



Security Platforms

Network Security



Storage Security

Content Protection



Security Modules

Cryptographic Libraries



# Embedded Security Market

## Your Embedded Security Technology Partner

The rapid growth of embedded computing along with demand for connectivity, open systems and multimedia are fueling the need for robust security. By enabling a broad range of applications and business models, while addressing the threats of theft and hacking - embedded security has become crucial to the continued development of the market. Embedded security requirements cut across a wide range of markets, including mobile devices, storage, networking, multifunction printers, consumer electronics, automotive and industrial machinery.

## Security Platforms

---

A range of embedded security platforms for processors and devices providing comprehensive system, application and content security.

## Network Security

---

High performance acceleration for network security protocols (IPSec).

## Storage Security

---

Comprehensive “in-storage” data protection solution for Flash cards, USB Flash drives, SSD, HDD and storage interface bridges.

## Content Protection

---

A flexible and easy to integrate content protection client for device vendors and service providers, supporting all major DRM schemes and operating systems; fully compliant with industry standards.

## Security Modules

---

Providing the key security building blocks required to address a broad range of applications and markets.

## Cryptographic Libraries

---

Hardware and software libraries offering an optimized implementation of cryptographic algorithms suited to all types applications.

# Security Platforms

The most comprehensive and widely deployed embedded security solution.

## ■ CryptoCell® Security Platforms - Introduction

CryptoCell® is a complete embedded security platform for a wide range of processors, devices and embedded systems which require a strong security infrastructure. While overcoming the challenges of performance, power consumption and silicon footprint, CryptoCell®'s flexible and modular architecture provides an exceptional level of security. CryptoCell® is deployed across multiple platforms and operating systems to secure a broad range of applications.

Comprised of a hardware sub-system and a middleware layer, CryptoCell® has been widely deployed by many tier-1 customers in various applications, environments and configurations.

The CryptoCell® platform is provided in three main configurations:

- **CryptoCell® Platform Security** – Ensures platform integrity and provides a complete set of cryptographic accelerators and an easy-to-use secure storage solution.
- **CryptoCell® Application Security** – A secure execution environment (SEE) sub-system to ensure trust for open operating systems and selected software applications.
- **CryptoCell® Network Security** – A secure execution environment with built-in packet engine providing acceleration for common networking security protocols (e.g. IPSec) while ensuring trust for SoCs.



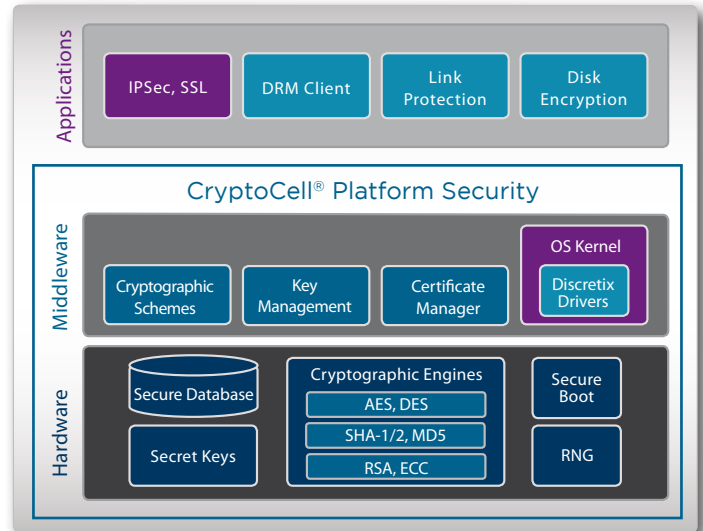
## ■ CryptoCell® Platform Security (PS)

CryptoCell® PS is designed for systems that use only trusted applications (e.g. RTOS-based devices). CryptoCell PS provides a root of trust, cryptographic acceleration, secure storage and common security building blocks.

