ARM Product News Summary

Get your design security right with ARM TrustZone CryptoCell-312

- ARM TrustZone CryptoCell-312 allows design teams to get security right, freeing up tens of man years to focus on differentiation
- Along with TrustZone for ARMv8-M, CryptoCell-312 enables the formation of a security platform , allowing relying parties to establish trust in services and devices
- CryptoCell-312 provides a rich set of platform security services, enabling brand-name protection, R&D investment monetization and various use cases across all IoT markets

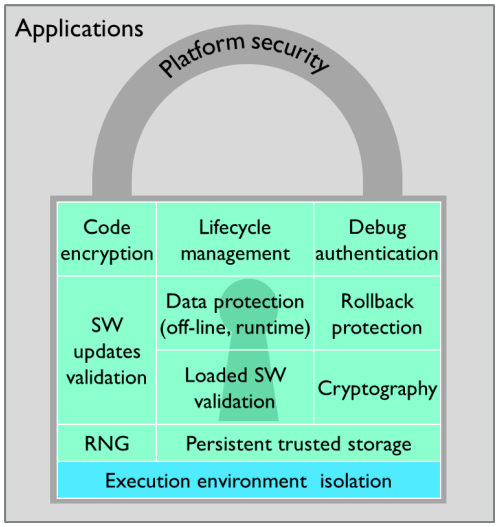
Challenge and or opportunity

With the introduction of IoT there are lots of things to think about. IoT nodes will power products all over the world therefore they need to be distributed remotely, have a long battery life and remain secure for their entire lifecycle. To achieve this, lots of stakeholders need to be involved – the real challenge is to maintain innovation whilst not compromising security.

All the different stakeholders in the ecosystem want to protect their investment and reputation, meet the security requirements needed for different use cases while maintaining high user satisfaction. The new CryptoCell-312 can balance the right security measures (addressing the threat model) with the needed usability (so user experience is not impacted), while maintaining the overall power and area budget.

Product overview

CryptoCell-312 is a comprehensive security solution, serving multiple use cases and allowing relying parties to establish trust in a broad spectrum of power and area constrained devices.



The certifiable CryptoCell-312 solution comprises HW and on-chip SW, provided in source code format. It also includes a rich set of off-device tools, addressing various manufacturing and ecosystem enablement processes. CryptoCell-312 supports the following functional features:

- Asymmetric and symmetric cryptography
- Lifecycle state management
- Roots-of-trust access policy enforced by HW means
- A device roots-of-trust ownership model allowing multiple entities to own different trust anchors, removing the need for default trust between entities along the value chain
- Random Number Generator (RNG)
- Key provisioning, management and isolation
- SW image validation and optional decryption both at boot time and update time
- Persistent and volatile data protection
- Secure debug / DFT

- In-factory and in-field features enablement and disablement

Together with TrustZone for ARMv8-M, CryptoCell-312 can form a security platform providing cryptographic services and platform security services, tailored to deal with different needs and threat models.