



## Discretix CryptoFlash™

### Embedded Security for Flash Memory

CryptoFlash is a complete security platform for Flash memory devices such as Flash cards, USB Flash drives, embedded Flash memory, high capacity SIM cards and hard disk drives. It offers an outstanding level of security, while overcoming the challenges of performance, power consumption and silicon footprint. CryptoFlash's flexible architecture offers semiconductor vendors and device manufacturers a robust solution that can be tailored to meet today's demanding mobile security requirements.

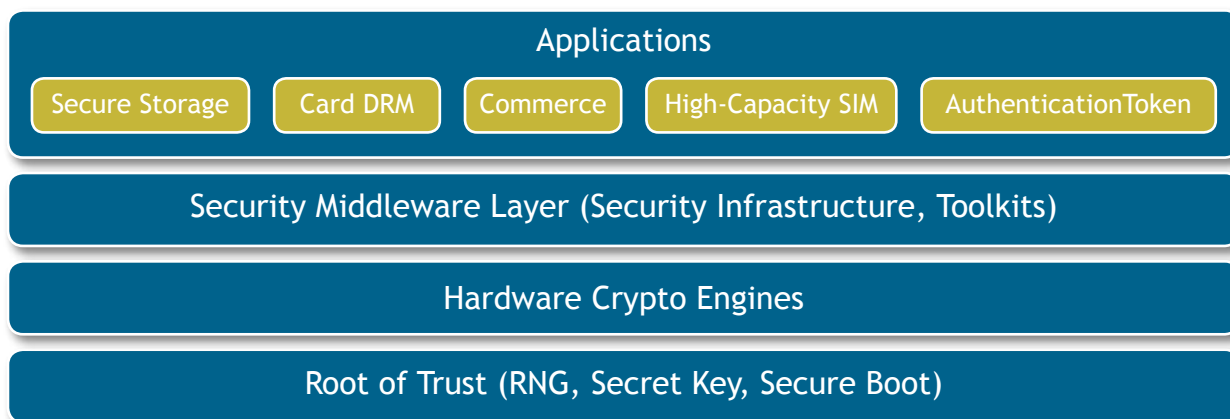
### Countering Threats, Securing Opportunities

CryptoFlash is a driving force behind the expansion of Flash memory into new markets and applications. New applications ranging from preloaded content to wireless telephony are exposing the device and its contents to a host of new opportunities and threats. CryptoFlash provides the necessary security foundation for the ongoing development of the market.

### Key Benefits

- Field proven in millions of devices and multiple form factors
- Verified by external labs and standard bodies
- Fully complies with requirements posed by the MMCA, SDA and OMA DRM Secure Removable Media (SRM)
- Rich security middleware layer including protocols, services and APIs
- Application toolkits enable developers to easily incorporate security into applications
- Cryptographic co-processor provides a solid foundation upon which the security solution is based
- Hardware based root of trust
- Secure implementation ensures only legitimate code can be loaded
- Attack resistant Secure Storage
- Anti-reflash protection

### Integrated Architecture - Robust Protection



### 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.

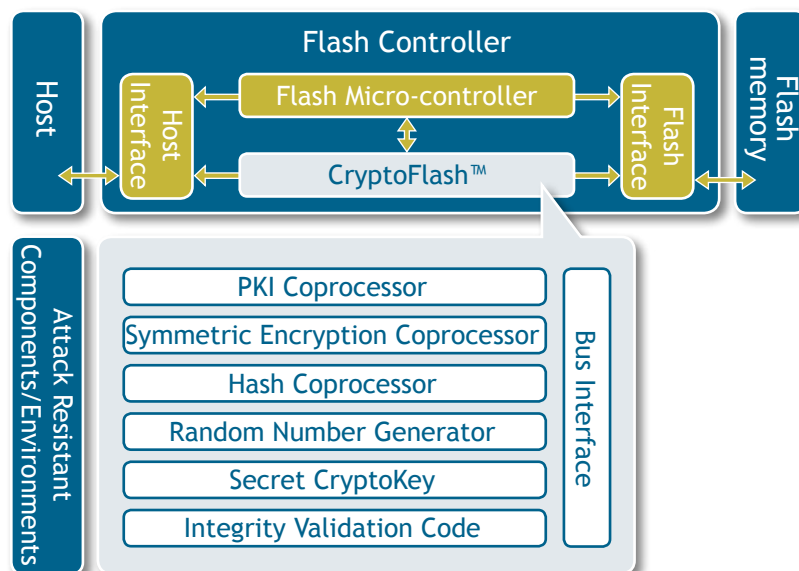
For the past three years, Discretix was ranked by Gartner among the largest vendors of encryption semiconductor IP.

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

# CryptoFlash™ Overview

CryptoFlash's multi-layered architecture ensures all components of the device and its applications are secure. Discretix has registered multiple patents for the implementation of cryptographic algorithms in a way that minimizes gate count and power consumption while maximizing performance and security.

Applications & Toolkits Layer	Essential toolkits for secure implementation of applications such as Digital Rights Management, Device Management and Secure Authentication.	<b>Attack-Resistant Cryptographic Core</b> Discretix deploys unique and patented mechanisms to provide robust protection against: <ul style="list-style-type: none"> <li>▪ Physical probing</li> <li>▪ Side channel attacks</li> <li>▪ Timing attacks</li> <li>▪ Fault analysis</li> <li>▪ Simple power analysis</li> <li>▪ Differential power analysis</li> <li>▪ Power consumption balancing</li> <li>▪ Fixed time-per-operation (operand agnostic)</li> </ul> These countermeasures span across all layers of the solution architecture.
System Security Middleware Layer	A suite of software modules including APIs and security protocols and services to reduce time-to-market and ease integration.  Enables secure access to the low level cryptographic functions, algorithms and the Random Number Generator. Implementation requires a minimum amount of code and run-time memory.	
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.	



Feature	Components	Benefit
Cryptographic capabilities	Cryptographic core	State-of-the-art high throughput and ultra-small engines Public key algorithms: RSA, ECC, DH Symmetric algorithms: AES, DES & 3DES Hash algorithms: SHA1, SHA256/384/512 Random Number Generation: Deterministic and Non-deterministic
Asset protection	Secure Boot	Prevents modification or replacement of software code images residing in non-volatile storage
	User or device authentication	Strong authentication mechanism based on public key algorithms
	Integrity Validation engine	Ensures the integrity of code and data
	Life Cycle	Enables and disables security features throughout the life span of the device
	Secure Storage Toolkit	Protects confidentiality and integrity of data items in off-chip non-volatile memory
Open system security	TrustedFlash Toolkit	Provides TrustedFlash infrastructure
	Secure execution environment	Runs protected applications in a secured domain
Performance	On-the-fly processing	Provides on-the-fly encryption/decryption at rates exceeding USB 2.0 without Flash controller intervention
	Sector Optimization	Optimizes Flash memory sector structure
	Power Management	Prolongs battery life