版本 1: 2022 年 3 月

安全连接设备的基本属性

PSA Certified 的 10 个安全目标和 Microsoft 的高安全设备的 7 个属性

Rob Smart，Arm（PSA 认证的联合创始人）高级首席安全架构师和来自微软的贡献

本文档由 PSA Certified 和 Microsoft 编写，旨在说明 PSA Certified 10 安全目标和 Microsoft 的高安全设备的七个属性的共同目标。它非常适合希望根据两个关键行业参与者的专业知识从高层次了解连接设备安全所必需的内容的人。
我们将介绍的主要内容是:

- Microsoft 和 PSA Certified 确定基本安全要求的观点和动机。
- 概述 Microsoft 的高安全设备的七项属性和 PSA 认证的 10 项安全目标。
- 看似不同的属性和目标，实际上有很多共同点。

我们进入了数字化转型时代，几乎每个行业都在采用技术，以前所未有的规模实现新的效率、产品和服务。这种数字化转型的核心是连接设备、收集和解释数据以及提供智能业务或服务洞察力的能力。然而，在保护支撑企业基本价值的设备方面投资不足，使消费者和企业都面临严重的安全风险。

最终，数字化转型将由数据驱动：真实、可信的数据比以往任何时候都重要。从每个传感器和执行器收集的少量数据必须是可信的，因为它累积成为驱动大规模新转型数字服务的大数据。可信数据和可信服务只有由具有健全安全原则的设备生成，才能真正成为可能并实现规模化。

随着物联网开始发展，Arm 和领先的安全评估实验室率先推出了 PSA Certified [1]，一种旨在与生态系统建立基线安全要求的合作伙伴关系。这是基于 PSA 认证的 10 个安全目标，每个连接的设备在与互联网交互之前都应满足这些目标。这些可以通过纳入信任根 (RoT) 来实现，他们推动了 PSA-RoT 的定义。目标是高级抽象自 Arm 在保护设备方面的长期经验，以及针对常见连接设备用例的特定威胁建模和安全分析。

同时，微软注意到高昂的开发成本和维护通常限制了在连接设备生态系统中采用强安全性。每一个设备，无论是连接的恒温器还是连接在工厂车间的设备，都是攻击的潜在目标，因此需要高完整性的安全。通过广泛的研究和测试，Microsoft 确定了至少应存在于所有被认为是高安全设备的七个属性。该研究的结果记录在“高安全设备的七个属性”文 [2] 中。

PSA 认证的 10 个安全目标和 Microsoft 的七项属性都旨在推动物联网设备生态系统中基础安全的采用。在本白皮书中，我们使用 PSA 认证和高安全设备的七种特性论文中的材料对两者进行了描述，以进行高层次比较以及我们对它们的异同的看法。

最终，号召行动非常简单：安全是每个人的责任，我们需要团结起来推进物联网的安全。

微软高安全设备的七个特性是什么？

以下摘自高安全设备的七个属性（第 2 版），© 2020 Microsoft Corporation，以及在本文其余部分中使用的对其的引用，均经许可使用。这些摘录是“按原文”提供的。这些摘录中表达的信息和观点，包括 URL 和其他互联网网站引用，可能会更改，恕不另行通知。您自行承担使用的风险。某些示例可能仅用于说明并且是虚构的。没有真正的关联是有意或推断的。本文档不向您提供任何 Microsoft 产品中任何知识产权的任何合法权利。

微软进行了广泛的研究和测试，以了解连接设备的安全基线要求。由此产生的证据为“高安全设备的七个属性”一文中提供了信息。该文详细介绍了在每个被认为是高安全的设备中发现的七个属性，形成了通常添加额外安全措施的安全基础。这七个属性应被视为每个连接设备中安全性的必需基线。对于丢失的任何资产，业主或客户需要实施其他方式来补偿。例如，安全事件可能需要在没有可更新安全性的情况下断开设备并召回或手动修补它们 [3]。