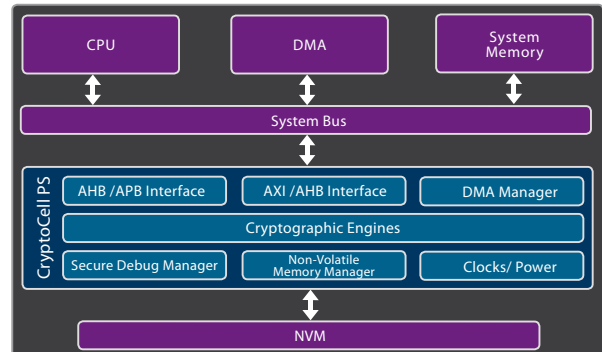
CryptoCell® PS is a multi-layered hardware and software solution. CryptoCell® PS includes state-of-the-art cryptography ciphers such as public key algorithms, symmetric encryption and hash functions at various modes and key sizes. The rich layer of security middleware provides support for various algorithms optimized for embedded applications. In addition, it provides attack-resistant secure database using standard external non-volatile memory. With industry standard connectivity such as AMBA AHB and APB interfaces and easy-to-use APIs, the low-power design easily integrates as a co-processing unit into baseband and application processors. The rich middleware includes highly optimized, performance-driven cryptographic libraries, a robust and flexible secure boot, secure storage, secure debug and support for common device management software toolkits.

### Features

- High throughput hardware cryptographic engines and random number generators
- Compact secure boot preventing unauthorized code modification; supporting software update with a boot load hierarchy
- Fault-tolerant secure database providing confidentiality and data integrity
- Robust key management handling all key material without exposing unencrypted keys
- Secure debug preventing software-based debug and test attacks
- High throughput for multimedia processing
- API support for various operating systems
  - Linux Cryptographic Module
  - Windows Mobile CAPI
  - Discretix APIs
- Easily integrated as a system-on-chip (SoC) peripheral
- Silicon-proven on multiple embedded systems and configurations



### CryptoCell® Platform Security Hardware Architecture



# Security Platforms

## ■ CryptoCell® Application Security (AS)

Designed for application processors, CryptoCell® AS is built to meet the need for a secure execution environment (SEE) for software applications without compromising the user experience. SEE provides robust execution and processor offloading for computationally-intensive cryptographic operations and critical security functions.

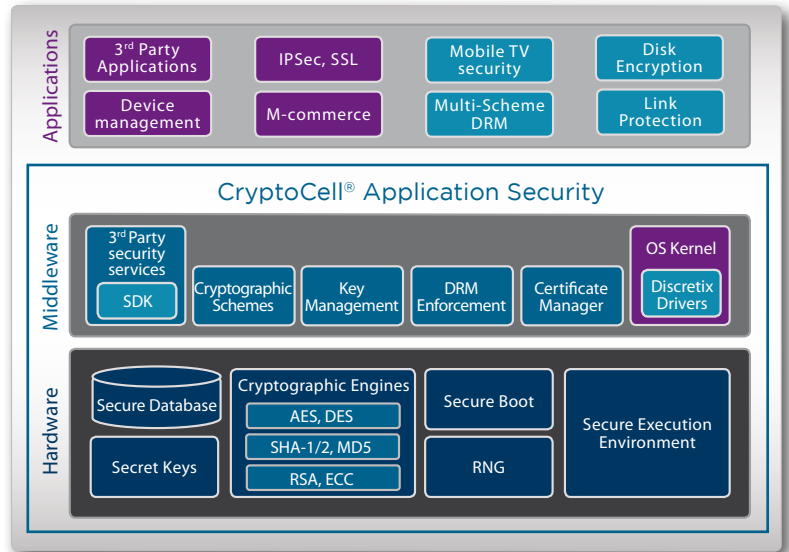
CryptoCell® AS includes a variety of asset protection capabilities such as secure boot, state-of-the-art secure storage capabilities, secure time management, key management and certificate handling.

Its APIs are integrated to common OS crypto libraries such as Linux and Moblin, providing acceleration to existing applications without any modification to the code.

