白皮书

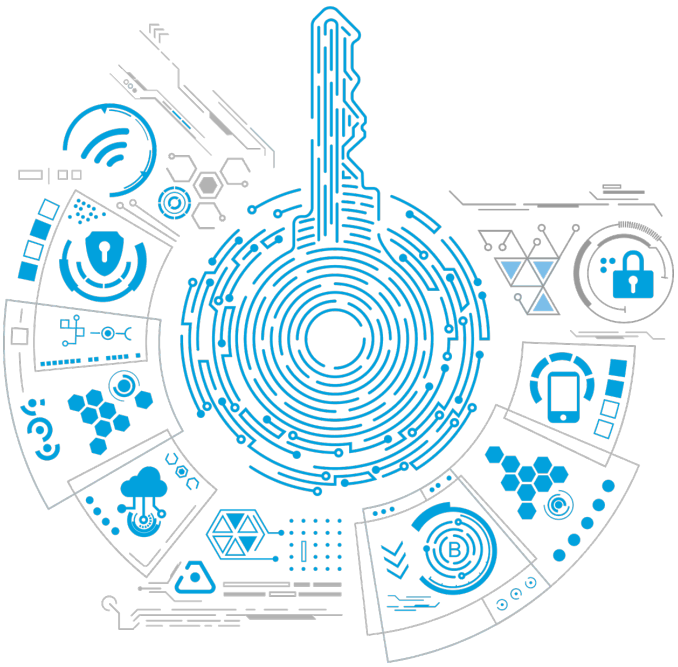
借助 Qorvo QPG6200 为物联网构建安全与信任

引言

在物联网（IoT）日益融入日常生活的时代，消费者对相关技术的信任建立在其安全性保障的基础之上。稳健的网络安全措施对于构建这种信任至关重要。为应对这一需求，行业和政府纷纷出台规定，加强了对网络威胁的防御要求，以保护消费者的隐私及安全。

在美国，网络安全标识（Cyber Trust Mark）作为消费者的一项重要参考标准，表明拥有该标识的产品遵循了如美国国家标准与技术研究院（NIST）IR 8425 文件中所详述的安全指南。同样，欧洲电信标准化协会（ETSI）即将通过 ETSI EN 303 645 设立一个强有力的框架，旨在为欧盟市场内的物联网设备设定高标准。

本白皮书深入探讨了 Qorvo 针对物联网量身定制的广泛多标准、节能型无线连接解决方案产品组合。接下来的章节将详细分析 QPG6200 的安全特性，并辅以全面的技术文档和应用说明。



目录

修订历史

版本	日期	备注
0.1	2023-10-13	面向实验室初版发布
0.2	2024-03-20	IoT SDK 0.1.6 版本发布
0.3	2024-08-xx	IoT SDK 1.0.0 版本发布

术语

芯片制造商：Qorvo

系统制造商：将芯片集成到产品中的一方，例如物联网消费类设备制造商

终端客户：使用系统制造商所销售产品的一方，例如购买物联网设备的消费者

下一代 Matter™ 解决方案

我们生活在一个物联网（IoT）的时代，身边遍布数以百万计的智能设备；从智能音箱等智能网关，到灯泡、恒温器等各式各样的智能家电，不一而足。Qorvo 立足行业前沿，为全球物联网制造商提供高性能解决方案。QPG6200 正是 Qorvo 致力于保障物联网安全的有力证明；其设计融入了满足市场严苛要求和行业标准认证的安全特性。

QPG6200 专为要求高安全性而又不影响成本效益或效率的物联网应用而设计。其具有专用的安全管理引擎——安全元件；该引擎提供安全的产品生命周期管理、安全存储、安全启动、安全调试，以及带侧信道分析（差分功率分析）保护功能的硬件加速加密。

QPG6200 已获得 PSA 2 级认证，标志着产品安全性的可靠保障。其配套的软件开发工具包（SDK）、硬件开发板以及一系列软件工具和文档，简化了安全设计的复杂性，使其更加直观易懂。着眼于未来，QPG6200 为 Matter 等先进协议奠定了坚实基础，确保其准备好迎接下一波物联网创新浪潮。

