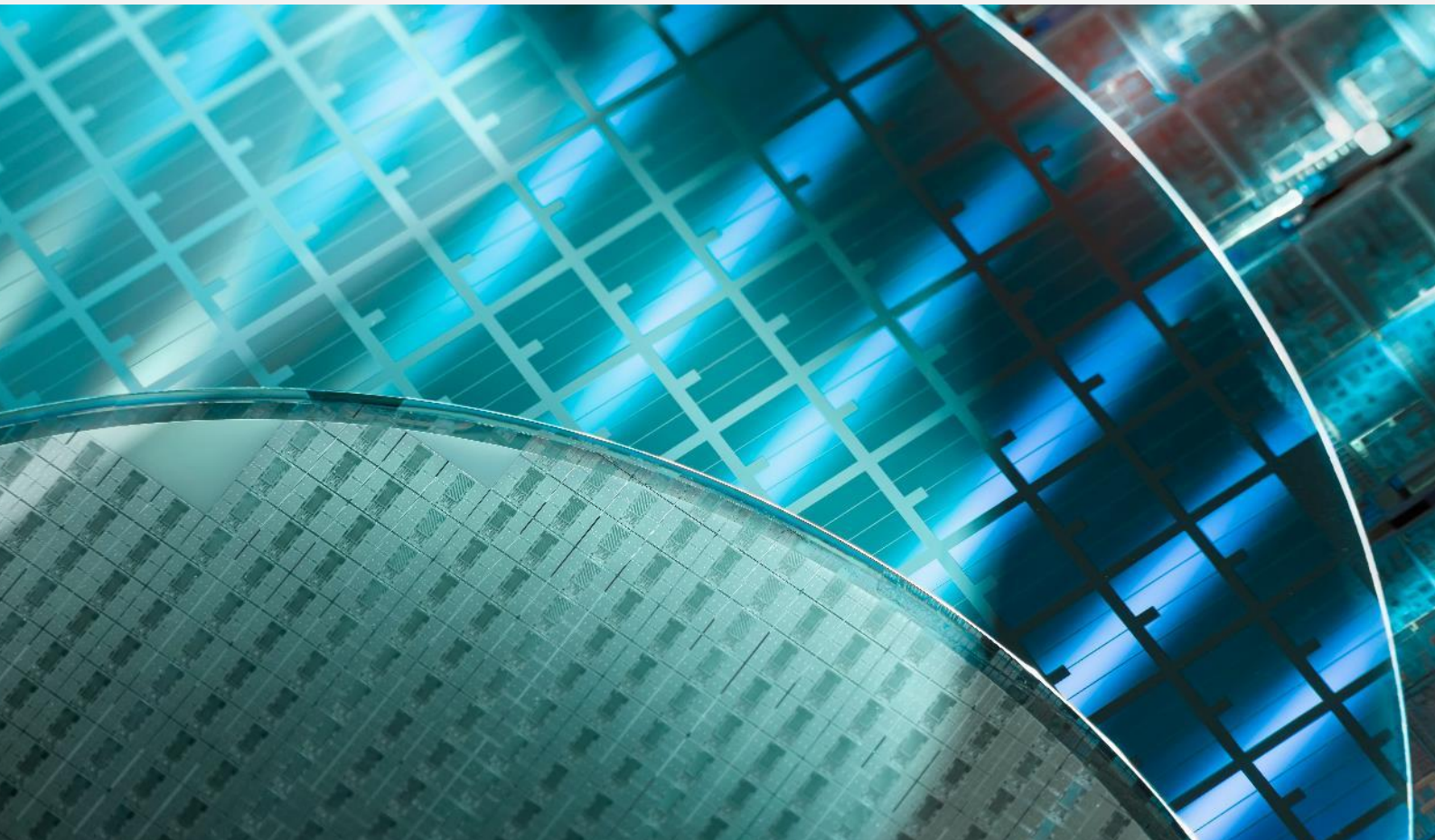
PSA-Certified 认证的加密协处理器 -- 为 Arm 生态系提供完整安全防护

Whitepaper

Lawrence Liu (刘持志)
Dr. Evans Yang (杨青松)
Stephanie Smith

March 2023



芯片到系统的安全性

在过去的五年里，Arm 通过安全宣言重申了保护其架构安全的承诺。 它为半导体行业做了明确的宣示。在面对当今计算所面临的日益严峻的威胁时，单依靠软件防护只能在一定程度上缓解漏洞，因此，需要硬件解决方案为设备奠定坚实的基础，支持整体系统安全运行。