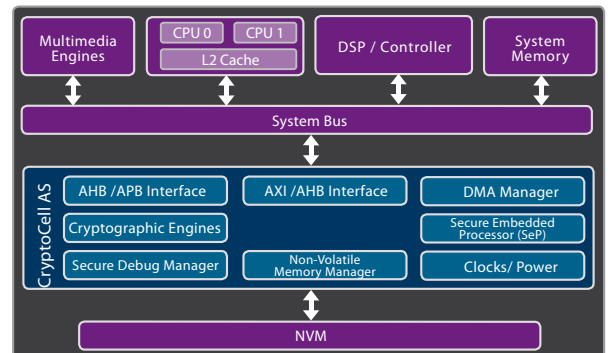
CryptoCell® is pre-integrated with common security applications requiring support for complex data flow and high throughput while conforming to industry standard robustness rules. The pre-integrated security applications include link protection as well as commonly used DRM schemes. An important feature of the CryptoCell AS is the inclusion of a full-featured SDK enabling 3rd parties developers to create their own security applications for the CryptoCell secure execution environment.

### Features

- High throughput supporting HD content
- Execution of protected application in a secured domain
- Security services for 3rd party application developers
- Pre-integrated with common DRM schemes including WM-DRM, OMA-DRM and CPRM
- Hardware support for synchronous and asynchronous modes of operation
- Asset protection functions executed in the SEE
- Comprehensive and robust symmetric and asymmetric hardware cryptography
- Rich security middleware integrated with common operating systems
- Fault-tolerant and high-performance secure storage
- Ultra-small and flexible secure boot
- Silicon proven and deployed in a variety of embedded systems
- Supports various power management schemes



### CryptoCell® Application Security Hardware Architecture





## ■ CryptoCell® Networking Security (NS)

CryptoCell® NS provides networking security capabilities in addition to all of the capabilities offered by the CryptoCell® AS solution. Typical network security protocols are based on specific data structures (e.g. packets) and require processing overhead that can be split into two components:

- Fixed overhead – Addressing packet metadata identification, anti-replay and other parameters, unrelated to the packet size.
- Variable overhead – Packet integrity and confidentiality, in proportion to the packet size.

CryptoCell® NS addresses fixed and variable overhead processing for a variety of network security protocols including IPsec, SRTP and SSL/TLS. It is ideal for mitigating platform and applications security risks while protecting and accelerating the network communication stack.

CryptoCell® NS includes hardware and firmware components to significantly accelerate the security protocols. The one-path data processing mechanism (for confidentiality and integrity) and efficient context switching (a critical requirement for packet processing engines), provides efficient data packet processing

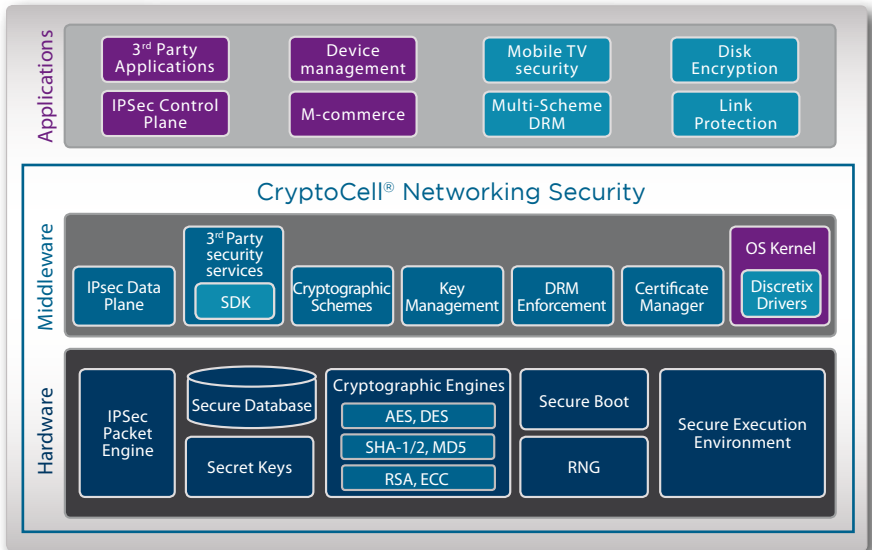
CryptoCell NS can be configured based on a combination of required performance and gate count. Hardware resources requiring security-related packet processing can be shared with all of the CryptoCell® AS solution capabilities.

CryptoCell® NS can be easily integrated with existing OS communication stack or can be provided with full software stack implementation supporting the latest RFCs for both control and data planes.

