# BLUESKYTEC'S RESPONSE TO THE UK GOVERNMENTS

# "SECURITY BY DESIGN"

A number of organisations are at the forefront of protecting our on-line digital life. They are producing policy, laws and industry best practice to help secure the internet of things. High profile people such as: Margot James, Minister for Digital and Creative Industries and Ian Levy, Technical Director NCSC have commissioned "SECURITY BY DESIGN" a guide to best-practice for the IoT/ICS industry.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

Microsoft have published a similar report on the recommended security model for IoT/ICS devices.

https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf

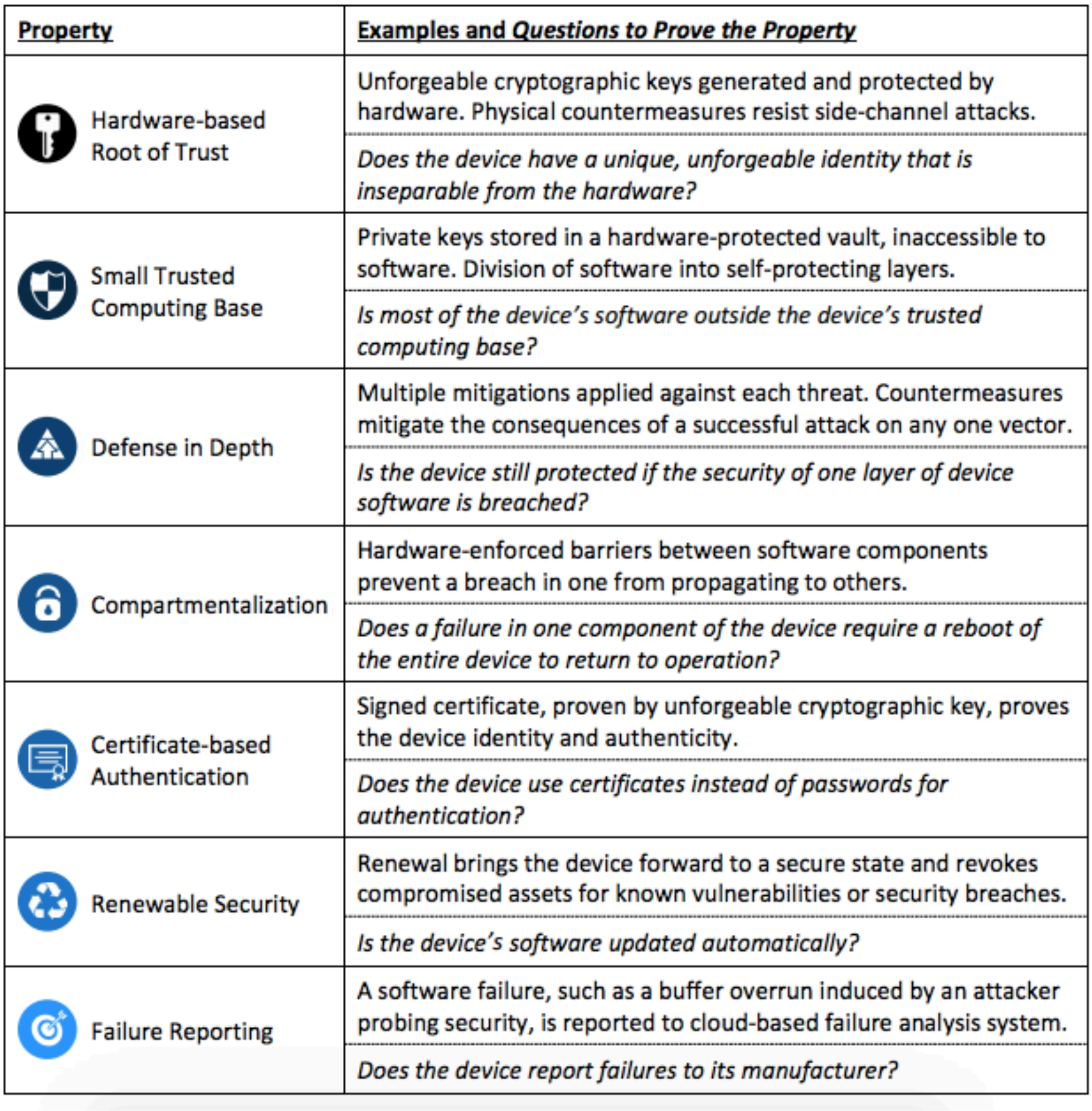
This paper details Blueskytec's response to the published recommendations and how we endorse and meet all aspects of the recommendations in a low cost hardware & software IoT device.