现实情况是，电子设备需要一个全面的安全生态系统来提供协作和分层的解决方案。 从物联网、人工智能，到移动设备，几乎没有一个计算过程不涉及 Arm 架构。 他们也因此号召合作伙伴一起推动“强化芯片到系统的安全性”，并为硬件级别提供全面的保护。

Standardizing IoT Security with PSA Certified
PSA Certified 建立物联网安全标准

由于物联网的成长太过快速，使得该相应落实的安全性标准订定工作相对落后，这促使 Arm 在 2019 年与合作伙伴率先提出了 PSA 认证。他们的目标是提倡将物联网安全主动纳入芯片设计考虑，以保护物联网设备免受侵害及恶意攻击。凭借一套强大的通用标准，PSA Certified，有助于改善各种物联网设备、应用程序和解决方案提供商之间安全协议的碎片化。

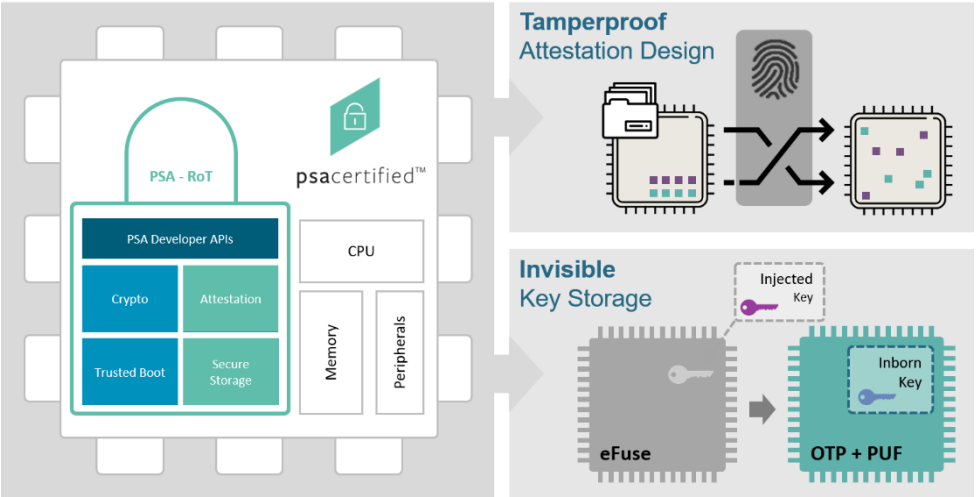


图1：PSA Certified 對物联网信任根的标准要求

PSA Certified 通过与第三方实验室合作，来检验设计的安全性，並推广可广泛通用的基础安全功能。此举不仅是为了减轻终端设备使用者对隐私侵犯的担忧，更是为了解决供应商近在眼前的挑战--各国政府即将推出的物联网安全要求。 由于存在各种类型的物联网产品，因此 PSA 认证计划也提供不同级别的认证。 其中包括 PSA Certified Level 1、PSA Certified Level 2、PSA Certified Level 2 Ready 和 PSA Certified Level 3。这样的安全级别分级反映了 “物联网安全没有一刀切的解决方案” 的现实。

PSA Certified Level 1 提供厂商以调查问卷的方式完成第三方实验室的审核，但未进行实验室内的实际测试。 厂商并应证明該送審的物联网芯片/设备/软件设计遵循了物联网威胁模型、PSA Certified 的 10 个安全目标以及全球政府指南要求的最佳安全实践。

PSA Certified Level 2 和 PSA Certified Level 3 认证旨在衡量安全稳健性，故需要在实验室中进行测试。测试内容包括使用选定的一系列纯软件攻击，PSA Certified Level 3 则还需通过物理渗透评估（包括侧通道分析）。基于对硬件安全的关注，PSA Certified Level 2 和 PSA Certified Level 3 认证要求评估目标（TOE）必须有信任根（RoT）并满足九项安全功能要求才能获得认证。 这些功能包括：

1. Initialization 安全启动
2. Software Isolation 软件隔离
3. Secure Storage 安全存储
4. Firmware Update 固件更新
5. Secure State 安全状态
6. Cryptography 算法
7. Attestation 验证
8. Audit / Debug 审核/除错
9. Physical 物理防护

注意到这九个功能与 1 级认证中八个要求之间的重叠，因为安全硬件信任根 (HRoT) 自然必须遵循最佳安全实践。

PSA Certified Level 2 Ready 可以被视为帮助公司获得 PSA Certified Level 2 和 PSA Certified Level 3 的基石。随着科技的演进，现代化芯片设计变得越来越复杂，当今产品设计可能会包含来自第三方专家的一个或多个 IP。这导致所需的人力资源和预算紧张，整体产品开发时间也缩短了。采用通

