WHITE PAPER

# Secure Trust in IoT with Qorvo's QPG6200

## Introduction

In a world where the internet of things (IoT) is becoming more ingrained in everyday life, customer confidence in these technologies hinges on the assurance of security. Robust cybersecurity measures are critical for fostering this trust. In response to this need, regulations from both industry and governments have ramped up the requirement for defenses against cyber threats, protecting consumer privacy and security.

In the United States, the Cyber Trust Mark serves as a benchmark for consumers, signaling adherence to security guidelines such as those detailed in the National Institute of Standards and Technology's NIST IR 8425. Similarly, the European Telecommunications Standards Institute (ETSI) is on the cusp of instituting a robust framework through ETSI EN 303 645, poised to set the bar for IoT devices within the European Union market.

This white paper delves into Qorvo's broad portfolio of **multi-standard, energy efficient wireless connectivity solutions** tailored for the IoT. The following sections will provide an in-depth look at the QPG6200's security attributes, supported by comprehensive technical documentation and application notes.

## Table of Contents



## Revision History

| Version | Date | Comment |
|---|---|---|
| 0.1 | 2023-10-13 | Preliminary release to lab |
| 0.2 | 2024-03-20 | IoT SDK 0.1.6 release |
| 0.3 | 2024-08-xx | IoT SDK 1.0.0 release |

## Terminology

Chip Manufactuer: Qorvo

System Manufacturer: The party that integrates the chip in a product, for example, an IoT consumer device manufacturer

End Customer: The party using the product sold by the System Manufacturer, for example, a consumer who bought an IoT device

## Next-Generation Matter™ Solution

We live in an era where the IoT landscape is dotted with millions of connected devices, from intelligent gateways, such as smart speakers, to a myriad of smart home appliances like light bulbs and thermostats. Qorvo stands at the forefront, supplying high-performance solutions to IoT manufacturers across the globe. The QPG6200 is a testament to Qorvo's commitment to keeping the IoT safe, designed with security features that meet the stringent demands of market requirements and industry standard certifications.

Engineered for IoT applications that demand high security without compromising cost-effectiveness or efficiency, the QPG6200 is designed with a dedicated security management engine – the secure element. This engine provides secure product life cycle management, secure storage, secure boot, secure debug and hardware accelerated cryptography with side channel analysis (differential power analysis) protection.

The QPG6200 has achieved the **PSA Certified Level 2**, a mark of security assurance. Its associated software development kit (SDK), hardware development board and suite of software tools and documentation simplifies and demystifies the complexity of security design. With a focus on futureproofing, the QPG6200 lays the foundation for advanced protocols like Matter, ensuring readiness for the next wave of IoT innovation.

## Hardware Overview

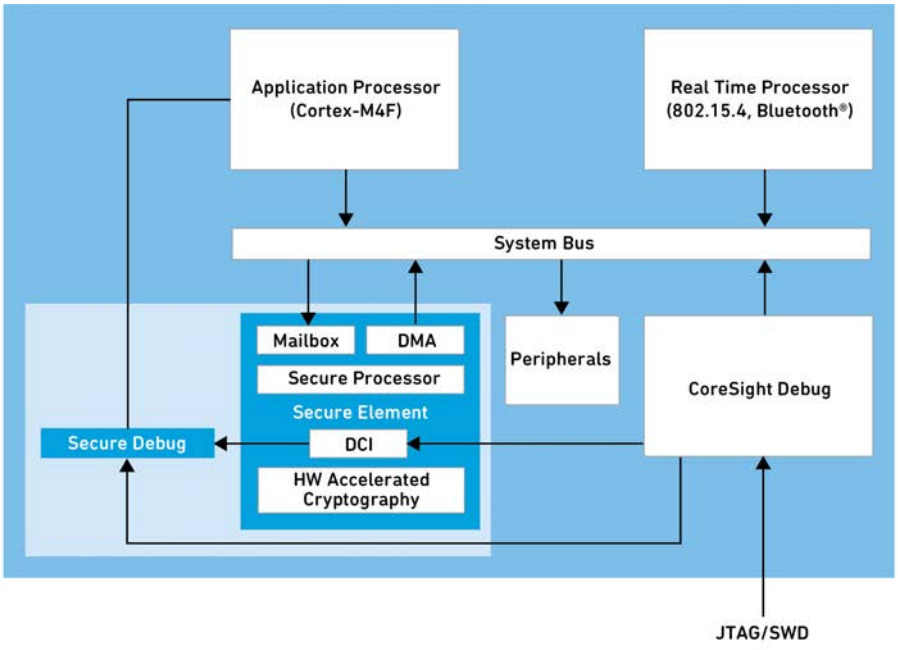




Figure 1: Simplified block diagram for the purpose of outlining security functionality.

As shown in **Figure 1**, the QPG6200 contains an application processor (an Arm® Cortex®-M4F), a real time (RT) system for RF communications and the secure element. The secure element is a stand-alone component and contains a secure processor, mailbox, DMA engine, debug challenge interface (DCI) and a block for hardware accelerated cryptography.

## Product Life Cycle

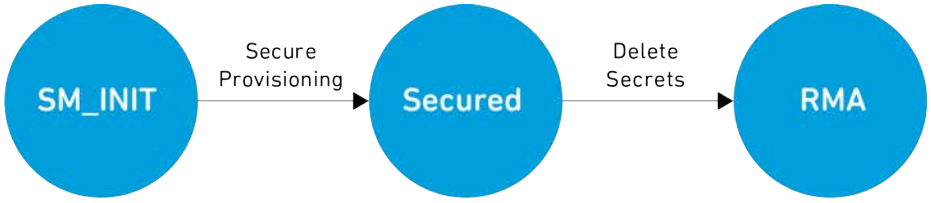




Figure 2: Product life cycle states.

The QPG6200 implements a secure product life cycle with well-defined transitions between the life cycle states (**Figure 2**). A fresh device is in the uninitialized life cycle state (LCS) SM_INIT. At this state, all configurable security features are disabled for ease of development.

Before products are shipped to end customers, the device must be initialized with security assets (see section **Secure Provisioning**). This transitions the device into the secured life cycle state. In the secured life cycle state, security functions such as secure boot and secure debug are available.

In the event a device needs to undergo the return merchandise authorization (RMA) process and be sent back to the chip manufacturer, system manufacturer data must be kept secure. Prior to return, the device's specific secrets can be erased, which transitions the device to the RMA life cycle status. This procedure guarantees the protection of all customer and manufacturer data, ensuring that no sensitive information can be retrieved from the device once it leaves the original user's environment.

## Secure Storage

Secure storage safeguards data confidentiality by utilizing the secure element, which encrypts the data with a unique storage root key. This key can originate from a physically unclonable function or can be created from the on-chip random number generator.

Each piece of data secured within secure storage is encrypted with a distinct key, which is a derivative of the storage root key known only to the secure element. This process, often termed 'key wrapping', encrypts sensitive data within the secure element. Subsequently, the encrypted data can be safely stored in non-secured memory, like application memory, with decryption possible only by the secure element.

System manufacturers have the option to impose usage restrictions on data within secure storage to bolster control. For instance, a key might be constrained for use solely in cryptographic operations, never exiting the secure element, thus safeguarding against potential leaks.

Keys for secure storage may be deployed through secure provisioning, created within the secure element, or negotiated by the application. These measures ensure that the keys, and the data they protect, remain impervious to unauthorized access.

## Secure Boot

The QPG6200's multi-stage secure boot (**Figure 3**) process ensures that only authorized software runs on the device.

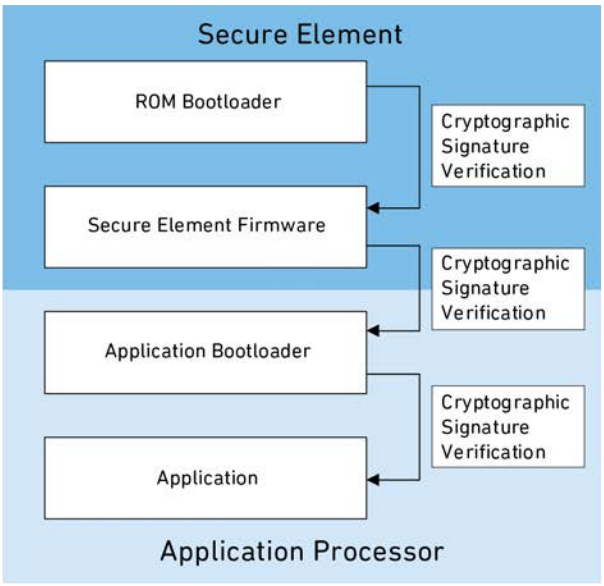




Figure 3: Secure boot overview.

Upon startup, both the application processor and real time processor are initially inactive, held in reset mode. The boot process begins with the ROM bootloader inside the secure element. Running on the secure processor, the ROM bootloader kickstarts the secure boot sequence. Its primary role is to serve as an immutable root of trust, anchored in hardware, and verifies the ECDSA signature over the secure element firmware. If this verification is successful, control of the secure element is transferred to the secure element firmware. Additionally, the ROM bootloader is equipped to handle secure upgrades to the secure element firmware, ensuring the device's security integrity from the outset.

The secure element firmware enables the security functions of the secure element and authenticates the application bootloader using the ECDSA signature. Once authenticated, the application processor is activated to run the verified application bootloader. The secure element firmware remains vigilant, processing security-related requests from the application processor, such as executing hardware accelerated cryptography and managing secure storage. It is also tasked with upgrading the application bootloader.

Following this, the application bootloader on the application processor takes over, verifying the ECDSA signature of the application using the secure element's security services. A successful verification hands off control to the application, which then executes on the application processor. In addition to this, the application bootloader manages updates to the application.

## Secure Upgrades

### Secure Element Firmware

The chip manufacturer may provide upgrades for the secure element firmware. These upgrades come in the form of opaque binaries. These binaries are encrypted and cryptographically signed by Qorvo. The application is responsible for downloading these upgrades in a timely matter. When an upgrade has been downloaded, the application must trigger the upgrade by sending a command to the secure element.

### Application Bootloader

The system manufacturer may provide upgrades for the application bootloader. These upgrades come in the form of encrypted and cryptographically signed binaries. The application is responsible for downloading these upgrades in a timely matter. Once the upgrade is downloaded, the application must trigger the upgrade by sending a command to the secure element.

### Application

Application Upgrades are carried out by the application bootloader, which gives the system manufacturer maximum flexibility when implementing a bespoke upgrade mechanism. A reference implementation is included in the QPG6200's SDK and covers the application bootloader and the application. The application is responsible for downloading the encrypted and signed upgrade image. It then instructs the application bootloader to carry out the upgrade and resets the device.

## Secure Debug

Developers can access the application processor's debug features using JTAG or SWD interfaces. These debug facilities are, by default, connected to a specific set of pins for ease of use, facilitating rapid development. However, this standard setup is not secure. If left unrestricted, the debug port could potentially compromise the security of the application processor. Therefore, it is crucial to secure the debug port before devices are shipped to customers.

The system manufacturer may choose one of two methods of securing debug access:

- Permanently close the debug port
- Enable secure debug

**Please note:** Configuring either of these two options is an irreversible action.

When secure debug is enabled, the debug port provides access to the debug challenge interface (DCI). The developer can request a one-time random challenge from the chip. The challenge, along with a command to unlock debugging of the application processor, must then be cryptographically signed by the user. Sending back this command and the signature unlocks full debug capabilities of the application processor. This process ensures that parties in possession of the private key can securely gain access to debug capabilities.

## Secure Provisioning

Provisioning is the process by which the system manufacturer initializes the security parameters of the QPG6200. These include, at least:

- The application bootloader and application signature verification key (ECDSA public key digest)
- The application bootloader and application upgrade encryption key (AES-256 key)
- The secure debug unlock command signature verification key (ECDSA public key digest)

Optionally, the provisioning process may include:

- Initial application bootloader
- Initial application
- Application specific security parameters, such as but not limited to:
  - Matter device attestation certificate (DAC) and attestation private key
  - Other application specific keys
    - These can be provisioned directly to secure storage

Provisioning data is bundled and encrypted with AES-GCM and the system manufacturer provisioning key which is unique to each system manufacturer. This protects the confidentiality of the provisioned data as well as its authenticity and simplifies security requirements for the production facility.

## Device Attestation

Attestation is a security process that allows an external verifier to confirm the authenticity of a device or system. Typically, the verifier sends a challenge, often a random string of data, to the device. The device then signs this data with its unique secret key and returns the signature, along with a certificate that includes the public key corresponding to the private key, to the verifier. This allows the verifier to verify both the signature and the authenticity of the certificate.

The QPG6200 is equipped to support this attestation process. It can authenticate the silicon chip itself, as well as offer application-level attestation mechanisms, such as those defined by the Matter protocol using a device attestation certificate (DAC). Each QPG6200 chip has a unique secret key embedded at the silicon level. Qorvo cryptographically signs the public counterpart of this key. System manufacturers can then use Qorvo's certificate chain to validate both the signature and the certificate, ensuring the authenticity of the Qorvo silicon.

While this is valuable information to the system manufacturer, attestation of a product that embeds the QPG6200 should validate the whole product, not just the silicon. Different standards recommend various attestation methods. The QPG6200 supports essential attestation requirements, including third-party device attestation (non-VID scoped PAA) and system manufacturer (VID scoped PAA), which have been defined specifically for Matter protocol compliance.

## Hardware Accelerated Cryptography

The Secure Element contains hardware that accelerates cryptographic operations. The major algorithms are highlighted below. A full list can be found in the QPG6200 datasheet.

Hardware cryptographic acceleration algorithms:

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

The AES engine and the public key (PK) crypto engine are protected against side channel analysis attacks. These countermeasures block attackers' efforts to infer sensitive key material through timing analysis or power consumption observation.

## Conclusion

Qorvo is dedicated to providing secure, certified solutions that mitigate risks and reduce costs for OEMs. The QPG6200 embodies this commitment, with a security architecture that meets critical industry standards and cybersecurity regulations for IoT devices. Its robust suite, highlighted by the secure element, offers comprehensive lifecycle management and advanced security features, achieving PSA Certified Level 2 status.

The complete SDK, hardware development board, and detailed documentation that accompany the QPG6200 simplify the intricacies of security design. This ensures OEMs can efficiently integrate state-of-the-art security measures, maintaining market competitiveness and readiness for protocols like Matter. The QPG6200 is not just a product, but a pathway to leadership in the next generation of IoT innovation.