## Accreditation

In the published reports given by the UK government and Microsoft they detail the measures taken for securing-by-design, an IoT device. These reports are aimed at subset of cyber-physical devices that span the Internet of Things, Industrial Control Systems, Personal Transport systems. Although the reports are aimed at IoT the recommendations should be applied to every device that is a cyber-physical system – i.e. and embedded system that connects to the internet.

These reports contain recommendations that are enshrined in many standards – Common Criteria, ISO13491, PCI PTS, FIPS140-2, CITA, Achilles. Blueskytec firmly believe that hardware enforced secure systems, backed up by standards are the only way to protect sensitive and valuable systems.

The Microsoft recommendations are highlighted in the table below, and these correspond to the 13 points outlined in the UK Governments "Secure by Design" document, which is included at the end of the document.



| **Property** | ***Examples and Questions to Prove the Property*** |
|---|---|
| Hardware-based Root of Trust | Unforgeable cryptographic keys generated and protected by hardware. Physical countermeasures resist side-channel attacks. |
| | *Does the device have a unique, unforgeable identity that is inseparable from the hardware?* |
| Small Trusted Computing Base | Private keys stored in a hardware-protected vault, inaccessible to software. Division of software into self-protecting layers. |
| | *Is most of the device's software outside the device's trusted computing base?* |
| Defense in Depth | Multiple mitigations applied against each threat. Countermeasures mitigate the consequences of a successful attack on any one vector. |
| | *Is the device still protected if the security of one layer of device software is breached?* |
| Compartmentalization | Hardware-enforced barriers between software components prevent a breach in one from propagating to others. |
| | *Does a failure in one component of the device require a reboot of the entire device to return to operation?* |
| Certificate-based Authentication | Signed certificate, proven by unforgeable cryptographic key, proves the device identity and authenticity. |
| | *Does the device use certificates instead of passwords for authentication?* |
| Renewable Security | Renewal brings the device forward to a secure state and revokes compromised assets for known vulnerabilities or security breaches. |
| | *Is the device's software updated automatically?* |
| Failure Reporting | A software failure, such as a buffer overrun induced by an attacker probing security, is reported to cloud-based failure analysis system. |
| | *Does the device report failures to its manufacturer?* |

Microsoft's answer to the question of security.

## BLUESKYTEC'S RESPONSE TO THE RECOMMENDATIONS:

### Hardware based root of trust

UK NCSC "Secure By Design" Recommendations:
(1) No default passwords.
(4) Securely store credentials and security-sensitive data.

Microsoft Industry Best Practice guide:
Unforgeable cryptographic keys generated and protected by hardware.

All modules should have a hardware based trust anchor. This is a set of cryptographic keys and Known Answer Tests that are unique to each device and provide a guaranteed point of trust for all cryptographic processes. The trust anchor is constructed from a set of Physically Uncloneable Functions – information that is destroyed upon attempted removal or copying. The PUF is immune from removal and copying even with the power removed from the module and invasive techniques such as Scanning Electron Microscopes or Ion Beam are used.

### Small trusted computing base

This applies to "Secure By Design" Recommendations:
(4) Securely store credentials and security-sensitive data.
(7) Ensure software integrity.

Microsoft Industry Best Practice guide:
Private keys stored in a hardware protected vault, inaccessible to software.
Division of software into self-protecting layers.

The trusted computing base must be contained within the hardware vault and cannot be tampered with. This is either a 16 or 32 bit simple processor, with no memory management. This trusted computing base cannot be updated and is verified as secure by the design and anti-tamper measures. The cryptographic keys and root of trust (PUF) can only be accessed by the trusted computing base. The trusted computing base provides the Security Enforcing Functions and will enter tamper alarm, where all the cryptographic keys are erased. The hardware of the trusted computing base is protected against physical tampering of the circuit board and will permanently erase and destroy the whole contents of the module upon physical tamper, rendering it scrap.

There are numerous physical parameters that the hardware vault measures in order to determine from its surroundings if it is under attack. These are a critical design requirement for FIPS140-2 level 3 or 4 and the design will not pass certification if these measures are not in place.

## Defence in depth

This applies to "Secure By Design" Recommendations:
(4) Securely store credentials and security-sensitive data.
(6) Minimise exposed attack surfaces.
(7) Ensure software integrity.

Microsoft Industry Best Practice guide:
Multiple mitigations applied against each threat.
Countermeasures mitigate the consequences of a successful attack on any one vector.