过 PSA Certified Level 2 Ready 的 IP 对产品提供了安全的保障，且有助于缩短最终产品设计通过安全认证所需的时间。

获得 PSA Certified Level 2 Ready 认证的加密协处理器

熵码科技的 PUFcc 加密协处理器就是通过 PSA Certified Level 2 Ready 的例子。

PUFcc 将硬件信任根(PUF、Secure OTP 、TRNG)与全套加密加速器相结合，形成一个兼容性极强的安全 IP 模块，可轻松集成到各种系统架构中。这种“现成的”解决方案使设计人员能够“即插即用”，轻松实现系统所需的安全协议。

PUFcc 可以安全地执行高机敏的工作，这些机要操作在执行上与非机敏功能（通常由主系统负责）以硬件隔离的方式分开，改在以防篡改设计保护的安全边界内执行。 此外，PUFcc 是一个通用的集成安全 IP 模块，支持所有常见的密码算法，允许使用者构建各种安全协议。

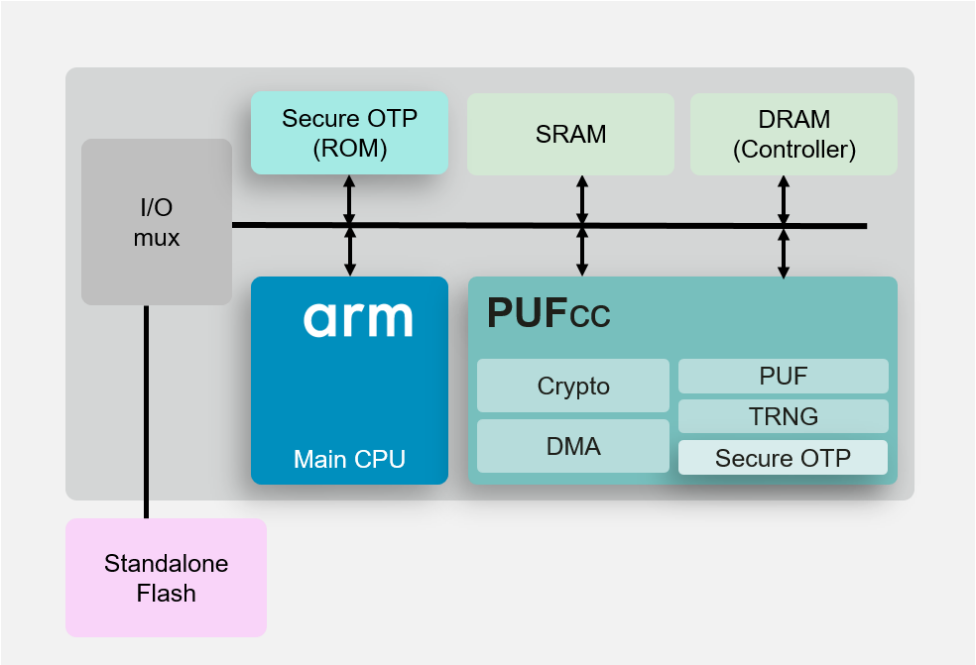


图 2：PUFcc 的典型集成图

PUFcc 作为加密协处理器并在安全边界内执行各项的操作，其设计必须能让系统无条件地信任。PUFcc 的任务是保障整体系统安全性，特别是当无法确保 PUFcc 安全边界之外的组件，例如系统内存、总线和共享系统总线的其他设备等，是100%安全的情况下。上述这些组件都是黑客为了获得系统访问或控制权、常见的攻击目标。

熵码科技已为 PUFcc 完成 PSA Certified Level 2 Ready 的认证，确保 PUFcc 能够满足可信任和隔离子系统的安全要求。具体地说，PUFcc 通过了安全启动、安全存储、固件更新、安全状态和加密算法的测试，是硅智财所能通过的所有项目。

加密协处理器中的信任根功能

安全启动意味着评估目标需要确保只有授权的软件才能在设备上执行。PUFcc 通过使用可信固件 M (TF-M) 包中的 MCUboot 引导加载程序(boot loader)，在安全启动(secure boot)流程中验证经签署的启动代码(boot code)来实现此目的。 值得关注的是，PUFcc 是通过内部生成了用于此安全启动的硬件密钥而节省了外部生成密钥与注入的各项成本。