硬件概览

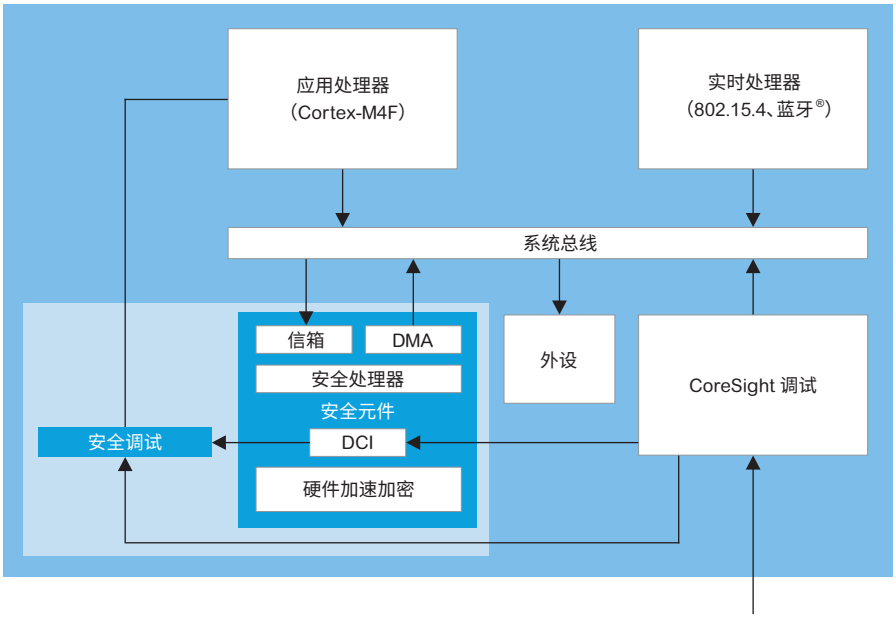


图 1，用于概述安全功能的简化方框图。

如**图 1** 所示，QPG6200 包含一个应用处理器（Arm® Cortex®-M4F）、一个用于射频（RF）通信的实时（RT）系统，以及安全元件。安全元件作为一个独立组件，内含安全处理器、信箱、DMA 引擎、调试质询接口（DCI），以及硬件加速加密模块。

产品生命周期

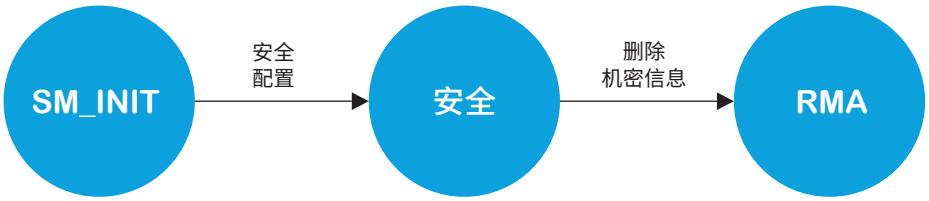


图 2，产品生命周期中的各个状态

QPG6200 实现了安全的产品生命周期，生命周期状态之间的转换定义明确（**图 2**）。新设备处于未初始化的生命周期状态（LCS）SM_INIT。在这种状态下，所有可配置的安全功能均被禁用，以方便开发。

在产品交付给最终客户之前，必须使用安全资产对设备进行初始化（请参阅“安全配置”章节）。这一步骤将设备转变为安全生命周期状态。在此状态下，可使用安全启动和安全调试等安全功能。

如果设备需要执行退货授权（RMA）流程并退回芯片制造商，则必须确保系统制造商的数据安全。在退回之前，可以擦除设备的特定机密信息，从而将设备转入 RMA 生命周期状态。这一过程保证了所有客户和制造商数据的安全；一旦设备离开原用户环境后便无法恢复任何敏感信息。

安全存储

安全存储利用安全元件保障数据机密性；该安全元件使用唯一的存储根密钥对数据进行加密。此密钥可源自物理不可克隆功能，也可由芯片上的随机数生成器创建。

安全存储内保护的每项数据均使用独特的密钥进行加密；该密钥是安全元件存储根密钥的派生密钥。此过程通常称为“密钥封装”，用于在安全元件内部加密敏感数据。之后，这些加密的数据可以安全地存储在非安全内存中（如应用内存），而解密只能由安全元件执行。

