



Discretix CryptoCell®

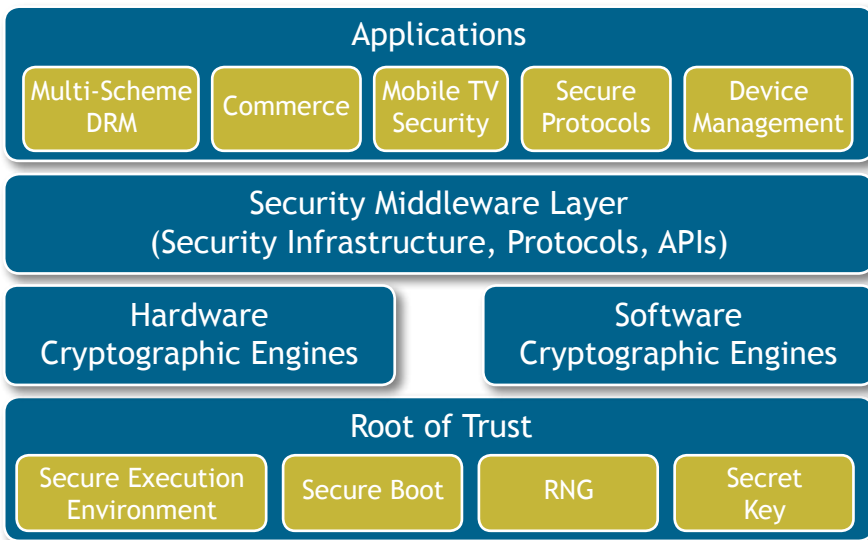
A Trusted Environment for Mobile Applications

CryptoCell is a complete embedded security platform for mobile devices. It provides an outstanding level of security, while overcoming the challenges of performance, power consumption and silicon footprint. Its flexible architecture offers semiconductor vendors and device manufacturers a robust solution that can be tailored to meet today's demanding mobile security requirements. CryptoCell can be deployed across multiple platforms and operating systems to secure a broad range of mobile applications.

Securing a Mobile Evolution

Today's mobile devices support a broad range of applications and services including content download, enterprise applications, commerce and mobile TV. Discretix pioneered mobile security to enable these applications and protect this new generation of devices from a growing range of threats.

Integrated Architecture - Robust Protection



Key Benefits

- Complete security platform enabling customized solutions for mobile devices
- Compliant with all industry standards and verified by external labs and standard bodies
- Field and silicon proven solutions-deployed in numerous handsets and environments
- Ensures trust to drive revenue generating applications for both open and closed systems
- Easily integrated, ensuring lower total cost of ownership
- Robust cryptographic core, countermeasures and protection of device assets
- Tight integration of the solution's components to ensure optimal security
- Minimal gate count and power consumption
- Secure Execution Environment provides a safe environment for open operating systems

Discretix Industry Leadership

Discretix is dedicated to delivering innovative solutions to the complex and ever-changing mobile security market. This specialized expertise allows Discretix to provide chipset and device vendors with a complete security platform that is ready to deploy, easily integrated and future-proof. Licensed by industry leaders worldwide, Discretix' solutions are field proven.

For the past three years, Discretix was ranked by Gartner among the largest vendors of encryption semiconductor IP.

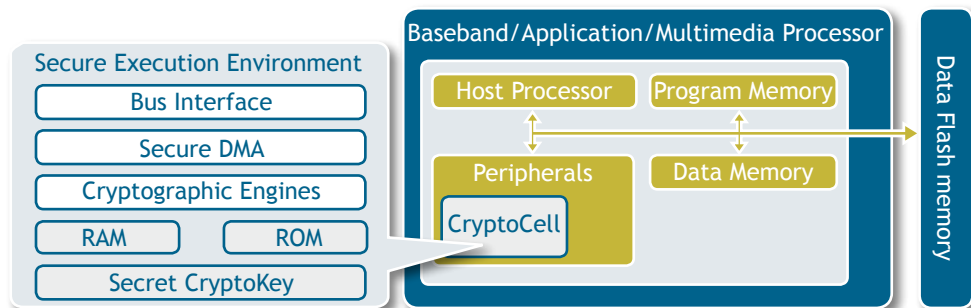
Discretix actively contributes to industry forums and standardization bodies to ensure compliance and certification:

CryptoCell® Technical Overview

The CryptoCell platform is deployed as an integral part of the device to deliver the highest level of security and performance. The solution's multi-layered architecture ensures that all components of the device and its applications are secured. CryptoCell is delivered as a tested and ready-to-implement platform.

| | | |
|---|--|---|
| Applications & Toolkits Layer | Essential security components for applications such as DRM, Mobile TV, FOTA, SIM Lock, and IPSec (VPN). To ensure secure implementation, these toolkits are integrated with the Discretix middleware and hardware layers. | Attack-Resistant Cryptographic Core Discretix deploys unique and patented mechanisms to provide robust protection against: <ul style="list-style-type: none">Timing Attacks (TA)Fault Attacks (FA)Power Analysis Robust countermeasures span across all layers of the solution architecture. |
| System Security Middleware Layer | The security middleware layer provides secure access to the Hardware cores and serves as a robust security infrastructure for the application layer. It also provides secure storage, cryptographic schemes, key management and certificate management across multiple platforms and operating systems. The secure boot mechanism supports different stages in the device life cycle and completes the system security solution. | |
| Hardware Core Layer | The hardware layer is delivered as IP for easy integration into ICs. Discretix patented technology implements the standardized cryptographic algorithms in a way that minimizes gate count and power consumption while maximizing performance and security. | |
| Software Cryptographic Algorithms (optional) | The CryptoCell platform includes a full software implementation of cryptographic algorithms. Optimized for the mobile environment, the cryptographic libraries allow the manufacturer a wide range of implementation options. | |

CryptoCell Hardware Architecture



The CryptoCell family of products offers optimized solutions for every mobile handset.

| Feature | Components | Benefit | |
|----------------------------|------------------------------|---|---|
| Flexible system design | Slave bus interface | Standard bus interface | |
| | DMA interface | Off-loading system processor | |
| | FIFO interface | High-speed streaming with no host intervention | |
| | API | Multiple standard options for various OS: Discretix CRY5 API; Symbian Cryptography Library API; Linux Cryptographic Library; Windows Mobile CAPI | |
| Cryptographic capabilities | Cryptographic cores | State-of-the-art high throughput and ultra-small engines Public Key Algorithms: RSA; ECC; DH Symmetric Algorithms: AES; DES/3DES; RC4 Hash Algorithms: MD5; SHA1; SHA256/384/512; HMAC Random Number Generation: Deterministic; Non-deterministic | |
| | | Secure Boot | Prevents modification or replacement of software code images residing in non-volatile storage |
| | | Secure Storage Enabler | Protects confidentiality and integrity of data items in off-chip non-volatile memory |
| | | Key Manager | Handles all key material internally, never exposing unencrypted keys outside CryptoCell |
| | | Secure Debug | Prevents software-based debug and test attacks |
| Open system security | Life Cycle | Enables and disables security features throughout the life span of the device | |
| | Secure execution environment | Runs protected applications in a secured domain | |
| | Multi-Master Manager | Facilitates domain separation by preventing non-secure software attacks initiated from one domain to affect other domains | |
| Performance | Memory Watcher | Supervises access to system memory, enabling flexible run-time allocation of memory space to the various system masters | |
| | Multi-Flow Manager | Enables smart time-sharing of the Cryptographic Cores, offloading host from management tasks | |
| | Master bus interface | Off-loading system processor | |
| | Power Management | Prolongs battery life | |