安全存储可防止私人数据被克隆或从设备中窃取。 PUFcc 通过基于关联数据认证加密（AEAD）安全数据策略的 AES（GCM 模式）实现安全存储，保护私有系统数据的完整性和真实性。 用于此安全数据策略的密钥源自硬件唯一密钥 (HUK)，只有 PUFcc 才能访问该密钥，该密钥源自芯片内置的物理不可克隆功能 (PUF)。 透过 PUF 能确保每个 PUFcc 的 HUK 都是唯一且完全随机的。

固件更新（或安全更新），与安全启动有间接关联，是设备允许进行的唯一授权更新。然而，更新后的固件的执行仍由安全启动（初始化）流程完成。PUFcc 通过限制对固件映像槽的写入权限来实现此目标，在安全更新过程中只允许写入经正确签名的固件映像。然后，在安全启动过程中，以最新的固件映像档执行启动，同时更新安全计数器至与固件的最新版本相匹配来防止任何对固件映像进行回复的动作。

安全状态将可信服务、低信任服务和不可信服务相互隔离。通过安全分区管理器（SPM），在 PSA 固件框架的一部分中，如果分区之间的隔离出现任何错误，将通过 panic (interrupt) call 终止该进程。PUFcc 以此建构了一个安全边界，将安全/非安全操作之间安全地隔离。

加密功能支持着关键的系统安全功能，例如安全生命周期、隔离、安全存储、安全验证、安全启动以及数据的安全加载和绑定。 PUFcc 支持全套加密算法，例如对称/非对称密码、HASH、MACs 和 AEAD，以满足各式密码安全功能要求。

由于 PUFcc 作为 IP，并非设计为独立产品，最多只能做到 PSA Certified Level 2 Ready 认证。要通过 PSA Certified Level 2 或 PSA Certified Level 3，取决于更大的集成系统来实施，以完整其他安全功能要求，包括软件隔离、验证、审核和除错。

CoreLink SSE-200 Integration

PUFcc 的 PSA Certified Level 2 Ready 认证是使用 Arm MPS3 评估板进行的。 Arm CoreLink SSE-200 子系统的 FPGA 实现（如应用笔记 AN524 中所述）与 PUFcc 以及 MPS3 板上的可信固件-M 端口集成。 CoreLink SSE-200 是适合用作 IoT SoC 基础的预组装组件（包括两个 Cortex-M33 内核）的集成，源自 Arm 系统 SIE-200 库。 Cortex-M33 内核的低功耗使得基于 CoreLink SSE-200 的系统成为边缘物联网应用的理想选择。

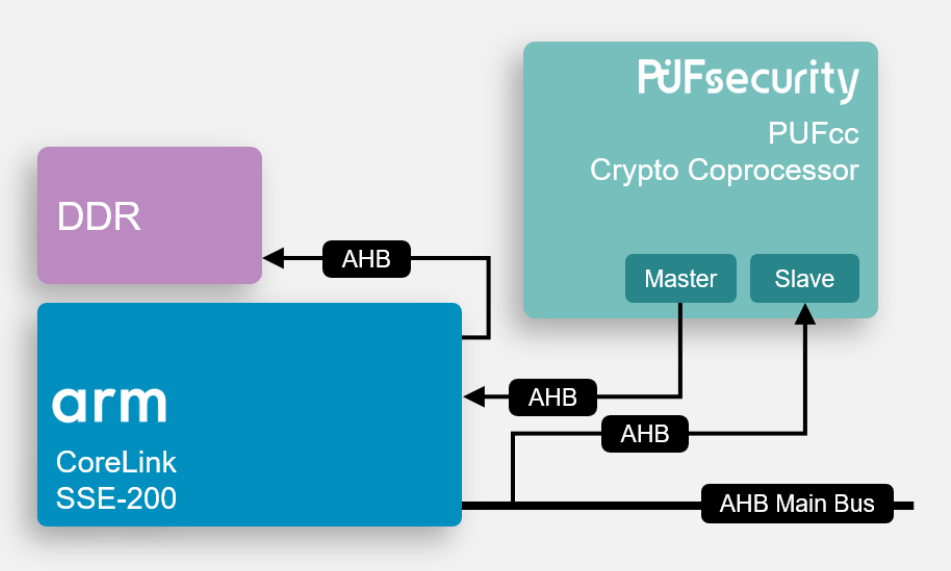


图 3：Arm SSE-200 子系统上的 PUFcc 集成

PUFcc 旨在提供构建 PSA-RoT 的原始元素，将唯一标识符 (PUF)、安全存储 (OTP)、TRNG 和加密引擎组合进一个支持加密操作的安全 IP 中。 因此，PUFcc 可以用作安全处理环境 (SPE) 内的外围设备。 由于加密密钥可以由信任根 (PUFcc) 本身在内部生成，因此避免了密钥泄漏的风险，从而可以将 PUFcc 视为在其自己的安全边界内。