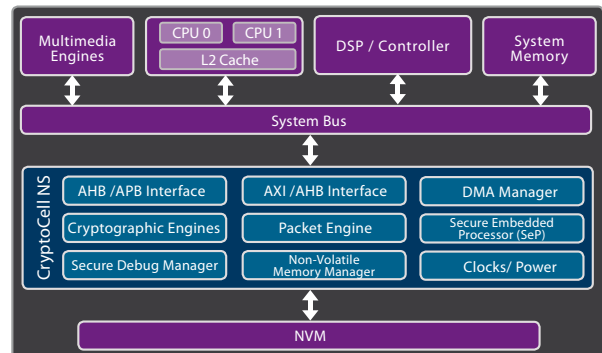
### Features

- Fixed and variable overhead processing for a variety of network security protocols
- Mitigates platform and application security risks
- Protects and accelerates the network communication stack
- One-path data processing mechanism and efficient context switching
- Flexible configuration for desired throughput
- Easily integrated with existing OS communication stacks
- Optional software stack implementation supporting the latest RFCs

\*\* For performance figures see the IPsec accelerator section on page 9.



### CryptoCell® Network Security Hardware Architecture



# Security Platforms



Feature	Components	Benefit	CryptoCell		
			PS	AS	NS
Asset protection	Secure boot	Prevents modification or replacement of code image. Supports boot load hierarchy, field updates with high performance and small code footprint	+	+	+
	Secure database	Protect confidentiality and integrity of data items in off-chip non volatile memory with high performance in retrieval and update of objects	+	+	+
	Key manager	Handles all key material internally, never exposing unencrypted keys outside of CryptoCell	+	+	+
	Secure debug	Prevents debug and test attacks; supports multiple debug domains	+	+	+
	Life cycle management	Enable and disable security features throughout the lifespan of the device	+	+	+
	Secure real-time clock	Supports updates and retrieval of system clock and enforces time sensitive objects	-	+	+
	Pre-integrated DRM (multiple schemes)	Supports complex data flows conforming to robustness compliancy for right objects and license management	-	+	+
Open system security	Secure Execution Environment	Runs protected applications in a secured domain	-	+	+
	3rd party software development kit (SDK) and rich libraries	Security services for 3rd party application developer providing protection of critical assets	-	+	+
	Memory watcher	Supervises access to system memory, enabling flexible run-time of memory space of the various system masters	-	+	+
Cryptographic capabilities	Cryptographic engines	State of the art, high throughput and ultra small engines Public key algorithms: RSA, ECC, D-H Symmetric algorithms: AES, 3DES, RC-4 Hash algorithms: MD-5, SHA-1, SHA-2 and HMAC Random number generators: TRNG and PRNG	+	+	+
Performance	Support asynchronous and synchronous mode of operation	Integrated with symmetric and asymmetric multi-processing execution	-	+	+
	High throughput	Support high definition audio and video streaming rates	-	+	+
	Power management	Support various power modes	+	+	+
Flexible system design	Slave and master bus interfaces	Standard bus interface integrated as a peripheral	+	+	+
	APIs	Multiple options: Discretix APIs; Linux and Moblin Crypto Module ; Windows Mobile CAPI	+	+	+
Protocol level acceleration	Packet engine	IPSec, SRTP and SSL host processor offloading	-	-	+

# Network Security

## Efficient acceleration of network security protocols along with device security

### ■ IPsec Accelerator

Internet protocol security (IPsec) provides security at the network layer of the protocol stack. Traditionally part of network equipment, IPsec is increasingly deployed in devices such as multifunction printers, femtocell access points and mobile phones. More recently IP networking standards are being extended into new device classes such as utility meters and vehicles. Security is required to protect data-at-rest in these devices and the data-in-transit on these networks, and is following the IP-based networking standard as it expands into these markets.

The transition to all IP networks and packet-based communication infrastructure, are underpinning the need for IPsec hardware acceleration across the gamut of connected devices. Moreover as bandwidth increases, dedicated processing power is needed to meet the ever-growing throughput and offload requirements of the host processor.