系统制造商可以选择对安全存储内的数据实施使用限制，以加强控制；例如，密钥可能仅限于在加密操作中使用，且永远不离开安全元件，从而防止潜在的信息泄露。

安全存储的密钥可以通过安全配置进行部署、在安全元件内创建，或由应用程序协商产生。这些措施确保密钥及其保护的数据免受未经授权的访问。

安全启动

QPG6200 的多阶段安全启动（如**图 3** 所示）流程确保只有授权软件能在设备上运行。

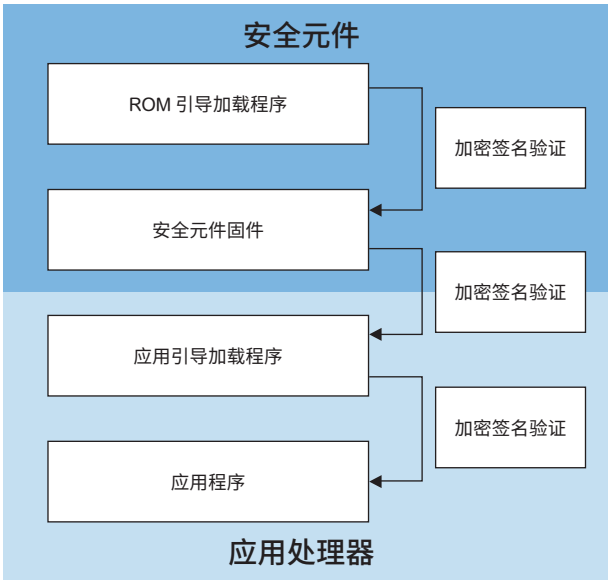


图 3，安全启动概览

在启动时，应用处理器和实时处理器最初都处于非工作状态，被置于复位模式。启动过程从安全元件内的 ROM 引导加载程序开始。该程序运行于安全处理器之上，触发安全启动序列。它的主要作用是作为硬件锚定且不可更改的信任根，并验证安全元件固件上的 ECDSA 签名。如果验证成功，安全元件的控制权将转移给安全元件固件。此外，ROM 引导加载程序还具备处理安全元件固件安全升级的功能，确保设备从一开始便拥有安全完整性。

安全元件固件启用安全元件的安全功能，并使用 ECDSA 签名认证应用程序的引导加载程序。一旦认证通过，应用处理器被激活以运行经验证的应用引导加载程序。安全元件固件继续保持警惕，处理来自应用处理器的安全相关请求；如执行硬件加速加密和管理安全存储。此外，它还负责升级应用引导加载程序。

随后，应用处理器上的应用引导加载程序接手，利用安全元件的安全服务来验证应用的 ECDSA 签名。验证成功后，控制权将移交给应用程序，然后由应用处理器执行。此外，应用引导加载程序还负责管理应用程序的更新。

安全升级

安全元件固件

芯片制造商可能会为安全元件固件提供升级。这些升级以不透明的二进制文件形式提供，由 Qorvo 进行加密和加密签名。应用程序负责及时下载这些升级包。当下载完成后，应用程序必须通过向安全元件发送命令来触发升级。

应用引导加载程序

系统制造商可为应用引导加载程序提供升级。这些升级同样以加密并经过加密签名的二进制文件形式提供。应用程序负责及时下载这些升级。下载完成后，应用程序必须向安全元件发送命令来触发升级。

应用程序

应用程序的升级由应用引导加载程序执行，这让系统制造商在实施定制升级机制时获得了最大的灵活性。QPG6200 SDK 中包含了一个涵盖应用引导加载程序和应用程序的参考实施方案；其中，应用程序负责下载加密并经过签名的升级镜像，然后指示应用引导加载程序进行升级并重置设备。

安全调试

开发人员可以使用 JTAG 或 SWD 接口访问应用处理器的调试功能。这些调试设施默认连接到一组特定的引脚，便于使用，从而促进快速开发。然而，这种标准设置并不安全。如果不加以限制，调试端口可能会危及应用处理器的安全性。因此，在设备发货给客户之前，确保调试端口的安全性至关重要。