高安全设备的七大属性

您的设备是高安全的还是仅具有一些安全功能？

硬件信任根
您的设备的身份和软件完整性是否受硬件保护？

纵深防御
即使某些安全机制被破坏了，您的设备是否仍然受到保护

小型可信计算基础
您设备的安全执行代码是否受到保护不受应用程序代码中 bug 影响？

动态隔间
部署后您的设备的安全性能否提高？

无密码身份验证
您的设备是否对自身进行身份验证？

错误报告
您的设备是否报告错误以让您了解现场情况？

可更新安全
您的设备软件会自动更新吗？

- **高安全设备具有硬件信任根。**

设备的私有身份密钥受硬件保护，设备软件的完整性
通过硬件验证，并且硬件包含针对侧信道攻击的物理防护。与软件不同，硬件具有作为设备安全基础所需的两个重要属性。首先，单一用途的硬件难以被攻击者重复用于非预期的操作。其次，硬件可以检测和缓解物理攻击；例如，在硬件中很容易实现对复位引脚进行脉冲测试以防止毛刺攻击。当用于保护机密和完整性时，硬件提供了坚实的基础
可以安全可靠地实现丰富的软件功能的信任。

- **高安全的设备具有纵深防御。**

在高安全的设备中，对每一类威胁都应用了多种缓解措施。在设备中
如果只有一层防御，例如大多数基于 RTOS 的设备，即使是设计或实现中的一个错误也足以导致灾难性的妥协。由于新威胁通常是完全出乎意料的，因此在实践中，拥有多种对策通常会成为安全设备和受损设备之间的区别。

- **高安全的设备具有小的可信计算基础。**

可信计算基 (TCB) 是“安全性所依赖的少量软件和硬件，我们将其与大量可以在不影响安全性的情况下行为不端的软件区分开来”。在一个设备内，用于不同操作的 TCB 可能不同。例如，用于保护静态数据的 TCB 可能包括硬件信任根、用于加密和解密的软件以及用于密封和解封加密密钥的软件。另一方面，用于安全通信的 TCB 也可能包括 TLS 实现。任何操作的 TCB 都应尽可能小，以最大限度地减少暴露给攻击面，并减少错误或功能被重新利用以规避安全保护的可能性。应保护 TCB 代码免受非关键设备代码的影响，以确保其正确操作，即使其他代码受到损害。安全性较低的设备通常没有隔离的 TCB - 这些设备中的安全代码与设备代码的其余部分在同一个区域中执行，结果是设备代码中任何地方的一个错误都可能导致灾难性的全系统妥协。

- **高安全的设备提供动态隔间。**

在计算设备中，网络安全隔间是硬件强制边界，可防止一个软件隔间中的破坏或缺陷传播到设备的其他软件隔间。隔间引入了额外的保护边界，以创建额外的纵深防御层。动态隔间允许在设备的整个部署生命周期内引入新的边界，以提高安全性以应对不断升级的安全威胁。

- **高安全的设备使用无密码身份验证。**

在与其他本地设备和云服务通信时，无密码身份验证（例如证书）用于证明相互身份验证的身份。证书或其他无密码身份验证令牌是使用秘密私钥签名的身份和授权证明，并且可以根据已知公钥进行验证。与基于共享机密的密码或其他身份验证机制不同，由硬件信任根支持的无密码身份验证机制不能被窃取、伪造或以其他方式用于验证冒名顶替者。

- **高安全的设备具有在线错误报告。**

当安全设备发生错误时，会自动收集错误报告并及时发送到错误分析系统。在最好的情况下，错误是由于对极其罕见的事件序列的编程不足。在最坏的情况下，该错误是由攻击者在设备上探测新的攻击向量引起的。无论哪种情况，错误分析系统都会关联整个设备群中的错误报告，以便自动诊断错误。有了足够大的报告基础，即使是极其罕见的错误情况也可以被诊断和纠正，并且可以在新的攻击向量被广泛利用之前识别和隔离它们。错误报告可在一系列高安全的设备中启用全球“免疫系统”。如果没有自动在线错误报告，设备制造商对于现场遇到的设备错误一无所知，对新出现的攻击可能措手不及

- **高安全设备具有可更新的安全性**。

具有可更新安全的设备可以自动更新到更安全的状态，即使在设备受到威胁之后也是如此。可更新的安全性是必要的，因为随着攻击者发现新的攻击向量并创建新的攻击方法和工具，安全威胁会不断演变和升级。 为了应对新出现的威胁，必须定期更新设备安全性。 在极端情况下，当设备软件的隔间和层受到零日漏洞攻击的影响时，较低层必须重建和更新设备更高级别的安全性。 远程证明和回滚保护保证，一旦更新，设备不能恢复到已知的易受攻击状态。 没有可更新安全性的设备是一场等待发生的危机。

