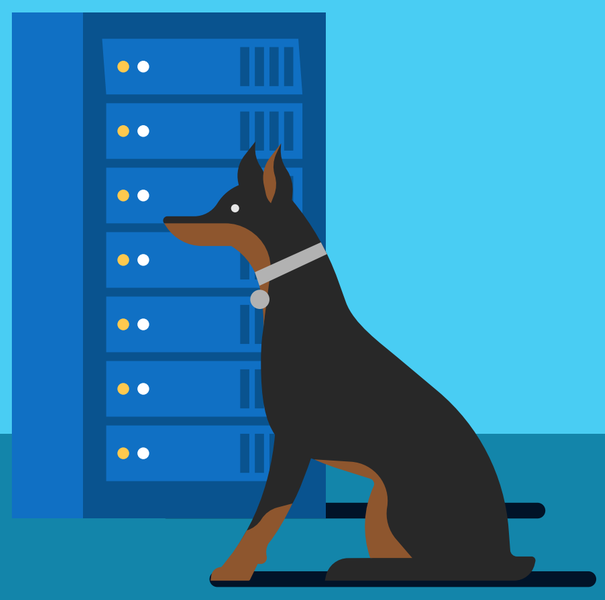
4 TYPES OF SECURE HARDWARE FOR IoT DEVICES



There are many classes of secure hardware, each one designed for a particular device segment. This, however, has created challenges such as a lack of interoperability between devices. Therefore, hardware standards were developed around usage protocols and application classes to solve this issue.

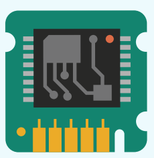
These are 4 protocols commonly used to protect today's devices:

Device Identifier Composition Engine (DICE)

DICE aims to solve the problem of security and privacy in the resource constraint devices that are prevalent in IoT.

Trusted Platform Module (TPM)

This protocol enables remotely connected systems to establish trust and communicate securely.



Secure Smartcard Modules

Commonly used in kiosk-type IoT systems that require removable cryptographic modules.

Hardware Secure Modules (HSM)

HSM are optimized for specific applications or use-cases, such as certificate processing or secure token generation.

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

Microsoft