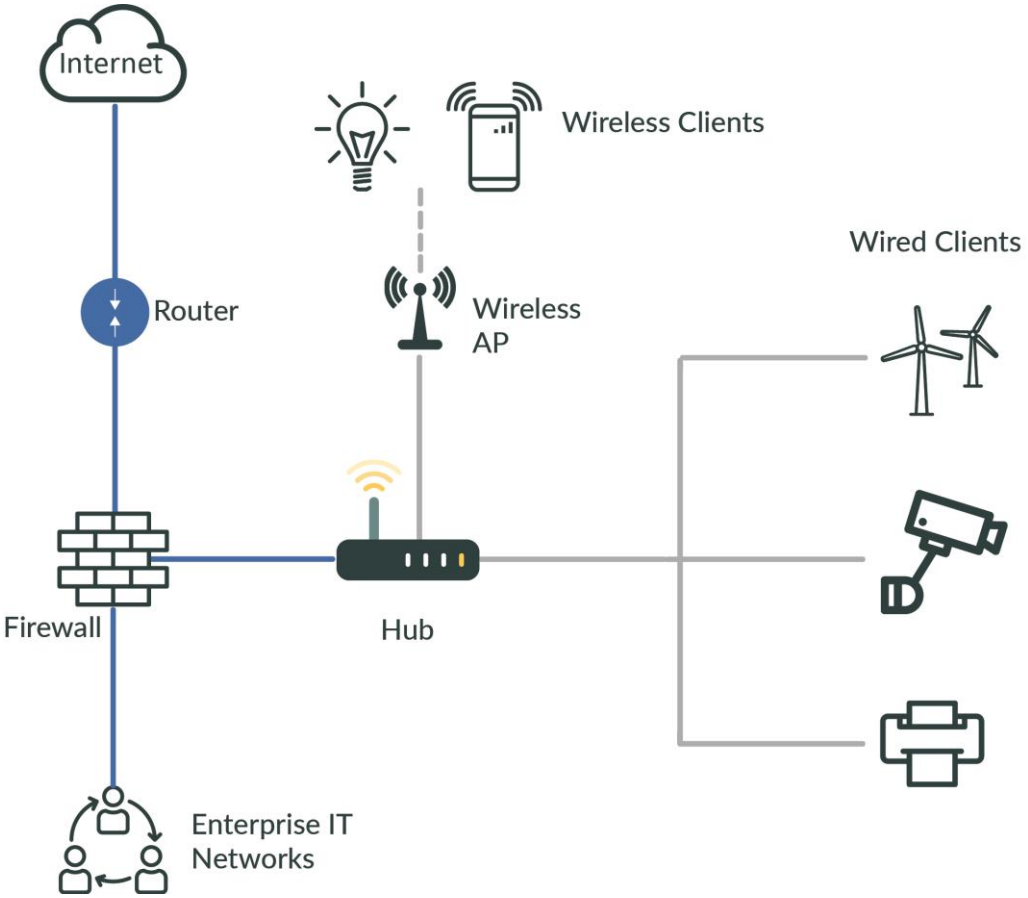

Figure 1: Example Hub Architecture

The visualization in **Figure 1** above shows the multi-layered communication structure within an Enterprise IoT environment, and reflects the complex communication structure between devices, networks and the central Hub. The functions of the router and firewall are shown separately but could also be incorporated into the Hub for Hubs intended for smaller Enterprises. The **local IoT network** (grey lines) is dedicated to IoT devices and separated from the Enterprises' business operations network. **Devices** (grey lines) use this network to talk between themselves, to the Hub and possibly with external elements via a Hub gateway. **The Hub** is at the centre of the IoT ecosystem as it aggregates information and communicates with other architectural elements such as devices and local networks. At the same time, the Hub can act via its connection to the firewall (blue line) as a gateway to external or Enterprise networks as needed.

3.1.2 Reading the Hub-Based Reference Architecture

The Hub-based reference architecture differs from most architectures in that it includes recommendations on the architecture and ideal Hub attributes. For this purpose, we are including a guide on how to read the architecture.

Architecture elements (i.e. Local IoT Network) are categorized under one of the key processes (i.e. Network Management and Security) for managing IoT security. Each architectural element includes three sections:

- Introduction to the topic (i.e. Local IoT Network)
- Architecture recommendations
- Hub Attributes

The **introduction** provides a brief overview of the topic and its relevance to the Hub architecture. This is targeted at a broad reader audience to provide background and context to the recommendations and attributes.

The **architecture recommendations** provide detail of good and best practices that should be implemented when adopting the Hub architecture, but are not focused on the capabilities of the Hub device.

The listed **Hub attributes** provide detail about what is required of the Hub device to support the overall architecture – a key and unique element of the Hub-based architecture.

An "Examples" section is also included for each of the three key processes. These are real-world examples of how the architectural elements described in that section can be implemented.

