Version 1: March 2022

Essential Properties of Secure Connected Devices

PSA Certified's 10 Security Goals and Microsoft's Seven Properties of Highly Secured Devices

Rob Smart, Senior Principal Security Architect, Arm (a PSA Certified Co-founder)
with contributions from Microsoft

This document was written by PSA Certified and Microsoft to illustrate the common objectives of the PSA Certified 10 Security Goals and the Microsoft's Seven Properties of Highly Secured Devices. It is well suited to people looking to understand, at a high-level, what is necessary for a connected device to be secure, based on expertise from two key industry players. Key things we will cover are:

- The perspectives and motivation of Microsoft and PSA Certified to identify the foundational security requirements.
- An overview of Microsoft's Seven Properties of Highly Secured Devices and the PSA Certified 10 Security Goals.
- How the seemingly different sets of properties and goals, in fact have a great deal in common.

psacertified™

Microsoft Azure

We enter the era of digital transformation in which nearly every industry is embracing technologies that make new efficiencies, products, and services possible at a scale never seen before. At the heart of this digital transformation is the ability to connect devices, collect and interpret data, and deliver intelligent business or service insights. However, insufficient investments in securing the devices that underpin the fundamental value for businesses have left both consumers and enterprises exposed to severe security risks.

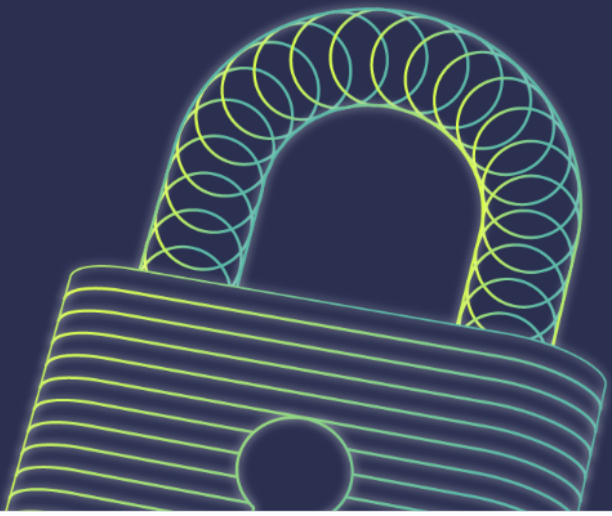
Ultimately, digital transformation will be powered by data: authentic, trustworthy data is more important than ever. The small quantities of data collected from every sensor and actuator must be trustworthy as it cumulatively becomes the big data driving the new transformational digital services at scale. Trusted data and trusted services can only be truly possible and achieve scale if they are generated by devices built with sound security principles.

As IoT started to grow, Arm and leading security evaluation laboratories spearheaded PSA Certified [1], a partnership that set out to establish baseline security requirements with the ecosystem. This was based on the PSA Certified 10 Security Goals that every connected device should meet before interacting with the Internet. These can be realized with the inclusion of a Root of Trust (RoT) and they motivated the definition of the PSA-RoT. The goals are a high-level abstraction derived from long-established Arm experience in securing devices, and from specific threat modeling and security analysis for common connected device use cases.

At the same time, Microsoft had observed that high development costs and maintenance often limited the adoption of strong security in the connected devices ecosystem. Every single device, be it a connected thermostat or equipment connected on a factory floor, is a potential target for an attack and therefore necessitates high-integrity security. Through extensive research and testing, Microsoft identified seven properties that should at a minimum be present in all devices considered to be highly secured. The results of that research is documented in The Seven Properties of Highly Secured Devices paper [2].

Both the PSA Certified 10 Security Goals and the Microsoft Seven Properties aim to advance the adoption of foundational security in the IoT device ecosystem. In this white paper, we provide a description of both with material from both PSA Certified and the Seven Properties of Highly Secured Device paper, to present a high-level comparison and our perspectives on their similarities and differences.

