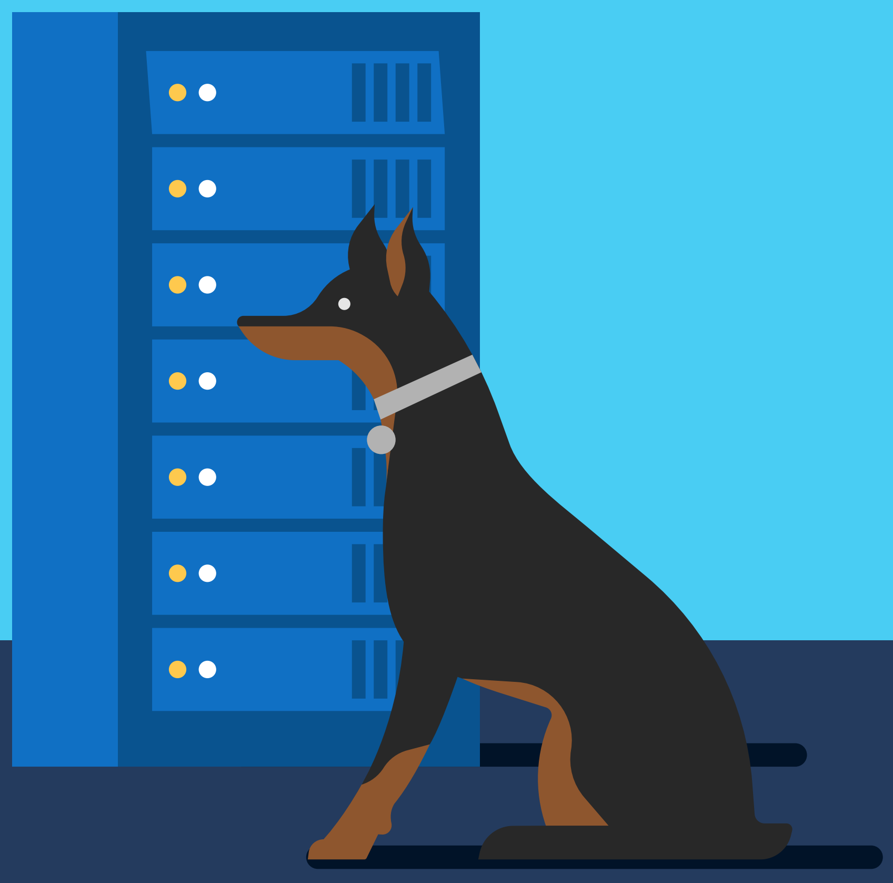
4 Types of secure hardware for IoT devices



There are various classes of secure hardware, with each one appealing to a particular device segment. However, this abundance of variations has presented multiple challenges, such as the lack of interoperability. To solve this issue, hardware standards have been developed around usage protocols and application classes.

The following are 4 protocols commonly used to protect today’s devices:

Device Identifier Composition Engine (DICE)

A class of secure hardware based on a set of security protocols standard by the **Trusted Computing Group** (TCG). **DICE** aims to solve the problem of security and privacy in the resource constraint devices that are prevalent in **IoT** and is most optimal for a standalone hardware architecture.

Trusted Platform Module (TPM)

A class of secure hardware based on a set of security protocols standard also by the **TCG.** The **TPM** protocol enables remotely connected systems to establish trust and communicate securely and **TPM** devices are also optimal for a standalone hardware architecture.

Secure Smartcard Modules

A class of secure hardware commonly governed by several de jure standards that specify attributes like form factor and communications protocol, but not security. They are commonly used in **kiosk-type IoT** systems that require removable cryptographic modules and are optimal for a standalone hardware architecture.

Hardware Secure Modules (HSM)

In the context of **IoT, HSM** is a catch-all for any secure hardware that does not adhere to a specific security protocol. These are sometimes optimized for specific applications or use-cases, such as certificate processing or secure token generation and are optimal for integrated secure hardware architecture.

To learn more about these and other types of secure hardware standards, download our Secure Hardware for IoT Deployment whitepaper.

Microsoft