3.2 Network Management and Security

3.2.1 Local IoT Network

Enterprises function in a variety of network settings. Some Enterprises may share networks with other organizations, have one or many multiple networks, and may have varying degrees of external network connections such as for cloud computing. For this architecture, it is considered best practice to have one dedicated local network for IoT devices. This is called the "local IoT network" and is considered to offer an extra layer of security to both the devices and Enterprise via separation of IoT device functions from the Enterprise business network in case of a security breach or malfunction.

The recommendations provided below are in order of increasing security, but not necessity. Enterprise IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

3.2.1.1 Architecture Recommendations

- The local IoT network should create an environment dedicated to IoT devices and communications
- The local IoT network should be separate from the "business" network (local or not)
- Enterprises that share networks with other organizations may consider implementing a new dedicated network, or partitioning their current network
- IoT devices should be networked in a way that ensures devices only communicate with the services and peers required and reinforces confidentiality, integrity, and accessibility of information and networks

3.2.1.2 Hub Attributes

- The Hub should act as a gateway between the IoT network and other networks
- The Hub should minimize the attack surface, identify and address threat vectors

3.2.2 Separation of Testing, Staging and Live Systems

Before connecting a new IoT device to the local network, an Enterprise may consider testing the device in a closed staging or test network to verify the device and reduce the risk of the new IoT device or devices, lowering the security of the current IoT ecosystem.

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

3.2.2.1 Architecture Recommendations

- The Enterprise should have the ability to connect and test devices before putting them on the live system
- The Enterprise should have at minimum a “test” or “staging” and “live” system
- The Enterprise may decide to have a “development” system if required

3.2.2.2 Hub Attributes

- The Hub should have a test or staging system function
- The Hub should have the ability to manage device setup
- The Hub should manage device connection

3.2.3 Gateways and Firewalls

A gateway is a hardware device that acts as a “gate” between two networks. The gateway function may be incorporated into a router, firewall or other device that controls the ingress and egress of traffic in and out of the network.

By it acting as a “gate” between two networks it is considered to be inevitably at the edge of a network, given that all the external network traffic must pass through it. Apart from acting as a gate it may also translate connections from the external network into protocols compatible with those supported by devices within the internal network.

A firewall is a more advanced type of gateway, which inspects and filters inbound and outbound network traffic and where necessary preventing connections being made with suspicious or unauthorized sources. A further evolution of the firewall that allows application layer (seven) filtering which allows the URL level traffic filtering.

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise’s IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

3.2.3.1 Architecture Recommendations

- The Enterprise should implement best practice network security using firewalls and gateways to protect networks and data flows
- The Enterprise should enable traffic segmentation and routing
- The Enterprise should enable traffic monitoring

3.2.3.2 Hub Attributes

- The Hub should act as a gateway to other local and/or external networks
- The Hub should act as a central point for monitoring gateways and firewalls
- The Hub should offer alert and notification in the event of anomalies

3.2.4 Examples of Network Management Tools

While this architecture does not prescribe any one specific solution or make assumptions regarding the IoT security requirements of the Enterprise, below are examples of how a Hub architecture may interface with or support network management in the IoT ecosystem.

- A router (or a Hub) in the Enterprise may be used to split the local network into two – one to function as a “business network” and the other as an “IoT network”
- The Hub can then act as a gateway between the business and IoT networks. For instance, to auto-update shipping logs for manufactured goods

- The IoT manager can use the Hub to further separate the IoT network into “testing” and “live” systems to set up new IoT devices before introducing them to the IoT ecosystem. For instance, for testing interoperability when introducing a new smart lightbulb make or model into the Enterprise environment

3.3 Connecting Devices Securely

3.3.1 Authentication and Authorization

The secure authentication of an IoT device’s identity and its software deployed in the Enterprise is critical to ensuring that only approved and trusted devices are deployed into the Enterprise. Authentication is the process of verifying that a thing (or person) is what it claims to be. Authenticating a device verifies its identity and/or attributes of the device. Once authenticated, the network manager can authorize the device to function on the network.

Authentication supports other good security practices such as authorization and non-repudiation. Non-repudiation is “the ability to prove that a person, entity or process cannot deny having carried out an action” [Ref 9]. Authorization grants permissions to the device, such as network access and associated parameters. In the same vein, permissions can be taken away from specific devices, for instance at end-of-life or in the event of ownership transfer.

