Simplifying Security for OEMs
A Four Step Framework

psacertified™

PSA Certified is the first complete security framework, open source firmware project and matching certification scheme designed to dramatically reduce the labor, guesswork and other challenges associated with designing security into IoT devices. It gives clarity to a fragmented, fast-moving market, and provides a foundation of trust for next-generation IoT devices.

PSA Certified consists of a four step program that guides OEMs through the security design and development process.

1
Analyze
Understand the Level of Security Needed

Define and create list of security requirements through a comprehensive analysis of use case threats and vulnerabilities, and match them to a list of security best practices.

PSA Certified offers:
- A Security Model document which outlines the 10 security goals and how to achieve them.
- Example threat model and security analysis documents to guide this process.

2
Architect
Plan What Security You Will Implement and How

Leverage best practices and specifications to build a blueprint of the required security architecture or select PSA Certified chips and RTOSes from the list of ready-Certified products.

PSA Certified offers:
- A simple way to identify the right component for your device on the PSA Certified products page.
- Specifications outlining hardware and firmware security architectures that comply with the 10 security goals.
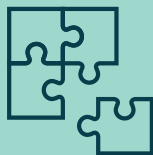
3
Implement
Build or Integrate Your Solution

Implement PSA Certified components or security design into your device and use application software and APIs to ensure communication with underlying security features within the silicon.

PSA Certified offers:
- A reference implementation of the PSA Root of Trust containing key security functions for silicon security.
- Free and open high-level APIs that provide an easy-to-use interface with the security functions in the PSA Root of Trust.

4
Certify
Evaluate and Certify Product Security

Test security implementations to be sure you're meeting all use case-based security robustness requirements.

PSA Certified offers:
- Independent security evaluation for connected devices to ensure adherence to security best practice and alignment to global regulations.
- Multi-level silicon security assessment so the right level of chip security can be selected for use in devices.
- A PSA Certified certificate and logo, providing a quality marker showing security commitment.

Adherence to the PSA Certified framework embeds security into the heart of your product and can protect your brand, bolster revenue, enhance your reputation and even act as a key selling point. With considerable industry support behind it, PSA Certified is quickly becoming the de facto standard for IoT device security.

Find out more at psacertified.org