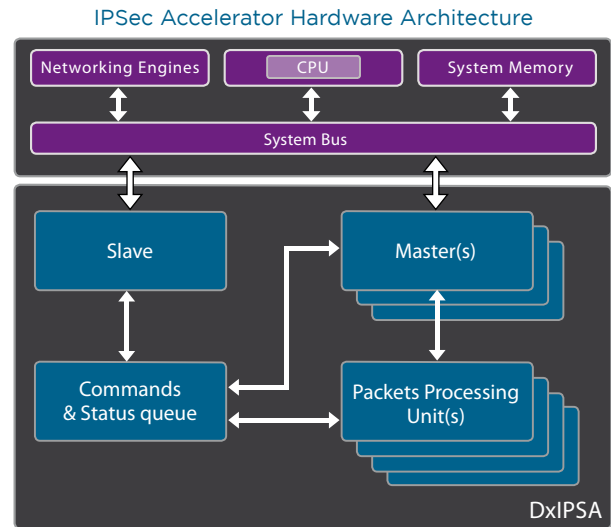
The Discretix IPsec Accelerator (DxIPSA) provides efficient processing of network security protocols as well as device security and is comprised of the following system elements:

- Software client for data plane processing
- Control plane software component (handling security associations)
- “Lookaside” hardware engine for host processor offloading and power consumption minimization

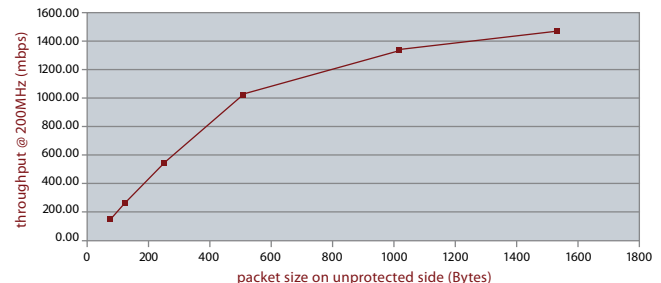
### Highlights:

- Full IPsec solution (hardware, firmware and software) adhering to the latest RFCs
- Efficient design resulting in minimal gatecount, bus traffic and power consumption
- Design scalability allowing optimal power and performance configuration

The Discretix packet engine can be integrated with the Discretix CryptoCell®, offering platform security capabilities such as secure boot, secure debug and secure database assuring device security and integrity.



### Sample Performance\*\*



\*\* Figures are for single cryptographic processing pipe, single bus master port (32-bit data interface), no bus latency, inbound ESP in tunnel mode (AES CBC with 128 bits key and HMAC-SHA1). DxIPSA is running at 200MHz and host processor is running at 1GHz.

# Storage Security

Optimized and efficient storage protection – protect your data at source

## ■ CryptoFlash®

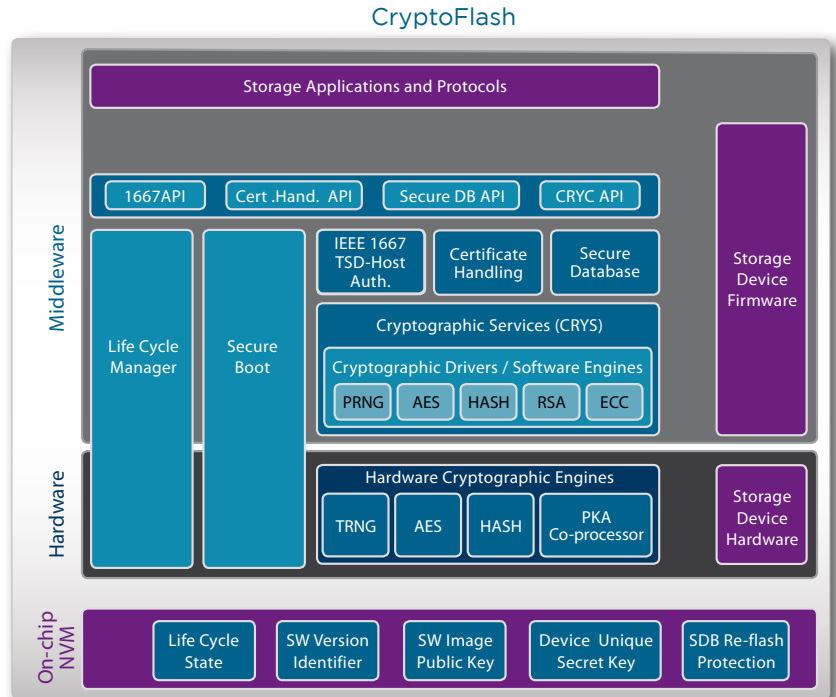
Removable storage devices (e.g. USB flash drives and SD Cards) allow large amounts of data to be easily transported between computers and between work and home. This convenience comes at the risk of data leakage and theft. Moreover as content delivery shifts from optical media to flash-based storage, content protection is required at the device level. Other markets such as healthcare, commerce, e-Payment and banking also require flash-based security as they transition their services to solid state storage devices.