为了与 CoreLink SSE-200 子系统集成，PUFcc 使用 AHB 和 APB 总线进行连接。 PUFcc 的 AHB 主机链接到 CoreLink SSE-200 安全管理控制器 (MSC)，以便根据 PUFcc 操作的需要向属性设置单元 (IDAU) 发送请求，例如通过 PUFcc 的直接内存访问模块 (DMA)访问的外部存储器。 APB 从属总线模块连接到 CoreLink 的外设保护控制器 (PPC)，以接收来自 CoreLink SSE-200 的安全和非安全请求，作为 “Expansion 1” 接口的一部分。

Corstone SSE-300 Integration

除了 CoreLink SSE-200 之外，此认证过程还使用具 Trusted Firmware-M 端口的同类型评估板 Arm MPS3 来演示 PUFcc 与 Corstone SSE-300 子系统的集成，如应用笔记 AN552（软核单元模型 – SM）。 AN552 具有一个带自定义数据路径扩展的 Cortex-M55 和一个 Ethos-U55 机器学习处理器。

与 CoreLink SSE-200 一样，Corstone SSE-300 是从 SIE-200 库中选择的预组装元素的集合（在本例中添加了 SIE-300 库）。凭借更强大的 Cortex-M55 内核，基于 Corstone SSE-300 的系统非常适合需要高性能的应用，如 AIoT。

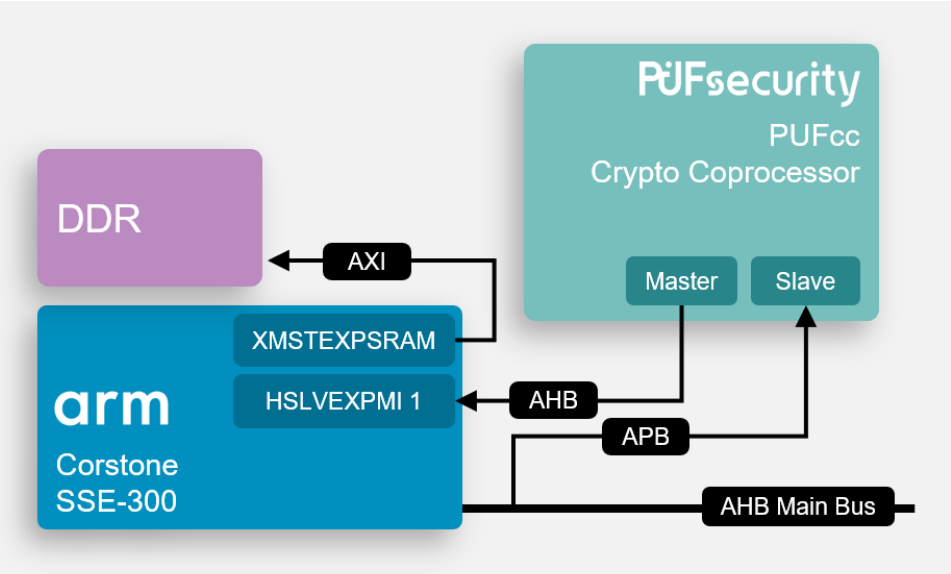


图 4：Arm Corstone SSE-300 子系统上的 PUFcc 集成

PUFcc 与 Corstone SSE-300 子系统的集成与 SSE-200 的情况非常相似，后者也使用 AHB 和 APB 总线。 PUFcc 的 AHB 主控再次连接到 CoreLink SSE-300 中位于从属主扩展接口 (HSLVEXPMI1)的安全管理控制器 (MSC)。 最后，APB 从属总线模块再次连接到 AN552 内存映射的非安全和安全外围区域中的 Corstone APB 外围保护控制器 (PPC)。

总结

Arm 的物联网整体解决方案是一项目光远大的计划，旨在推动物联网行业下一阶段的发展。PUFcc 是众多 PUFsecurity 解决方案中第一个获得 PSA 认证计划认证的解决方案。因此 PUFsecurity 计划作为合作伙伴与 Arm 携手合作，促进安全的物联网世界并保护我们互联的世界。