In order for successful authentication and authorization in a mixed-vendor environment (i.e. for the Enterprise to not be constrained by vendor or ecosystem lock-in) devices need to be interoperable and support internationally recognized standards. Whilst standardization is still in its infancy, there are initiatives in this area, an example is the IETF draft on the remote bootstrapping of PKI credentials [ref 17]. Solving issues of interoperability is not a primary aim of this document, but should be a key consideration for OEMs developing devices for the Enterprise and for IoT managers and developers implementing these hub architectures. Particular areas that need standardization are:

- Protocol or protocols for IoT devices and hubs which support:
    - Trusted software update which allows the option of a Hub to act as a broker between manufacturer and device, particularly within a heterogeneous environment of multiple manufacturers and their devices
    - IoT device secure credential dissemination which can be authenticated by the Hub or Hubs.
    - A Hub being able to enumerate IoT devices and establish their state in a safe and secure way.
- A common method of describing detected security events acting on an IoT device

Unlike traditional IT equipment which either has a human interface or a standards-based interface used to configure and load trust credential, IoT devices are typically “headless”. As a result, the installation of the trust credentials to allow the device(s) and the Enterprises’ network to authenticate each other represent a challenge to scalable deployment. In the case of network access this can be problematic for Enterprises when a device expects its wireless configuration to be carried out over a local wireless interface and involves the sharing of the Enterprise’s wireless credentials to the device.

Throughout the lifecycle of an IoT device, authentication and authorization will be used repeatedly to verify and manage devices, including assigning and revoking privileges. Authentication and authorization form a foundation for additional security layers such as (in order of increasing security, but not necessity):

- **Device Identity Management** – the ability to identify a device or group of devices, enabling actions such as authorization and privilege management
- **Black or Whitelisting** – verifying only desired (e.g. authenticated) devices access the network by managing access or privilege control tools (e.g. granting authorization)

- **Granting Privileges** – authorizing access or actions based on attributes (e.g. allowing devices connected to a "visitor network" access to a "visitor printer", but not the Enterprise business network)
- **Revoking Privileges** – removing or preventing a privilege based on attributes (i.e. removing authorization to access the Hub system from a decommissions smart light solution which is installed in the building but no longer in use)
- **Roots of Trust** – use of trust-building tools, such as certificates or encryption, to provide a trust foundation in the IoT system (e.g. using certificate authorities to authenticate devices)
- **Validating Software Updates** – with the use of digital signatures and/or encryption based upon a suitable root of trust to validate that the software update is from an authentic source, typically the product's OEM or authorized software provider

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

3.3.1.1 Architecture Recommendations

- Enterprises should use only IoT solutions that can be authenticated where possible to ensure only known devices are allowed on the network and support ongoing trust between devices
- Develop authorization management structure to determine a device's privileges on the network (i.e. connectivity, routing, requests, files)
- Have the ability to revoke authentication and/or authorization to decommission devices or transfer ownership

3.3.1.2 Hub Attributes

- The Hub should be a central point for supporting authentication. It may:
    - Carry out authentication processes
    - Act as a cache for authenticated devices
    - Store authentication credentials
    - Support varying levels of authentication (e.g. single token, server, and mutual authentication)
- The Hub should be a central point for supporting authorization. It may:
    - Act as a device management tool to apply or revoke privileges
    - Support creation and enforcement of permissions lists (e.g. black- and whitelists)
    - Support trusted device/group identity management
- The Hub should provide alerts if an authenticated device has been tampered, authorization privileges have been modified, or is trying to execute unauthorized actions
- A Hub should use at minimum best practices in password and cryptography systems to support authentication and authorization processes

3.3.2 Secure Boot

Secure boot is the process through which the device validates the integrity of the software from boot time onwards. For larger systems there are three levels of secure boot types in increasing level of security listed below:

- **Secure Boot**: The device verifies that its bootloader is correctly digitally signed and that no changes have been made to the firmware
- **Trusted Boot**: The device's bootloader checks the digital signature of the operating system and the operating system checks the integrity of every component of the startup process before loading it
- **Measured Boot**: The device's firmware logs the boot process metrics including the Operating System boot and securely sends the metrics to a trusted server that can attest to the trustworthiness of the device

In smaller embedded systems, the Secure Boot and Trusted Boot may involve the use of a microcontroller or microprocessor that starts executing software from internal and immutable memory. The software stored in the immutable memory in the microcontroller is considered inherently trusted (i.e., the root of trust) because it cannot be modified. This inherently trusted software then authenticates the software, such as the operating system not stored in immutable memory, through a cryptographic process such as digital signing or decryption, using a root of trust stored securely within the microcontroller/processor.

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

3.3.2.1 Architecture Recommendations

- Use only Hub solutions that support secure boot to ensure that their integrity cannot be compromised and that only authorized software can be deployed onto them
- Have the ability to revoke authentication and/or authorization to enable the secure decommissioning of Hubs or transfer Hub ownership

3.3.2.2 Hub Attributes

- The Hub should provide alerts if an attempt is made to install unauthenticated software or the Hub has been tampered, authorization privileges have been modified, or is trying to execute unauthorized actions
- A Hub should use at minimum best practices in roots of trust and sources of entropy, for its cryptography systems to ensure support for secure authentication and authorization processes. For further details on this best practice subject please see in the "IoT Security Compliance Framework" section" [ref 1]

3.3.3 Roots of Trust

Roots of trust are at the core of this Hub-based architecture because the Hub acts as a central trust anchor and management tool, deciding which devices or network infrastructure to trust. Without a root of trust, particularly public roots of trust, this is a difficult problem to solve. Public roots of trust are considered a more secure and practical solution than private roots of trust in the Enterprise context, primarily because of the increased responsibility placed on the Enterprise and risks that come with poor management of private roots of trust. Public roots of trust also better support other needs such as interoperability.

Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. By design, roots of trust must be highly secure since they are used as a fundamental trust point. To prevent tampering or extraction of their contents, roots of trust are normally implemented in hardware to provide a strong trust foundation.

An Enterprise will need to make an informed decision on whether best to use public or private roots of trust for its specific IoT deployment model. While there might be certain situations where private roots are preferable as discussed below, in general private roots of trust are not considered the most effective solution in the context of Enterprise IoT. Implementing a private root of trust places additional responsibility on the Enterprise to ensure roots of trust are managed appropriately.

Executing key management and creating private roots of trust can result in interoperability issues and security weaknesses. For instance, private roots of trust used to embed certificates in devices may result in issues of management and scalability – particularly where devices may have limited or no user interface ("headless devices"). Keys left unmanaged, certificates not revoked appropriately, or not re-issued to keep pace with technological change can weaken security and negatively impact trust in the IoT ecosystem.

Private roots of trust do have specific benefits in the case of internal services authentication, for example authenticating connections into the Enterprise's internal WiFi or virtual private network(s) (VPN). These are cases where there are significant benefits to the Enterprise being able to specifically control which devices or connections can be authenticated by internal systems. If the Enterprise uses it own private root then no other entity can issue certificates except those authorized within the Enterprise and the certificate profiles can be customised to suit the Enterprise's specific requirements.

As their name implies, public roots of trust are ones which are publicly accessible and allow third parties to authenticate each other without prior credential exchange. Embedding public roots of trust where possible helps circumvent issues presented by private roots – such as scalability – and supports a long-term approach to treating risks associated with Enterprise IoT deployments. A number of the challenges of the deployment of roots of trust can be overcome with a combination of the use of public roots of trust and the use of Identity Access Management systems.

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

3.3.3.1 Architecture Recommendations

- If considering private roots of trust, the Enterprise should execute a risk assessment to help identify the best way forward
- Implementations should support best practices in roots of trust [see refs 3, 12 and 16]
- Roots of trust should be utilized to support authentication and authorization processes
- Roots of trust may be used to support identification of malicious software

3.3.3.2 Hub Attributes

- The Hub shall support the cryptographic hashing and encryption/decryption functions used in the authentication of chains of trust, in particular:
    - A Hub shall support industry standards in cryptography
    - A Hub shall support best practices in cryptography [see ref 1]
    - A Hub shall have a hardware root of trust
- The Hub should have the ability to manage private and public roots of trust
    - The Hub may be able to create and manage private roots of trust for the Enterprise
    - The Hub should be able to support public roots of trust
    - The Hub should securely store and/or cache roots of trust
- The Hub may enable roots of trust by acting as an intermediary between device and certificate authority
- The Hub should provide a cryptographically secure method to update and revoke its cryptographic keys, including those keys used for the authentication of updates
- The Hub may use roots of trust to assist detection of malicious software

3.3.4 Examples of Tools to Connect Devices Securely

While this architecture does not prescribe any one specific solution or make assumptions regarding the IoT security requirements of the Enterprise, below are examples of how a Hub architecture may interface with or support connecting devices securely in the IoT ecosystem.

- A Hub can manage white lists to ensure only authorized devices connect to the IoT network. For instance, in shared office spaces multiple Enterprises may have access to local networks. However, whitelisting IoT devices allowed onto the IoT network will protect the network from being accessed by office, IoT and BYOD devices in the shared space

- A headless device, such a motion sensor, with a root of trust may need to be authenticated by a certificate authority. In this case, the Hub can act as an intermediary, communicating directly with a certificate authority and providing a user interface to prompt or track the authentication process. After the root of trust has been authenticated, the IoT manager can grant the motion sensor authorization to access the IoT network

3.4 Lifecycle Management

3.4.1 Monitoring and Audit

Monitoring and audit of IoT ecosystem devices, networks, resources, and performance are key elements of IoT security. Information and measures resulting from monitoring and auditing can be aggregated in a centralized location for better IoT ecosystem visibility and control. A Hub acts as a central repository of information for IoT managers about the functioning and statuses of the IoT ecosystem and can be used to inform resulting actions. The IoT manager will be able to take more informed decisions based on what is learned and can be applied via the Hub, particularly with the rapid development of machine learning and data analytics. This includes aggregation of information from other security tools such as firewalls, gateways, and network access controls. These tools may or may not be directly managed from the Hub, however, they may share information such as:

- **Notifications** – A notification is information delivered by the system to the IoT ecosystem managers and/or IoT users as appropriate. This could include push notifications (such as an unexpected incident alert notification) or pull notifications (such as requested status updates). Notifications support security by providing essential information to the IoT manager on events and incidents in the ecosystem and thus respond appropriately
- **Alerts** - An alert is a type of notification that is important or time sensitive. For instance, alerts can support IoT security via timely notification, and thus response, when incidents are detected in the IoT ecosystem
- **Status Updates** – Status updates are a type of notification that provide the ability for IoT managers to determine the status of an IoT device or network at any given time, such as device status (e.g. on/off, in use/not in use), or software update/ patch status. Status updates support security by contributing to the overall snapshot of IoT ecosystem statuses, health, and security management processes
- **Report** – A report, such as an incident report or system snapshot, can include historic and current information such as time/date stamps, impacted networks and devices, taken or scheduled actions. Reporting provides an understanding of events and may also assist in demonstrating compliance with local and industry-specific regulations

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment and security requirements should be taken into consideration when identifying the most desirable Hub features.

3.4.1.1 Architecture Recommendations

- An Enterprise should have tools for monitoring and auditing its IoT ecosystem, which supports troubleshooting, checking network health, tracking data flows, and demonstrating policy compliance. This may include:
    - Monitoring/auditing devices
    - Monitoring/auditing networks and Hubs
    - Monitoring/auditing traffic flows
    - Raising alerts and notifications when an event is detected
- An Enterprise should have a central location to review alerts, notifications, or reports resulting from monitoring and audits
- Monitoring and auditing should be provided to the extent needed to manage the network. This may include information such as:

- Metrics on resource consumption (e.g. power)
- Data transfer and flows
- Access requests and logs
- Changes to device and network parameters
- Temporary devices and associated actions

It is important to note that network monitoring and audit are subject to local policy and regulation – such as privacy and data protection – and should be implemented in a manner consistent with relevant legislation for that Enterprise sector.

3.4.1.2 Hub Attributes

- The Hub should enable monitoring and audits. These may be done continuously, be time-constrained or done routinely
- The Hub should provide reporting tools for monitoring and audits, this may include:
  - A log of monitoring and audit activity
  - Access to past reports
  - Query options
- Following monitoring or audit, the Hub should provide alerts or notifications of relevant information such as incidents or measures outside set parameters
- As a result of monitoring and audit, the Hub should enable Enterprise IoT managers to take necessary actions either directly via the Hub or outside the Hub. This may include actions such as:
  - Controlling traffic flows and segmentation
  - Implementing anti-virus/malware solutions
  - Pushing updates or patches to devices
- Hubs supporting roots of trust should be able to audit and update roots as necessary

3.4.2 Update and Patch

A simple but configurable way of securely updating and patching across the IoT ecosystem is an important aspect of IoT security. Updating and patching helps to protect against known threats, fix security vulnerabilities, protect against bugs and improve performance. IoT managers should be able to have a central point of reference for related information such as:

- Completed Updates
- Scheduled Updates
- Update Source
- Update Verification

Implementing reliable mechanisms for tracking and implementing updates supports the integrity, privacy and security of the IoT ecosystem and helps to enable interoperability.

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

3.4.2.1 Architecture Recommendations

- IoT devices should support software and firmware updates and patching from necessary sources (e.g. Enterprise- or manufacturer-pushed)
- The IoT manager should be able to log updates/patches and create related reports
- Update mechanisms should include secure boots and regular reboots for devices, such as code signing to verify updates

3.4.2.2 Hub Attributes

- The Hub should keep an update/patch log with reporting capabilities, for example:
    - The Hub should log information regarding past and future updates such as time stamps or scheduled updates
    - The Hub should log information about update provenance and verification
    - The Hub should support automatic and manual input
- The Hub should be able to manage updates and patching centrally to the extent possible, for example:
    - The Hub may be able to cache updates for IoT devices
    - The Hub should support devices with limited or intermittent connectivity and multi-part updates
    - The Hub should support automatic and manual initiation of updates
    - The Hub should be able to manage updates from a variety of sources (e.g. Enterprise- and manufacturer-pushed)
- The Hub itself should be kept as up to date as possible as it provides a high level of security to the IoT ecosystem and management
    - The Hub should be easy to update
    - The Hub should be able to monitor, audit, and report its update and patch status
    - The Hub may be able to auto-update if allowed

3.4.3 Manage Device Identity and Authorization

Device identity is not a primary focus of this proposed Hub architecture. However, it is worth noting that identity has a useful role in supporting security functions enabled by this Hub architecture – such as authentication, roots of trust, and device lifecycle management. For instance, identifying a device can support assigning or revoking device privileges and make tracking and implementing updates easier.

The specific technologies, services, or other resources that may be used to assign and/or manage device identity is not within the scope of this proposed Hub architecture. No identity solution or management tool is presumed or prescribed here. There are a range of solutions, both available and developing, that can be successfully used in IoT deployment.