CryptoFlash® is a complete security platform for removable storage devices such as flash cards and USB flash drives. It offers semiconductor vendors and device manufacturers a comprehensive solution that can be tailored to meet today's demanding mobile security requirements.

CryptoFlash® offers an outstanding level of security, while overcoming the challenges of performance, power consumption and silicon footprint. It includes cryptographic co-processors enabling high-performance cryptographic operations, as well as a set of sophisticated security features enabling secure storage and a high-level of robustness.

## Key Benefits and Highlights

- Security foundation for protection of user information and content
- Field-proven in millions of devices and multiple form factors
- Rich security middleware layer including protocols, services and APIs
- High-speed cryptographic co-processor
  - AES-128/192/256 encryption in multiple modes
  - Hash algorithms: MD5, SHA-1, SHA-256/512
  - Public key: RSA, ECC, DH
  - TRNG and NIST 800-90 PRNG
- RSA-based boot-time integrity checking
- Secure storage with anti-reflash protection
- IEEE 1667™ authentication





## ■ Secure Disk

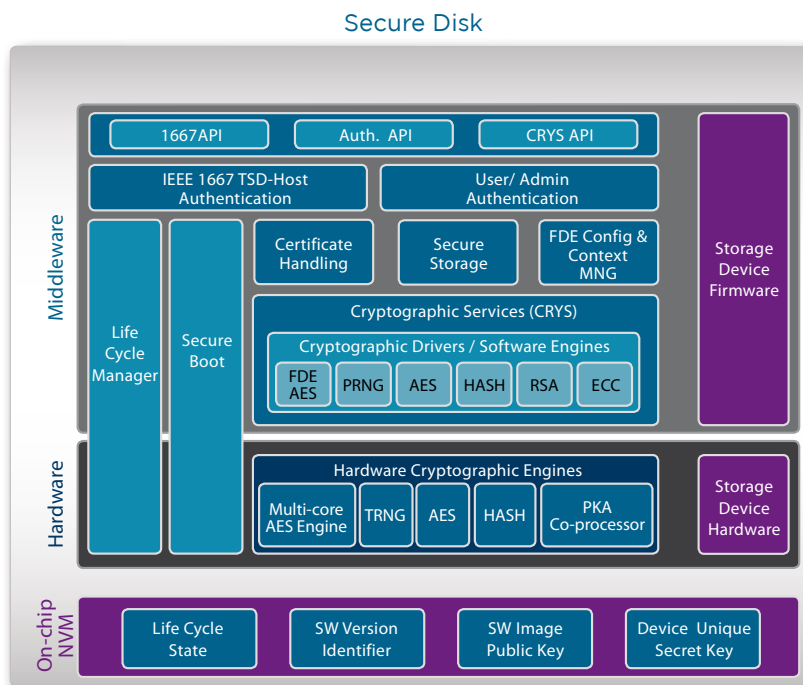
Our most valuable assets are stored on numerous fixed and mobile devices, vulnerable to theft and unauthorized access. Moreover, government and industry regulations mandate privacy and strict control of data. To achieve true protection, data must be protected where it is stored, and not by the application that uses it.

Discretix Secure Disk (DxSD) protects disk content from unauthorized access or misuse. Disk content is protected via full disk encryption (FDE) requiring pre-boot password authentication prior to disk access. Post-boot authentication based on IEEE 1667™ is used for transient and secondary disks. Once access to the disk is granted, the DxSD AES engine seamlessly decrypts data that is read from the disk and encrypts data that is written to the disk.

