TrustIoT Framework for Industry 4.0

"Secure Boot: Cryptographic verification of firmware"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *TrustIoT Framework for Industry 4.0* |
| Version: | *1* |
| Document Author: | *Jibran Saleem* |
| Document Owner: |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

Table of Contents

[1. Introduction 4](#_Toc176332199)

[2. Purpose 4](#_Toc176332200)

[3. Scope 4](#_Toc176332201)

[4. Policy Statement 4](#_Toc176332202)

[4.1. Secure Boot Process 4](#_Toc176332203)

[4.2. Firmware Verification 4](#_Toc176332204)

[4.3. Key Management 4](#_Toc176332205)

[4.4. Secure Storage 5](#_Toc176332206)

[5. Responsibilities 5](#_Toc176332207)

[6. Breaches of Policy 5](#_Toc176332208)

[7. Document Management 5](#_Toc176332209)

# Introduction

The firmware embedded within IoT devices serves as the foundational software layer, governing their operation and behaviour. Ensuring the integrity and authenticity of this firmware is paramount to prevent unauthorised modifications, malware infections, and other cyber threats that can compromise the device's functionality, data confidentiality, and overall system security. Secure Boot mechanisms, employing cryptographic verification, provide a robust defence against such threats by ensuring that only trusted and validated firmware is executed on IoT devices.

# Purpose

The purpose of this policy is to establish stringent guidelines and requirements for the implementation and management of Secure Boot mechanisms on IoT devices within the organisation. This policy aims to:

* Prevent the execution of unauthorised or malicious firmware on IoT devices.
* Protect the integrity of the boot process and critical system components.
* Mitigate the risk of supply chain attacks and firmware tampering.
* Ensure the trustworthiness and reliability of IoT devices throughout their lifecycle.

# Scope

This policy applies to all IoT devices within the organisation that utilise firmware, including but not limited to:

* Sensors, actuators, and controllers
* Gateways and edge devices
* Industrial control systems (ICS)
* Wearable and embedded devices

# Policy Statement

## Secure Boot Process

* **Chain of Trust:** A hardware-based root of trust shall be established to anchor the chain of trust for firmware verification.
* **Bootloader Protection:** The bootloader, responsible for initiating the boot process, shall be protected against unauthorised modification or replacement.
* **Measured Boot:** A measured boot process shall be implemented to record the cryptographic hashes of each firmware component loaded during startup.
* **Secure Storage:** The measurements collected during the boot process shall be securely stored in tamper-proof hardware or a trusted execution environment.

## Firmware Verification

* **Digital Signatures:** Firmware images shall be digitally signed by authorised parties using strong cryptographic algorithms and private keys.
* **Signature Verification:** IoT devices shall verify the digital signatures of firmware images before loading and executing them.
* **Secure Key Storage:** Private keys used for firmware signing shall be stored and managed securely to prevent unauthorised access or compromise.

## Key Management

* **Key Generation and Protection:** Robust key management practices shall be implemented for the generation, distribution, storage, and rotation of cryptographic keys used in the secure boot process.
* **Hardware Security Modules (HSMs):** Where feasible, HSMs shall be utilised for the secure generation and storage of cryptographic keys.

## Secure Storage

* **Firmware Storage:** Firmware images shall be stored in secure repositories with access controls to prevent unauthorised modification or distribution.
* **Secure Update Mechanisms:** Secure update mechanisms shall be employed to ensure the integrity and authenticity of firmware updates during transmission and installation.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for configuring and managing secure boot mechanisms, firmware updates, and key management processes.
* **Device Manufacturers/Vendors:** Responsible for implementing secure boot capabilities and providing signed firmware updates.
* **Users:** Responsible for reporting any security incidents or concerns related to IoT devices.

# Breaches of Policy

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships.

# Document Management

This document is valid as of [dd/mm/yyyy].

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

* Compliant with the Internet of Things (IoT) Security Framework for Industry 4.0.
* Legislative requirements defined by law, where appropriate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name 1]

Manager