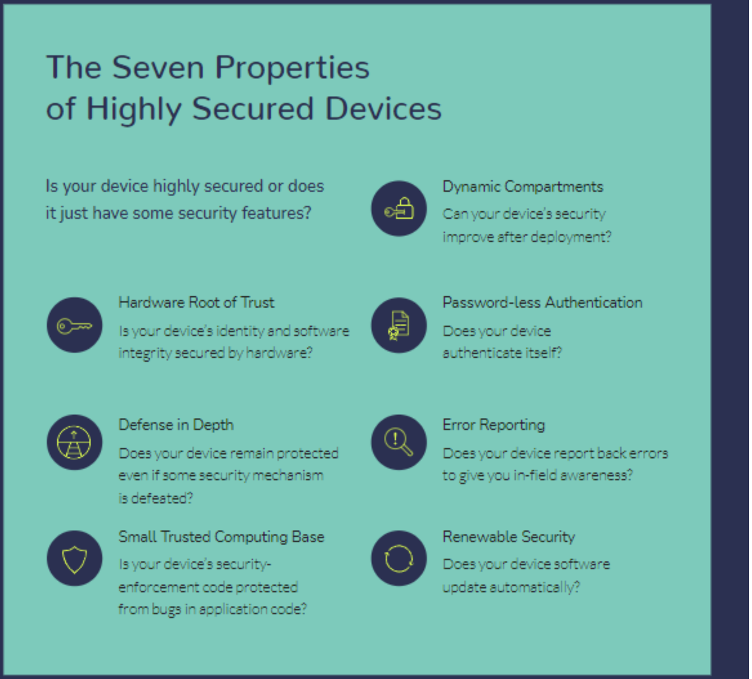
Ultimately, the call-to-action is simple: security is everyone's responsibility, and we need to rally together to advance the security of the IoT.



What are the Microsoft Seven Properties of Highly Secured Devices?

The following excerpts from The Seven Properties of Highly Secured Devices (2nd Edition), © 2020 Microsoft Corporation, and references to it used throughout the remainder of this paper, are used with permission. These excerpts are provided "as-is." The information and views expressed in these excerpts, including URL and other internet website references may change without notice. You bear the risk of using it. Some examples may be for illustration only and are fictitious. No real association is intended or inferred. This document does not provide you with any legal rights to any intellectual property in any Microsoft product.

Microsoft conducted extensive research and testing to understand the baseline requirements for security in connected devices. The resulting evidence informed the paper "The Seven Properties of Highly Secured Devices." That paper details the seven properties found in every device considered to be highly secured, forming a foundation of security upon which additional security measures are often added. These seven properties should be considered a required baseline for security in every connected device. For any property that is missing, other practices would need to be implemented by the owner or customer to compensate. For example, a security incident might make it necessary to disconnect devices and recall or manually patch them without renewable security [3].



The Seven Properties of Highly Secured Devices

Is your device highly secured or does it just have some security features?

Dynamic Compartments
Can your device's security improve after deployment?

Hardware Root of Trust
Is your device's identity and software integrity secured by hardware?

Password-less Authentication
Does your device authenticate itself?

Defense in Depth
Does your device remain protected even if some security mechanism is defeated?

Error Reporting
Does your device report back errors to give you in-field awareness?

Small Trusted Computing Base
Is your device's security-enforcement code protected from bugs in application code?

Renewable Security
Does your device software update automatically?

aka.ms/7properties

Highly secured devices have a *hardware root of trust.*

A device's private identity keys are protected by hardware, the integrity of device software is validated by hardware, and the hardware contains physical countermeasures against side-channel attacks. Unlike software, hardware has two important properties needed as foundation for device security. First, single-purpose hardware is resistant to reuse by an attacker for unintended actions. Second, hardware can detect and mitigate against physical attacks; for example, pulse testing the reset pin to prevent glitching attacks is easily implemented in hardware. When used to protect secrets and integrity, hardware provides a solid root of trust upon which rich software functionality can be implemented securely and safely.

Highly secured devices have *defense in depth.*

In highly secured devices, multiple mitigations are applied to each class of threat. In devices with only a single layer of defense, such as most RTOS-based devices, even a single error in design or implementation is sufficient to lead to catastrophic compromise. Because new threats are often completely unanticipated, in practice, having multiple countermeasures often becomes the difference between a secured device and compromised device.

Highly secured devices have a *small trusted computing base.*

A trusted computing base (TCB) is "a small amount of software and hardware that security depends on and that we distinguish from a much larger amount of software that can misbehave without affecting security". Within a device, the TCB for different operations with may differ. For example, the TCB for securing data at rest may include the hardware root of trust, software for encryption and decryption, and software for sealing and unsealing crypto keys. On the other hand, the TCB for secure communication might also include an TLS implementation. The TCB for any operation should be kept as small as possible to minimize the surface that is exposed to attackers and to reduce the possibility that a bug or feature can be repurposed to circumvent security protections. The TCB code should be protected from non-critical device code to ensure its correct operation even if the other code is compromised. Less secured devices often have no isolated TCB - security code in these devices executes in the same compartment as the rest of the device code with the result that just one bug, anywhere in the device's code, can lead to a catastrophic full-system compromise.