PSA 认证的 10 个安全目标是什么？

右侧的 PSA 认证安全目标提供了一种高级抽象方式来考虑保护和建立对连接设备的信任的基本功能。 基于整个行业的最佳安全实践，这套目标广泛适用于供应链中的不同实体，从芯片设计人员、软件开发人员和设备供应商到云和网络基础设施提供商。 抽象允许根据需要应用这些目标，例如，应用于最终用户连接的设备、硬件组件、软件组件或服务。 在描述目标时，术语设备用于表示任何级别的任何实体必须是安全和值得信赖的。应该注意尽管重点是本地或互联网连接的设备，但许多方面与保护未连接的设备有关。

PSA 认证平台安全模型概述了 10 个目标：

唯一标识
防回滚
隔离
认证
交互
安全启动
安全存储
安全更新
密码和可信服务

1. **唯一标识：**为了与特定设备交互，唯一标识身份应该分配给设备，并且这个身份应该是可证明的。 此身份有助于与设备进行可信交互，例如交换数据和管理设备。

2. **安全生命周期**：设备应支持依赖于软件版本、运行时状态、硬件配置、调试端口状态和产品生命周期阶段的安全生命周期。 安全生命周期的每个安全状态都应该是可证明的，并且可能会影响对设备的访问。

3. **证明**：应通过证明提供设备属性的证据，包括设备的身份和安全生命周期状态。 设备标识和证明数据应该是使用受信任第三方的设备验证过程的一部分

4. **安全启动**：为确保只能在设备上执行授权软件，需要安全启动和安全加载过程。 应该检测和防止未经授权的引导代码。 如果软件不能破坏设备，未经授权的软件可能被允许使用。

5. **安全更新**：为设备提供安全或功能更新时，只能在设备上更新真实合法的固件。 可以在下载时执行身份验证，但是必须通过安全启动授权更新的执行。

6. **防回滚**：防止回滚到以前的软件版本对于确保无法恢复以前版本的代码至关重要。 只有在获得授权时，才可以出于恢复目的进行回滚。

7. **隔离**：隔离旨在防止一项服务损害其他服务。 这是通过将可信服务与其他可信服务、更低信任服务和不受信任的服务隔离开来完成的。

8. **交互**：设备应支持跨隔离边界的交互，以使隔离的服务能够正常工作。 接口不得让系统受到损害。 可能需要对数据保密。 应考虑设备内部以及设备与外部世界之间的交互。

9. **安全存储**：为防止私有数据在受信任的服务或设备之外被克隆或泄露，必须对其进行唯一绑定。 私有数据的机密性和完整性通常使用密钥来实现，密钥本身需要绑定到设备和服务。

10. **密码和可信服务**：应实施一组最小的可信服务和密码操作作为可信设备的构建模块块。这些应支持关键功能，包括安全生命周期、隔离、安全存储、证明、安全启动、安全加载和数据绑定。

PSA 认证的安全目标构成了平台安全模型 [4] 的基础，该模型是一个总体文档，以与架构无关的方式定义了重要的概念和术语。 它还推动了其他 PSA 认证规范，其中一些以及与独立 PSA 认证评估计划相关的所有规范不依赖于任何基于 Arm 技术的实施。 然而，促进安全产品的构建是有价值的，因此一些平台安全文档是关于如何使用 Arm 技术满足要求的指南。 此外，还有 PSA 功能 API [5] 用于标准服务，例如密码、安全存储和设备认证，旨在鼓励采用此类标准服务。

将七个属性和十个目标联系起来

PSA 认证计划已将其要求映射到领先的国际安全指南集。尽管通常很明显存在很多共性，确定任何两组之间的关系被证明不是一项简单的任务。在本文中，我们旨在说明这对于七属性和十个目标之间的关系也是如此。为了更详细地探讨两者之间的关系，我们将依次讨论七个属性中的每一个以及其在 10 个安全目标中的含义。这样做没有任何意义，我们可以很容易地依次查看这 10 个目标中的每一个。

硬件信任根

硬件信任根，在 PSA Certified 中称为不可变信任根，包括建立和维护设备信任所需的硬件和任何固定固件和数据。正是这些项目的不变性意味着它可以被固有地信任。与软件不同，硬件的不变性使得攻击者难以将其重用于非预期的操作。

包括从复位释放后立即启动的第一阶段。这必须得到保护，因为它是通过对要在设备上运行的软件进行签名验证来确保完整性的锚。换句话说，确保只有授权的软件可以执行 ④⑥。硬件信任根还负责不可变数据的安全存储。包括设备身份①、能够证明（或证明）设备身份的任何私钥③ 、用于确保软件完整性的公钥④（可能来自制造商）、用于回滚保护的不可逆存储⑥ 、以及任何秘密，例如保护静态数据的唯一加密密钥 ⑨.

