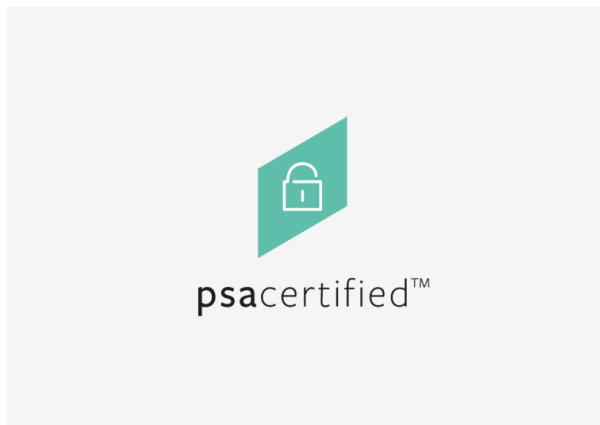# PSA Certified Security Evaluations

While IoT solutions are getting traction, most cybersecurity regulations are still in development or at the first implementation stages. PSA Certified offers an industry-led framework and certification scheme, based on an expert laboratory evaluation approach and aligned with other standards and regulations.

PSA Certified has a tiered model of assurance, which goes from ensuring good practices have been followed to deep evaluations with state-of-the-art software and hardware attacks.

PSA Certified helps device manufacturers to choose the appropriate level of security assurance and robustness for their product (including its chip and software), according to their market needs and its use case.

Applus+ Laboratories is a [member of PSA Certified](#), and an accredited lab for evaluating IoT products to get PSA Certified. We can provide services for the different levels to device manufacturers, software developers and silicon vendors.

PSA Certified Level 1 for device, software, and chip vendors

- **Demonstrates that good security principles** have been applied.
- **Based on an independent security assessment** that reviews security implementations.

- **Helps reduce fragmentation** by aligning with major global guidelines and legislations. PSA provides a mapping between its L1 certification and the requirements of other standards such as ETSI EN 303 645, NIST 8259A, and Californian State Law SB-327, Matter and ioXt.
- **Reuse Certifications for Market-Specific Standards**: PSA Certified Level 1 certification can be reused in other industry certification schemes, enabling alignment with end market and vertical applications. IoXt Alliance and UL recognize PSA Root of Trust as a way to obtain a fast-tracked certification

---

PSA Certified Level 2 for chip vendors

- Uses **independent testing** to show that their **PSA Root of Trust (PSA-RoT) security** component can protect against scalable, remote software attacks
- **Provides security assurance** suitable for many mass-market IoT solutions, backed by an independent laboratory evaluation.
- **Evaluation takes less time** (and has a lower cost) than PSA Certified Level 3, a factor that may be key in the product development schedule.

PSA Certified Level 2 + Secure Element for Chip Vendors

- An augmented version of Level 2, with additional recognition for the solution that has substantial physical protection for the cryptographic keys and cryptographic operations.

PSA Certified Level 3 is for chip vendors

- Provide evidence that the **PSA-RoT** protects against substantial hardware and software attacks.

- This higher level is aimed at **IoT solutions that must protect high-value assets;** solutions particularly susceptible to attack due to potential economic gain or brand damage; solutions that are physically accessible and thus require protection against hardware attacks.
- Our laboratory will conduct a white-box evaluation that includes vulnerability analysis and pentesting.
- **Protection Profile:** PSA-RoT Level 3 Protection Profile or PSA-RoT Level 3 SESIP Profile.

PSA Certified Level 3 + Secure Element for Chip Vendors

- An augmented version of Level 3, with additional recognition for the solution that has substantial physical protection for the cryptographic keys and cryptographic operations.

PSA Certified Level 4 for ISE/ES Chip vendors

- **Enhanced Resilience**: Products certified at Level 4 are designed to withstand even higher potential attackers and threats compared to Level 3, making them suitable for protecting extremely sensitive assets or facing sophisticated adversaries.
- **High Assurance Evaluations**: Evaluations for Level 4 certifications are conducted by high assurance evaluation laboratories, like Applus+. We employ rigorous testing methodologies and state-of-the-art equipment testing benches to assess the security robustness of the products.
- **Comprehensive Testing**: The evaluation process includes comprehensive testing scenarios to ensure the products' resilience against both hardware and software attacks. This may involve white-box evaluations, vulnerability analysis, penetration testing, and other advanced testing techniques.
- **Industry Recognition**: Level 4 certification signifies the highest level of security assurance within the PSA Certified framework. It demonstrates a product's capability to provide top-tier security for critical applications and environments.