PSA认证安全评估

虽然物联网解决方案越来越受欢迎，但大多数网络安全法规仍处于制定或实施初期。PSA认证提供行业领先的框架和认证计划，以专家实验室评估方法为基础，并与其他标准和法规保持一致。

PSA认证采用分层保障模式，从确保遵循良好实践到使用最先进的软件和硬件攻击进行深入评估。

PSA认证帮助设备制造商根据市场需求和用例，为其产品（包括芯片和软件）选择适当的安全保证和稳健性级别。

Applus+ Laboratories是PSA认证的成员，也是获得PSA认证的物联网产品评估认证实验室。我们可以为设备制造商、软件开发商和芯片供应商提供不同级别的认证服务。

PSA认证1级认证，适用于设备、软件和芯片供应商

- **表明已应用了良好的安全原则。**
- **基于独立的安全评估**，审查安全实施情况。
- **通过与全球主要准则和法规保持一致**，有助于减少碎片化。 PSA在其L1认证与其他标准（如ETSI EN 303 645、NIST 8259A和加利福尼亚州法律SB-327、Matter和ioXt）的要求之间建立了映射关系。

- **重复使用特定市场标准的认证**：PSA认证1级认证可以重复用于其他行业认证方案，从而与终端市场和垂直应用保持一致。IoXt联盟和UL认可PSA信任根（PSA Root of Trust）作为获得快速认证的一种方式

芯片供应商的PSA认证2级

- 通过**独立测试**证明其**PSA信任根（PSA-RoT）安全组件**能够抵御可扩展的远程软件攻击
- **提供安全保证**，适用于众多大众市场物联网解决方案，并得到独立实验室评估的支持。
- **评估所需时间（和成本）比PSA认证3级少**，这一点对于产品开发进度至关重要。

PSA认证2级+芯片供应商安全元件

- 2级的增强版，额外认可为加密密钥和加密操作提供实质性物理保护的解决方案。

PSA认证3级适用于芯片供应商

- 提供证据证明**PSA-RoT**能够抵御实质性的硬件和软件攻击。
- 这一更高等级认证针对的是**物联网解决方案，这些解决方案必须能够保护高价值资产**；由于潜在的经济利益或品牌损害，这些解决方案特别容易受到攻击；这些解决方案可以被物理访问，因此需要防止其被硬件攻击。
- 我们的实验室将进行白盒评估，包括漏洞分析和渗透测试。
- **保护配置文件：**PSA-RoT 3级保护配置文件或PSA-RoT 3级SESIP配置文件。

PSA认证3级+芯片供应商安全元件

- 3级的增强版，额外认可对加密密钥和加密操作提供实质性物理保护的解决方案。

PSA认证4级，适用于ISE/ES芯片供应商

- **增强的恢复能力**：与3级认证相比，4级认证的产品能够抵御更高级别的潜在攻击和威胁，适用于保护极其敏感的资产或应对老练的对手。
- **高保障评估**：4级认证的评估由高保障评估实验室（如Applus+）进行。我们采用严格的测试方法和最先进的设备测试台来评估产品的安全稳健性。
- **全面测试**：评估过程包括全面的测试方案，以确保产品能够抵御硬件和软件攻击。这可能涉及白盒评估、漏洞分析、渗透测试和其他先进的测试技术。
- **行业认可**：4级认证是PSA认证框架内最高级别的安全保证。它表明产品能够为关键应用和环境提供顶级安全保护。