通常需要额外的硬件来加强设备的安全性。包括基于生命周期状态，例如配置、安全和调试②。访问控制，通过隔离机制访问控制，包括对所需数据字段的写锁定和/或读锁定⑦。可以提供加密硬件，利用不可变的信任根秘密和可信赖的熵源来生成随机数⑩。

根据适用于目标产品的风险或任何所需的认证计划保证级别，硬件信任根实施可能是防篡改的，并且可能包括针对某些类别的侧信道攻击的对策，可能通过使用硬件电压和时钟故障探测器。

小型可信计算基

连接的设备非常依赖软件，因此区分实现可信安全功能的软件（和硬件）和系统软件的其余部分非常重要。

目的是最小化安全关键功能的攻击面；那里的代码越少接口定义得越好⑧，存在漏洞或可以重新利用以规避安全保护的功能。不可能将所有必需的安全功能集中在一个小的可验证功能中。因此，设备内的不同操作可能依赖于不同的 TCB。这些 TCB 的隔离⑦允许单独测试和验证每个 TCB，并且每个 TCB 的攻击面减少到跨接口的交互⑧。

小型 TCB 是一个实施目标，不直接反映在安全目标中。 PSA 认证平台安全模型建议信任根的不可变部分小、简单、可验证；一旦芯片制造完成，就无法更改。进一步的信任根功能通常必须存在于软件中。 TCB 中的代码应由精通攻击者使用的最新工具和方法的熟练专家进行严格测试，以防止潜在的危害。

非关键软件影响任何安全关键代码操作的能力依赖于该 TCB 的隔离⑦。隔离可用于将安全关键系统划分为一组具有已定义接口的隔离 TCB，这些接口执行不同的安全功能。这些可能是可分离验证的。然而，这种隔离是不够的。

动态隔间

隔离⑦是系统软件分区（分区化）和访问关键系统资源的基础。从安全的角度来看，目标通常被认为意味着将更可信软件与不太受信任的软件隔离开来。但是，隔离实际上是承认所有软件都可能包含可能被利用来破坏设备安全性的缺陷。在更广泛的意义上，隔离旨在防止一个软件组件损害另一个软件组件

PSA 认证平台安全模型中确定了三个隔离边界概念，但部署将取决于适用于目标市场的威胁以及任何适用的认证方案。至少，需要硬件强制将安全服务与系统的其余部分隔离。这自然映射到 Arm TrustZoneTM，但 PSA Certified 以不需要基于 Arm 的解决方案的方式表达所有要求。例如，使用具有硬件过滤的多个处理器是一种有效的方法，在某些情况下，使用操作系统进程或独立虚拟机是一种有效的方法。当然，这些技术可以部署在任何系统中，并且可以增加分层防御的概念。

动态划分允许隔离边界随着新的安全现场更新⑤而改变，旨在提高安全性以应对新出现的安全威胁和攻击。安全性较低的设备，通常是采用实时操作系统 (RTOS) 的低成本设备，要么没有软件隔间，要么只有少量或固定数量，在部署设备后无法重新配置，因此，应对新的安全威胁的能力非常有限。当然，这需要一个安全的更新机制⑤ 和一种撤销以前版本的方法⑥。但是，支持设备更新可能会受到资源限制的影响，例如用于处理下载的易失性存储器、用于软件和数据存储的非易失性存储器，一次性可编程内存和性能。

隔离是必不可少的，但如果这些隔离的组件要在整个系统中服务于某个目的，那么隔离组件之间的交互通常是必要的⑧。这些接口的设计必须确保它们不能被使用或滥用，以便通过以下方式危及安全性 以非预期的方式使用该功能或导致泄露其拥有的任何敏感数据
该功能或通过该配置控制的任何系统重新配置。例如，滥用接口不得导致密码密钥泄露，或禁用建立系统安全性的机制。此外，PSA Certified 认识到可能有必要确保通过此类接口交换的任何数据的机密性和完整性。如果接口是对外的尤其如此，其拦截数据交换的能力远大于系统内部。

无密码身份验证

身份验证涉及安全地识别某些东西。那东西可能是要执行的软件④，下载的任何更新的完整性⑤，设备安全状态，通过认证反映设备中的硬件和软件的状态②③，或者设备身份①，用于与其他本地设备和云服务通信时的相互认证⑧。

基于密码的技术，或更一般地说，那些依赖于共享“秘密”的技术，很容易泄露秘密。对于要求密码或秘密通过易于监控的通道进行通信的身份验证协议尤其如此。证书或其他无密码身份验证令牌是使用秘密私钥签名的真实性证明，并且可以根据已知的公钥进行验证。与基于共享秘密的密码或其他身份验证机制不同，由硬件信任根支持的无密码身份验证机制不能被窃取、伪造或以其他方式用于验证冒名顶替者。PSA Certified 建议使用不使用的技术共享秘密，这通常意味着使用证书和非对称加密。

除了需要启动授权代码④⑥和设备身份①③ 的最小实现之外，证书可以证明在设备上运行的软件的身份②③。例如，这允许验证服务检查设备是否正在运行 最新的软件，它解决了所有已知的安全漏洞，或者需要安全更新⑤并在服务继续之前确认它已被应用。换一种说法，连接服务必须能够验证声明的设备身份确实指的是它声称的设备。这可能依赖于必须由硬件信任根保护的嵌入式私钥，以确保它永远不会被泄露，这对于确保设备不会被欺骗至关重要。

可更新安全

完全在硬件信任根中实现所有功能，包括设计时 ROM 中的代码是有风险的。如果在设计的任何可更新部分中发现了无法解决的故障，唯一的做法是重新切割硅片，这可能会非常昂贵。显然，这只涉及未来的生产，而不是已经制造的零件。完全依赖固定硬件解决方案也意味着无法灵活适应不同的需求，也无法添加新的信任根服务。

这些因素就是为什么 PSA 认证平台安全模型为硬件信任根定义了一个最小可信计算基础，并确定了对在由硬件信任根进行身份验证的软件中实施的安全服务的需求。“具有可更新安全性的设备可以更新到更安全的状态⑤，理想情况下是自动更新，即使在设备受到威胁之后也是如此。可更新安全是必要的，因为随着攻击者发现新的攻击向量并创建新的攻击方法和工具，安全威胁会不断演变和升级。为了应对新出现的威胁，必须定期更新设备安全性。在极端情况下，当设备软件的隔间和层受到零日漏洞攻击的影响时，较低层必须重建和更新设备更高级别的安全性。远程证明③和回滚保护⑥保证，一旦更新，设备就不能恢复到有效签名但有缺陷的状态。没有可更新安全性的设备是一场等待发生的危机。” [2]

通常，设备软件防御的每一层都应该独立更新，而不会使其他层失效，甚至可能是自动更新。重要的是，任何更新都必须经过身份验证，最终通过信任链链接到硬件根。信任并保持稳健，以确保更新本身不会危及设备⑤ “可更新安全的可靠实施提供了强大的机制，即使更新失败或外部条件（如更新期间的电源或网络故障）也能自动恢复。” [2] 这允许在实际情况下，如果更新在交付后出现问题，则需要安全地恢复到以前的可验证版本。

纵深防御

如果只有一层防御，设计或实施中的一个错误可能足以导致灾难性的妥协。新威胁往往完全出乎意料因此，在实践中，多层防御通常会在安全设备和受损设备之间产生差异。几乎所有纵深防御设计的共同点必须是“假设违反”和“零信任”的理念。如果攻击者已经破坏了设备的其他部分，设计人员必须评估每种保护机制的有效性。

纵深防御可以采取多种形式。例如，仅执行授权代码④，防止回滚到具有已知漏洞的旧版本代码⑥，这当然意味着通过安全更新机制可更新安全性⑤。隔离各种代码⑦是一项非常重要的纵深防御技术例如，防止网络堆栈覆盖闪存中的设备固件。在物理隔离的内核上运行关键任务是提供这种隔离的强大机制，并且可以比较容易推理。但是，使用具有内存管理单元支持的访问控制的处理器特权执行模型非常普遍。虚拟化的使用可以在设备固件保护的防御中增加另一层。

这种隔离确实解决了设计者不希望的交互。有意交互必须是健壮的⑧，换句话说，如果有意的交互点导致例如数据泄漏，则提供隔离几乎没有意义。

硬件也应该考虑纵深防御。例如，配置寄存器上的一次写入锁存器和程序代码上的写保护锁存器将范围限制为即使设备的软件暂时受到损害，设备也可以重新利用。这些机制是通过将 RoT 划分为不可变和可变组件、时间隔离的概念和提供可信服务来配置安全硬件和支持安全性来实现 PSA 认证平台安全模型中涉及的概念的方法功能⑩.