系统制造商可以选择以下两种方法之一来保障调试访问的安全性：

- 永久关闭调试端口
- 启用安全调试

请注意：配置这两个选项中的任何一项，都是不可逆的操作。

当启用安全调试时，调试端口提供对调试质询接口（DCI）的访问。开发人员可以向芯片请求一次性随机质询。质询内容连同解锁应用处理器调试的命令必须由用户使用私钥进行加密签名。发送回此命令和签名后，将解锁应用处理器的完整调试功能。这一过程确保了持有私钥的各方能够安全地获得调试权限。

安全配置

安全配置是系统制造商初始化 QPG6200 安全参数的过程。这些参数至少包括：

- 应用引导加载程序和应用程序签名验证密钥（ECDSA 公钥摘要）
- 应用引导加载程序和应用程序升级加密密钥（AES-256 密钥）
- 安全调试解锁命令签名验证密钥（ECDSA 公钥摘要）

配置流程可包括以下可选内容：

- 初始应用引导加载程序
- 初始应用程序
- 特定于应用程序的安全参数，包括但不限于：
  - Matter 设备认证证书（DAC）和认证私钥
  - 其它特定应用密钥
    - 这些可直接配置到安全存储中

配置数据通过 AES-GCM 算法和每个系统制造商独有的系统制造商配置密钥进行打包并加密。这既保护了配置数据的机密性及真实性，又简化了生产设施的安全要求。

设备认证

认证作为一种安全流程，允许外部验证者确认设备或系统的真实性。通常，验证者会向设备发送质询信息，通常是一串随机数据。设备随后使用其唯一的私钥对该数据进行签名，并将签名以及包含与私钥对应公钥的证书返回给验证者。这样，验证者就可以验证签名和证书的真实性。

QPG6200 支持此认证流程。它可以验证硅芯片本身的真实性，也提供应用级别的认证机制；如 Matter 协议中定义的设备认证证书（DAC）。每个 QPG6200 芯片都嵌入了芯片级的唯一私钥，Qorvo 对该私钥的公钥进行加密签名。随后，系统制造商可以使用 Qorvo 的证书链来验证签名及证书，确保 Qorvo 硅芯片的真实性。

虽然这对系统制造商来说是有价值的信息，但对嵌入 QPG6200 的产品进行认证时，应验证整个产品，而不仅仅是芯片。不同的标准推荐了不同的认证方法。QPG6200 支持基本的认证要求，包括第三方设备认证（非 VID 范围的 PAA）和系统制造商（VID 范围的 PAA），这些要求已专门针对 Matter 协议合规性进行了定义。

硬件加速加密

安全元件包含用于加速加密操作的硬件。下文重点介绍了主要算法，完整列表请参见 QPG6200 数据手册。

硬件加密加速算法：

- AES128/192/256，支持 ECB/CTR/CBC/CFB 以及 CCM/GCM/GMAC 模式
- SHA-1、SHA-2/256/384/512
- ECDSA、ECDH（P-192、P-256、P-384、P-521）
- EdDSA（Ed25519/Curve25519）
- J-PAKE
- PBKDF2、HKDF

AES 引擎和公钥（PK）加密引擎均具备抵御侧信道分析攻击的保护措施。这些防御手段阻止了攻击者通过时间分析或功耗观察来推断敏感密钥材料。

结论

Qorvo 致力于提供安全的认证解决方案，以降低 OEM 的风险并减少成本。QPG6200 正是这一承诺的体现，其安全架构符合物联网设备的关键行业标准和网络安全法规。其强大的套件以安全元素为亮点，提供全面的生命周期管理和先进的安全功能，并达到 PSA 2 级认证水平。

QPG6200 随附的完整 SDK、硬件开发板和详细文档简化了复杂的安全设计；确保了 OEM 能够高效集成最先进的安全措施，保持市场竞争力，并为 Matter 等协议做好准备。QPG6200 不仅仅是一款产品，更开拓了通往下一代物联网创新领导地位的路径。