All certified modules contain many layers of security – passive physical, active physical, active logical that protect all data within the module. All data at rest, stored in on-module memory is encrypted to AES256. If the power is removed NO data remains on the device that is not encrypted to AES256. Multiple levels of anti-tamper are built into the hardware to compartmentalise and fortify the computing platform. The trusted computing base is protected in the secure vault by hardware and can only be accessed by user code through the security interface. The user code running on the main processor is segmented into areas that have different levels of access. The main operating systems area (Linux for example) can only be run from ROM code that cannot be updated in the field – this is the secure BOOT feature. User code running in FLASH can be updated – but only after the signature has been validated.

## Compartmentalization

This applies to "Secure By Design" Recommendations:
(7) Ensure software integrity
10) Monitor system telemetry data

Microsoft Industry Best Practice guide:
Hardware enforced barriers between software components prevent a breach in one from propagating to another.

Processors used in the main processing sub-system must be separated into a number of areas with different security levels applied to these areas. For example the USB is at a different security level from the UART or CAN bus. Any attempt by software to access these devices without the necessary security results in a tamper alarm and a range of security measures are performed – from complete erasure and destroy of the module (catastrophic breach) to notification over the communications interface of a tamper alarm.

The software is compartmentalised into Operating system components, libraries and user code. Any attempt by user code to overwrite the operating system and library will result in tamper alarm. User code has 2 areas – the active region and the update region. When an over the air update is performed – the code is received, decrypted and authenticated and then placed in the update region. The program then jumps to the update code. If this results in failure the system reboots (via the watchdog timer – or a tamper alarm) and the original code is run. If however the update code is deemed to be correct, this area becomes the new user code and the old area becomes the next update.

## Certificate based authentication

This applies to "Secure By Design" Recommendations:
(5) Communicate securely

Microsoft Industry Best Practice guide:
Signed certificate, proven by unforgeable cryptographic key, proves the device identity and authenticity.

The NIST guidelines recommend that for Symmetrical Cryptography Authentication (the strongest) that the hardware based root of trust is used to provide the authentication for tokens and then once authentication has been established Traffic Keys are exchanged using AES256. For public based authentication where asymmetrical key exchange and authentication is performed the 384 bit ECC is recommended to provide the authentication tokens.

## Renewable Security

This applies to "Secure By Design" Recommendations:
12) Make installation and maintenance of devices easy
3) Keep software updated

Microsoft Industry Best Practice guide:
Renewal brings the device forward to a secure state and revokes compromised assets for known vulnerabilities or security breaches.

Blueskytec believes that to have a fully FIPS140-2 level 3 or 4 accredited Hardware Security Module updates cannot be applied and are not needed. This is because the design MUST be right first time – by verification and validation. The concept of limited testing and user updates, simply does not work with hardware enforced cryptography - this is built into the design so that external forces cannot overwrite the accredited security features. However, application code that is shipped with the system can be extended. The original default "known good code" that can never be overwritten – only extended by updateable modules. In the event of a tamper alarm the system always reverts to this "known good code" and a further user code can then be update and/or patched. If the application that runs on the trusted hardware, has a security breach the system reverts to the known good code and notifies the host system. The host system can then accomplished an OTA update, outlined in the preceding Compartmentalisation section.

## Failure reporting

Microsoft Industry Best Practice guide:
Software failure, such as a buffer overrun induced by an attacker probing the security, is reported to cloud-based failure analysis system.

This applies to "Secure By Design" Recommendations:
(10) Monitor system telemetry data
(2) Implement a vulnerability disclosure policy

All Blueskytec modules have total connectivity SMS/SSD, GPRS, 3G, 4G or 4GNB, WiFi, Satellite and BT. In the event of a tamper alarm or failure of any description the trusted computing base can send a message via any interface to any cloud based monitoring system. This is independent from any software running on the processor.

## Security accreditation – peace of mind

Blueskytec modules include FIPS approved algorithms and processes:

Asymmetrical Cryptography (ECC) - NIST certification number 335 – NIST FIPS 186-4
Symmetrical Cryptography (AES256) - NIST certification numbers 2908 & 2935 – NIST FIPS 192.
Secure Hash Standard - NIST certification numbers 2447 & 2472 – NIST FIPS 202
Deterministic Random Bit Generator - NIST certification numbers 535 & 542 – NIST 800-90A
CRI DPA Countermeasures Validation Program

BST M12t is undergoing the following accreditation:

ISO13491 (Secure crypto device for retail)
PCI PTS (Payment Card Industry Pin Transaction Security Standard)
INTERNATIONAL COMMON CRITERIA
FIPS140-2 LEVEL 3 (Q2 2019)
CITA (Q1 2019)
Achilles Level 3 (Q3 2019)

In addition to the above standards, BST modules have patents-pending in Quantum Anti-Tamper, Quantum Random Bit Generation and Quantum Physically Uncloneable Functions. These are in the process of being developed and will be accredited in due course.