对已识别威胁的多重缓解不直接表示为 PSA 认证的安全目标。 除了 PSA 安全目标之外，PSA 认证规范还推荐了硬件防篡改和针对侧信道攻击的对策、对硬件资源的访问控制、存储数据的加密、对调试端口的访问控制等。 这些有助于提高设备的防御深度。 支持的程度将取决于目标市场、成本影响以及与认证计划相关的任何保护概况。

错误报告属性

及时向在线错误分析系统报告在安全设备上检测到的错误是高安全设备的 7 个特性之一。确切地说，哪些错误可以通过足够的信息检测并报告，尤其是对于最不可预测的问题，将是非常具体的实施。此外，在线错误分析系统必须能够分析报告，并且更广泛的生态系统必须能够确定适当的纠正措施，这两者都不是连接设备的功能。因此，错误报告超出了 PSA Certified 的范围和目标。尽管如此，如果设备能够应用纠正措施（例如，执行安全更新⑤、防止回滚到易受攻击的版本⑥ 并根据已知设备状态允许服务执行②③.

PSA 认证的 1 级要求来记录安全相关事件并确保日志的机密性和完整性 [4]。设备上生成的任何故障报告的真实性可以按照绑定目标绑定到该设备⑨，或通过证明目标③并由 PSA Certified Initial Attestation 服务绑定到该设备。

PSA 认证的安全生命周期目标

七个属性未直接涵盖的一个 PSA 认证目标是设备支持安全生命周期状态。安全生命周期中的每个安全状态都定义了设备的安全属性，并且取决于软件版本、设备上的运行时测量、硬件配置、调试模式以及产品生命周期阶段等因素（例如，开发、部署、退货和报废）。这个目标的动机是需要连接的服务以取决于安全状态的方式行事。

虽然不区分不同的生命周期状态，但高安全设备的七个属性提供了一种关于证明的观点。例如，使用设备根据证明颁发的证书或身份验证令牌，使设备访问的服务能够验证并要求设备执行软件更新并且不运行其软件的旧版本。此外，远程证明和回滚保护可确保设备无法恢复到已知的易受攻击状态。

结论

随着对数字化转型、可信数据和连接设备的依赖迅速飙升，企业显然需要认真对待设备的安全性。为了保护企业和服务的声誉，领导者需要采取积极措施，确保他们不会通过不安全的设备将薄弱环节引入系统。然而，开发、制造、部署、最终安全地管理物联网设备可能会带来独特的挑战。

PSA Certified 的 10 个安全目标和 Microsoft 的高安全设备的七个属性提供了信息丰富的清单以供使用。他们揭开了基线设备安全要求的神秘面纱，并帮助业务领导者了解他们应该向供应商提出什么要求，并在他们自己的产品中实现目标。实施必要的功能包括芯片要求，例如基于硬件的信任根、软件架构决策以及与云服务的深度集成 [3] 以使客户有信心信任他们的设备。由于这种范围和复杂性，七大属性和十个目标在这些要求的实施方式以及确保满足和管理这些要求的责任所在方面可能存在差异。为了提供帮助，PSA 认证计划包括威胁模型和安全分析、安全需求规范和应用程序编程接口，所有这些都与架构无关，也提供了开源参考实现和测试套件。总之，这些可以促使正确的安全级别上实现一致的信任根设计。虽然 Arm 和 Microsoft 绝对不是该领域的唯一贡献者，但我们一致认为一组最低要求应该应用到物联网设备。

尽管存在相似之处和不同之处，但我们认为应该保护我们的客户免受威胁。他们正面临着数字化转型的旅程。我们共同呼吁生态系统--不要因为“不知道从哪里开始”而无所适从，而是使用我们的指南来引领更安全的未来。

References
1. PSA Certified, see psacertified.org
2. Microsoft Research; The Seven Properties of Highly Secured Devices (2nd Edition)
3. Ed Nightingale & Penny Orwick, Cybersecurity best practices to implement highly secured devices, see Cybersecurity best practices to implement highly secured devices – Microsoft Security Blog
4. Platform Security Model, see psacertified.org/app/uploads/2020/10/DEN0079_PSA_SM_BETA-0.pdf
5. PSA Functional API Certification, see psacertified.org/development-resources/certification-resources