In addition, there may be situations when sharing or assigning a device identity may not be desired by either party. For instance, personal devices brought onto the Enterprise network by employees, such as smart watches or fitness trackers. Personally identifiable information, particularly that which is not required for business functions, is not in scope of this paper and should be handled in a manner consistent with local data protection and privacy policies.

Taking this into consideration, in an IoT ecosystem, it should be possible to assign identity to all devices or groups of devices as appropriate. Identity may be provided via a variety of resources including, but not restricted to:

- Manufacturers
- Private and bespoke identity schemes
- Third party solutions or services
- Hub solutions

If an Enterprise decides to implement an identity scheme, a Hub may:

- Improve overall IoT ecosystem management and security
- Provide a centralized database for device and/or identity management
- Provide flexibility to assign a device to one or multiple groups
- Provide flexibility to assign attributes and authorizations to a device and/or group of devices

3.4.4 Managing Device End-of-Life

An IoT device's lifetime can be unique to each deployment. For an IoT device, the end of life will most likely be the result of a number of factors, including but not limited to:

- Manufacturer end-of-sale or support (such as discontinuing updates and patches)
- Enterprise upgrade or solution change including integrating new devices and decommissioning old devices
- Change of ownership, where an Enterprise may inherit or transfer ownership of IoT systems (for example in the case of office location change)

Security practices included in this architecture support good practices for end-of-life management. For instance, there are a number of security practices that need to be considered when managing end-of-life, including but not limited to:

- Managing permissions and revoking authorization
- Understanding what Enterprise information is accessible by the device and removing or protecting this data
- Data erasure – permanent deletion of any settings, user account information etc.
- Decommissioning or transferring device identity
- Precautions for transferring device ownership, such as data erasure, factory re-set, etc.

A Hub architecture provides a central location to query information about the device, its authenticity, authorizations, network access and in some cases execute the necessary actions to revoke permissions and decommission a device and/or the Hub itself from the IoT ecosystem.

3.4.5 Examples of Lifecycle Management Tools

While this architecture does not prescribe any one specific solution or make assumptions regarding the IoT security requirements of the Enterprise, below are examples of how a Hub architecture may interface with or support lifecycle management IoT ecosystem:

- A Hub should monitor the traffic in and out of the IoT network. For instance, there might be coffee machines communicating with the office manager as well as sending usage statistics to the supplier once a day. However, if outward coffee machine traffic suddenly spikes to once a minute then the Hub may alert the IoT manager to suspicious activity. It may be that the device has been compromised, such as infected by malware utilized in a DDoS attack. In this case, the IoT manager can immediately take the device offline
- Some updates may need to be pushed to devices by IoT managers. For instance, a Hub can receive alerts from a smart board manufacturer when an update or patch is available. The IoT manager can then immediately push the update to the device or place it in a queue for updating outside of normal business hours. Once the update has been installed, the Hub can receive notification and update the patch log for the smart board
- A Hub will have a user-friendly interface to manage IoT devices. An Enterprise adopting solutions from multiple vendors – such as light bulbs form Vendors A and B and door locks from Vendor C – may find a variety of identifiers, not necessarily user friendly, attached to the devices (such as lb_12345 or lock_jfk). In the Hub interface, the IoT manager can assign unique identifiers and location or vendor attributes to devices (such as "Light: vendor A, Office 245" or "Door Lock: Vendor B, meeting room A"). The IoT manager can then search by vendors, locations, or type of IoT solution to oversee, grant or revoke authorization, and delete data relating to a device or group of devices

3.5 Hub Device Security

In the end, the Hub architecture presented here is based on a central device and user interface as the foundational element of the Enterprise IoT ecosystem and security. Hub device security and development are not the focus of this document, but it is worth noting that the device must include robust security. This includes features such as:

- User access permissions that support best practices in system and information security
- Ability to securely store sensitive information such as roots of trust
- Alerts and notification of anomalies
- Security considerations for web and mobile user interfaces as well as network connections
- Secure Boot

The Hub device should adopt security best practices. There are public resources available that help Enterprises as well as developers implement security best practices into their IoT solutions. One example is the IoTSF's "IoT Security Compliance Framework" [ref 1]. In this document, security compliance frameworks are laid out for a range of topics related to the four main Hub functions and support capabilities included in this Hub architecture. The compliance framework sections as presented here are relevant to Hub device security and development and are mapped to the Hub-based reference architecture below.

Hub Functions	Compliance Framework Sections
Network Management	• Cloud and network elements • Secure supply chain and production
Connecting Devices Securely	• Device wired and wireless interfaces • Authentication and authorization • Encryption and key management for hardware • Configuration
Lifecycle Management	• Device hardware and physical security • Device software • Device operating system • Device ownership transfer
Information Security	• Business security processes and responsibility • Web user interface • Mobile application • Privacy

Table 3 IoTSF Compliance Framework Mapping

4 References and Abbreviations

4.1 References

The following references are used in this document:

1. IoTSF "IoT Security Compliance Framework": https://www.iotsecurityfoundation.org/best-practice-guidelines
2. IETF "Key words for use in RFCs to Indicate Requirement Levels": https://www.ietf.org/rfc/rfc2119.txt
3. NIST Computer Security Resource Center "Roots of Trust": https://csrc.nist.gov/Projects/Hardware-Roots-of-Trust
4. NIST SP 800-57 Part 1 Rev. 4 "Recommendation for Key Management, Part 1: General" https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final
5. NIST SP800-57 Part 3 Revision 1" NIST Special Publication 800 – 57 Part 3 Revision 1 Recommendation for Key Management Part 3: Application - Specific Key Management Guidance" http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf
6. FIPS PUB 140-2, Security Requirements for Cryptographic Modules http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
7. UK Government DCMS "Secure by Design report": https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
8. IoTSF "Application Note: Mapping the IoT Security Foundation's Compliance Framework to the DCMS proposed Code of Practice for Security in Consumer IoT": https://www.iotsecurityfoundation.org/wp-content/uploads/2018/03/RELEASE-DCMS_Principles_Application_Note_07_03_2018.pdf
9. ISO/IEC "Information Technology – Security techniques – Information security management systems – Overview and vocabulary: http://standards.iso.org/ittf/PubliclyAvailableStandards
10. IoTSF "Make it safe to connect: Establishing principles for Internet of Things Security": https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf
11. IoTSF "Secure Design - Best Practice Guidelines L Software Update Policy": https://www.iotsecurityfoundation.org/best-practice-guidelines
12. NCSC UK "Guidance - Provisioning and securing security certificates" https://www.ncsc.gov.uk/guidance/provisioning-and-securing-security-certificates
13. European Commission "2018 Reform of Data Protection Rules": https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
14. European Commission "Latest NIS Cooperation Group's guidelines for implementing the NIS Directive and addressing wider cybersecurity policy issues": https://ec.europa.eu/digital-single-market/en/news/latest-nis-cooperation-groups-guidelines-implementing-nis-directive-and-addressing-wider
15. Office of the Federal Register (US). "CISA 2015 Final Guidance Documents": https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability
16. NIST Computer Security Resource Center "Guidelines on Hardware - Rooted Security in Mobile Devices (Draft)": https://csrc.nist.gov/publications/detail/sp/800-164/draft
17. IETF Bootstrapping Remote Secure Key Infrastructures (BRSKI) draft 16, June 21st 2018: https://tools.ietf.org/html/draft-ietf-anima-bootstrapping-keyinfra-16

4.2 Definitions and Abbreviations

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

PKI	Public Key Infrastructure
TRNG	True Random Number Generator
TBC	To Be Confirmed
TBD	To Be Determined
TLS	Transport Layer Security

5 Appendix A – Sample Threat Modelling

Threat	Threat Example	Treatment Examples	Hub Architecture Treatment Correlation
Spoofing	Employing spoofing of IP addresses and/or user datagram protocol (UDP) to obtain credentials to gain unauthorized access to a device Address resolution protocol (ARP) spoofing used to redirect data traffic to the attacker Spoofing notifications or alerts Sending spoofed packets to influence the functioning of a device (e.g. stop, start, or modify data collection and transfer) Enterprise user unknowingly being directed to a spoofed website of a cloud service provider	Update and patch devices to prevent vulnerability exploitation Roots of trust to support trusted identity and access Manage device identity to support a compromised devices' authorization and access privileges and end of life provisioning Implementing gateways and firewalls to identify suspicious traffic	Gateways and Firewalls [3.2.3] Authentication & Authorization [3.3.1] Roots of Trust [3.3.3] Update and Patch [3.4.2] Device Identity and Authorization [3.4.3] Managing End-Of-Life [3.4.4]
Tampering	Tampering with a connected door lock to gain unauthorized control Covertly modifying a sensor's data sharing permissions Tampering with software to modify permissions, install spyware or backdoors Tampering with data, impacting the trust, and possibly business processes, in the IoT ecosystem	Use roots of trust to support non-repudiation Secure boot and update to ensure software and hardware are modified by trusted sources Secure management of access controls Monitor and audit device status and traffic flow to identify unauthorized activities Set up new devices or services in a staging system to prevent tampered devices from accessing the live network	Separation of Systems [3.2.2] Gateways and Firewalls [3.2.3] Authentication & Authorization [3.3.1] Secure Boot [3.3.2] Roots of Trust [3.3.3] Monitor & Audit [3.4.1]

Repudiation	Sensor data is modified in transit to the cloud service and Enterprise metrics are affected Device A receives a command seemingly from Device B but it was sent actually by an unknown source and leads to malfunction A staff group share a group password/authentication process for accessing a system	Use of digital certificates to support secure identity of users and devices Public key infrastructure to manage and revoke digital certificates and roots of trust Secure boot and update to ensure only authorized modification of software and hardware Information security best practices – managing individual user access controls	Authentication and Authorization [3.3.1] Roots of Trust [3.3.3] Secure Boot [3.3.2] Device Identity and Authorization [3.4.3] Managing End-Of-Life [3.4.4]
Information Disclosure (Data Breach)	Corporate espionage and black hat hacking Disgruntled employee accesses and copies confidential or sensitive information Diagnostics information shared with an OEM which discloses proprietary Enterprise information Unauthorized access to security cameras Password leaks or unauthorized password/credential modification Packet capture via man-in-the-middle or similar type attacks	Monitor and audit traffic on and outside of the local IoT network Alerts for suspicious data traffic Privilege-based or other fine-grain user authorization management Adoption of information security management best practices Separating business and IoT networks Encryption of data	Local IoT Network [3.2.1] Gateway and Firewalls [3.2.3] Authentication and Authorization [3.3.1] Monitoring and Audit [3.4.1] Device Identity and Authorization [3.4.3] Managing End-Of-Life [3.4.4]
Denial of Service	Using exploits in connected devices to execute a DoS attack on the Enterprise website Using exploits in connected devices to disrupt normal business functions of the Enterprise's connected systems Using exploits in connected devices to execute a DoS or	Traffic monitoring and management (ingoing and outgoing) Use of gateways and firewalls to monitor and block traffic Blocking devices from communicating outside the LAN or Enterprise Restricting access to	Local IoT Network [3.2.1] Gateways and Firewalls [3.2.3] Monitor and Audit [3.4.1] Update and Patch [3.4.2] Device Identity and

	DDoS attack on a third-party network or site Using exploits in connected devices to execute a DoS or DDoS attack on another IoT device in the network	command/control functions of devices Taking compromised and irreparable devices out of the Enterprise IoT ecosystem securely	Authorization [3.4.3] Manage End-Of-Life [3.4.4]
Elevation of Privilege	A smart device zero-day exploit that allows a third party onto the LAN Unauthorized access of a cloud service provider's system enabling access to the Enterprise business network Gaining high-level privileges which enable command and control of a thing-bot	Lifecycle management and decommissioning old or compromised devices Separation of IoT and business networks to discourage privileged users from accessing non-relevant business information Privilege-based or other fine-grain user authorization management to prevent access to non-relevant information, controls and devices	Local IoT Network [3.2.1] Authentication & Authorization [3.3.1] Monitor and Audit [3.4.1] Device Identity and Authorization [3.4.3] Managing End-Of-Life [3.4.4]
Regulatory Non-Compliance	Inability to or difficulty in proving compliance for audit purposes Lack of easily applied metrics to measure compliance or identify security shortfalls Need to prove compliance after a data breach to show due diligence	Log and report on security features and ecosystem management Enable security best practices Identify, manage, and update regulation compliance measures	Highly dependent on regulatory requirements. Common examples are: Gateways and Firewalls [3.2.3] Authentication & Authorization [3.3.1] Monitoring and Audit [3.4.1]
Unsupported endpoint management	Out of date devices with known exploits or bugs being exploited to access IoT networks Devices with outdated software or firmware Inability to encrypt data or assign a root of trust Inability to remotely manage end-of-life	Monitor data traffic and enable alerts for suspicious traffic Manage authorization and access to devices Physically manage updates or push updates where possible Create a secure environment for devices - separate devices from WAN and	Local IoT Network [3.2.1] Separation of Systems [3.2.2] Gateways and Firewalls [3.2.3] Monitor and Audit [3.4.1] Update and Patch [3.4.2]

		business networks Set up devices with minimal security features in a testing or staging system to prevent impact on local IoT network	Manage End-Of-Life [3.4.4]

6 Appendix B – Note on Information Security Best Practices

It is assumed that information security best practices will be implemented with IoT deployments, be structured in a way that best meets the needs of the Enterprise, and is in compliance with relevant regulations such as local data protection and privacy regulations. Information security best practice are not the focus of the architecture, but more information on how they relate can be found in Appendix B.

Because many IoT solutions are wholly or in part provided via a cloud-based service it is important to note that an Enterprise should assess risks associated with data transfers outside the organization. This may include business operational data (such as client information), sensor data (such as lights and temperature), or other types of data which provide information about the Enterprise. Data which is sensitive or business-critical may require additional levels of security which is best managed within the organization, while others may find service providers better-suited to some types of information management and security. Risks associated with external and/or internal data management will be unique to the Enterprise, therefore no assumptions are made here about the Enterprise's chosen solution.

Information security best practices should be incorporated throughout the IoT system were necessary, for example:

- Data security at rest and in transit
- User authentication and access privileges
- Securing sensitive information (e.g. keys and certificate management)

For these reasons there is not a dedicated information security section of this Hub architecture. However, relevant information on this topic is provided where needed.

For more information on this topic specifically, Enterprises can consult a range of resources regarding information security standards and best practices made publicly available through independent organizations, standards bodies, and national governments including IoT Security Foundation, ISO, BSI, NIST, and NCSC.

www.iotsecurityfoundation.org