## Proposed Code of Practice for Security in Consumer IoT Products and Associated Services

This Code of Practice is designed to improve the security of consumer IoT products and associated services. Many severe cyber security issues stem from poor security design and bad practice in products sold to consumers.

The guidance is listed in order of importance and the top three should be addressed as a matter of priority. An indication is given as to which stakeholder the responsibility primarily rests upon. These stakeholders are defined as:

**Device Manufacturer**: The entity that creates an assembled final internet-connected product. A final product may contain the products of many other different manufacturers.
**IoT Service Providers**: Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.

**Mobile Application Developers**: Entities that develop and provide applications which run on mobile devices. These are often offered as a way of interacting with devices as part of an IoT solution.
**Retailers**: The sellers of internet-connected products and associated services to consumers.

### 1) No default passwords

*All IoT device passwords must be unique and not resettable to any universal factory default value.*

Many IoT devices are being sold with universal default usernames and passwords (such as “admin, admin”) which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed. Further details are available on the NCSC website.

Primarily applies to: Device Manufacturers

### 2) Implement a vulnerability disclosure policy

*All companies that provide internet-connected devices and services must provide a public point of contact as part of a vulnerability disclosure policy in order that* *security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.*

Knowing about a security vulnerability allows companies to respond. Companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle. Reports of vulnerabilities can be sent to: security@ncsc.gov.uk. Companies are also encouraged to share information with competent industry bodies.[26]

Primarily applies to: Device Manufacturers, IoT Service Providers and Mobile Application Developers

### 3) Keep software updated

*All software components in internet-connected devices should be securely updateable. Updates must be timely and not impact on the functioning of the device. An end-of-life policy must be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons why. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.*

Software updates should be provided after the sale of a device and pushed to devices for a period appropriate to the device. This period of software update support must be made clear to a consumer when purchasing the product. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear.

Primarily applies to: Device Manufacturers, IoT Service Providers and Mobile Application Developers

### 4) Securely store credentials and security-sensitive data

*Any credentials must be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.*

Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be stored securely includes, for example, cryptographic keys and initialisation vectors. Secure, trusted storage mechanisms should be used such as those provided by a Trusted Execution

Environment and associated trusted, secure storage. Stored credentials in services should follow best practices.

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers

### 5) Communicate securely

*Security-sensitive data, including any remote management and control, should be encrypted when transiting the internet, appropriate to the properties of the technology and usage. All keys should be managed securely.*

The use of open, peer-reviewed internet standards is strongly encouraged.

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers

### 6) Minimise exposed attack surfaces

*All devices and services should operate on the "principle of least privilege"; unused ports must be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.*

The principle of least privilege is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

Primarily applies to: Device Manufacturers, IoT Service Providers

### 7) Ensure software integrity

*Software on IoT devices must be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.*

Primarily applies to: Device Manufacturers

### 8) Ensure that personal data is protected

*Where devices and/or services process personal data, they should do so in accordance with data protection law. Device manufacturers and IoT service providers must provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this must be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time. Consumers should also be provided with guidance on how to securely set up their device, as well as how they may eventually securely dispose of it.*

This ensures that IoT manufacturers, service providers and application developers adhere to data protection obligations when developing products and services; that personal data is processed in accordance with data protection law; that users are assisted in assuring that the data processing operations of their products are consistent and that they are functioning as specified; and that users are provided with means to preserve their privacy by configuring device and service functionality appropriately.

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers, Retailers

### 9) Make systems resilient to outages

*Resilience must be built in to IoT services where required by the usage or other relying systems, such that the IoT services remain operating and functional.*

IoT systems and devices are relied upon by consumers for increasingly important use cases that may be safety relevant or life-impacting. This may include building redundancy into services as well as mitigations against DDoS attacks.

Primarily applies to: Device Manufacturers, IoT Service Providers

### 10) Monitor system telemetry data

*If collected, all telemetry such as usage and measurement data from IoT devices and services should be monitored for security anomalies within it.*

Any unusual circumstances can be identified early and dealt with, minimising security risk and allowing quick mitigation of problems that do emerge.

Primarily applies to: IoT Service Providers

### 11) Make it easy for consumers to delete personal data

*Devices and services should be configured such that personal data can easily be removed when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.*

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers

### 12) Make installation and maintenance of devices easy

*Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability.*

This is in order to prevent security issues caused by consumer confusion or misconfiguration, sometimes caused by complexity and poor or unclear design in user interfaces.

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers

### 13) Validate input data

*Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices must be validated.*

This ensures that systems are not easily subverted by incorrectly formatted data or code.

Primarily Applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers