Ambiq SecureSPOT® Feature Comparison Guide

www.ambiq.com
sales@ambiq.com
+(512) 879-2850

6500 River Place Boulevard, Building 7, Suite 200, Austin, TX 78730
A-SOCAMQ-QGNA01EN v1.1 October 2022

	SecureSPOT 1.0	SecureSPOT 2.0	
Security Features	• Secure Boot[1] • Extensible to Custom Secondary Boot Loader[2] • Flash Protections (copy and write protection) • Secure Upgrade (OTA) • Wired Interface Support • Key Revocation • Anti-Rollback • Encryption Support for Updates • Recovery (factory reset) • Hardware Entropy • Debugger Lockout Support	• Secure Boot • Extensible to Custom Secondary Boot Loader • Flash Protections (copy and write protection) • Hardware Cryptographic Acceleration • Hardware Keys (Inaccessible to software) • Secure Upgrade (OTA) • Wired Interface Support • Key Revocation • Anti-Rollback • Encryption Support for Updates • Recovery (factory reset) • Hardware Entropy • Security Lifecycles • Secure Debug • OTP Support • Secure Key Storage	
Supported Products	**Apollo3 Family**	**Apollo4 Family**	**TrustZone[3]**
Secure Boot[4,5]	Leverages secure boot loader (SBL) to establish initial firmware authentication in Apollo3 Blue Plus SoCs.	Enhances security with hardened secure boot loader, hardware crypto to perform authentication, and physical memory isolation for critical assets.	Requires secure boot to establish its root of trust. Manages secure vs non-secure operating modes within the CPU or uses physically separate security processor.
Secure Firmware Update/ Security OTA[5]	Leverages secure boot loader to perform firmware authentication, decryption, and installation with recovery.	Enhances security with hardened secure boot loader, hardware crypto to perform authentication, and physical memory isolation for critical assets.	Isolates the OTA process and performs runtime firmware updates. Secure partitions allow isolation for critical assets.
Secure Key Management[5]	Utilizes private keys to access key bank during runtime.	Enhances key storage security through hardware crypto (physical isolation), as well as extended key bank access to customer and Ambiq-specific keys.	Isolates key storage access.
Secure Debug	Provides dedicated hardware to lock/unlock various debug capabilities. These locks are either hard one-way locks or soft locks for temporary protection.	Enables crypto hardware plus dedicated hardware to support secure lifecycle states and debug feature enables/disables that can be updated based on debug certificates.	Facilitates access to secure and non-secure debug or non-secure debug only. Separate secure and non-secure debug credentials.
Memory Protection	Provides dedicated hardware to lock various non-volatile memory assets within the SoC. Customers can leverage the MPU to enforce memory protection, but Apollo3 and Apollo4 Family products do not support differentiation between secure and non-secure operating modes.		Leverages TrustZone security extensions and hardware within the CPU to provide secure vs non-secure continuous run-time memory protections.
Secure Peripherals/ Secure I/O	The Apollo3 and Apollo4 Family products do not support secure peripheral or secure I/O on dedicated hardware.		Leverages TrustZone security extensions and SoC security attributes plus dedicated hardware to restrict access to certain peripherals or I/O.
Trusted Execution Environment (TEE)	The Apollo3 Family supports this only for the secure boot loader. There is currently no support for isolating secure vs non-secure runtime services on the same processor.	Same as Apollo3 Family except additional physical isolation for certain security services in the hardware crypto block is supported.	Supports secure and non-secure operating modes within the CPU. This allows devices to support isolation-specific security services running on the same processor as other potentially untrusted applications. This is generally needed to support third-party applications on a device.

[1] SBL requires review of the application before security feature support may be provided. Contact sales@ambiq.com for more information.
[2] The framework supports customers to write a secondary bootloader which can support external flash, along with a host of other items (e.g., USB, eMMC).
[3] Security features are SoC implementation specific.
[4] See the FAQ for product specific SBL support.
[5] Takes advantage of temporal processing isolation.

Ambiq SecureSPOT® Feature Comparison Guide

Frequently Asked Questions

1	**Q:**	**Does SecureSPOT provide as much security as TrustZone?**
	A:	Both solutions offer features used to create secure products: • Secure Boot • Secure Firmware Update / Secure OTA • Secure Key Management • Secure Debug • Memory Protection TrustZone can optionally provide a secure hardware operating environment and the ability to differentiate security operating modes within the CPU. • Connection of secure peripherals • Supporting execution of third-party apps on the device
2	**Q:**	**Will Apollo3 or Apollo4 products support TrustZone?**
	A:	TrustZone is a hardware capability requiring a Cortex-M33 or later and cannot be incrementally added to existing products.
3	**Q:**	**What level of PSA certification do Apollo SoCs deliver?**
	A:	Apollo3 Family: Not PSA Certified. Apollo4 Family: PSA Level 1 Certified.
4	**Q:**	**Is secure boot a feature on all Apollo products?**
	A:	Apollo3 Family: • Apollo3 / Apollo3 Blue: Secure boot is not supported. • Apollo3 Blue Plus: SBL requires review of the application before security feature support may be provided. Contact sales@ambiq.com for more information. Apollo4 Family: • Secure boot is supported by default on all Apollo4 Family products.