DxSD also provides protection for the storage device itself. A DxSD secure boot function verifies that the controller firmware has not been tampered with or modified, guaranteeing a known and trusted starting point. In addition, the master boot record authenticity is verified.

### Key Benefits and Highlights

- Full disk encryption (FDE)
- Strong, robust XTS-AES-128/256 encryption
- Encryption at disk throughput
- Prevents theft of sensitive information
- Avoids information leaks resulting from inaccurate data classification
- Prohibits usage in unauthorized systems
- Platform and OS independent
- Very fast secure data sanitization
- RSA-based boot-time integrity checking
- Secure firmware updates
- Master boot record tampering detection
- IEEE 1667™ authentication with host
- Pre-boot event logging
- Multi-user support



# Content Protection

Protects the distribution and consumption of content on multimedia devices.

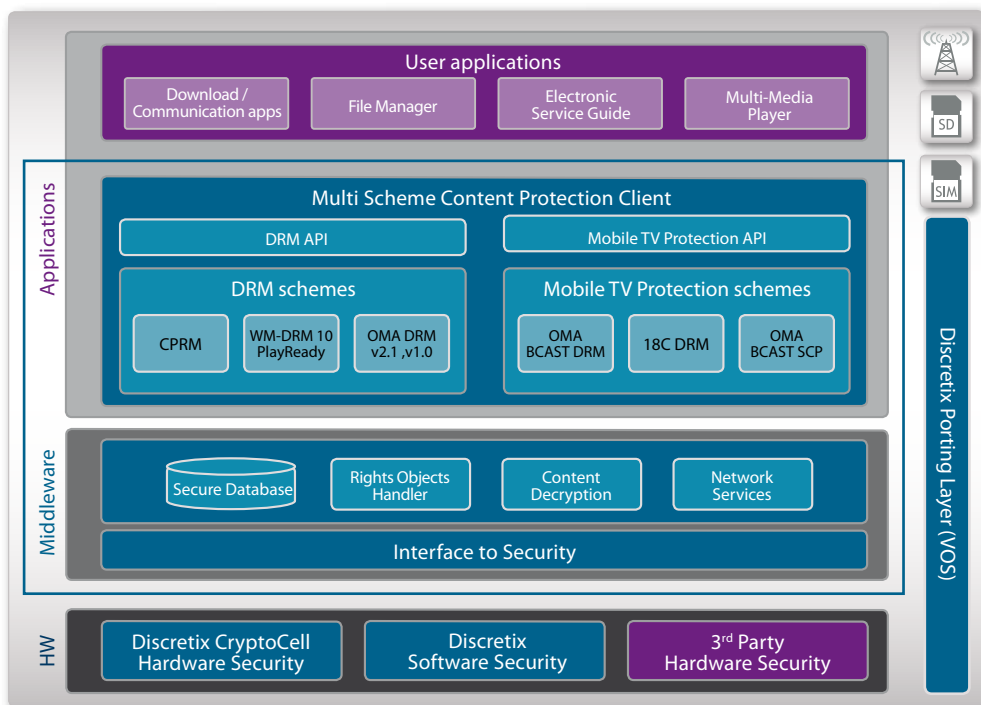
## ■ Multi-Scheme Content Protection Client for Device Vendors and Service Providers

Discretix Multi-Scheme Content Protection Client is a future-ready solution, providing a complete implementation of the major schemes in use today including OMA DRM V1.0, OMA DRM V2.1, Microsoft WMDRM 10, Microsoft PlayReady, CPRM and OMA BCAST. In addition, this solution provides the flexibility to implement new schemes. It has been ported to a large number of operating systems (such as Android, Symbian, Windows Mobile, BREW) and hardware platforms (such as TI OMAP, Qualcomm MSM, Renesas SH-Mobile, Intel Atom and more).

The client's architecture is designed to accelerate the integration and deployment process, allowing a shorter time to market. This is accomplished using a unified API for the application layer (i.e. browser, multimedia player and applications) that is common to all DRM schemes. Additionally the Discretix solution is pre-integrated with leading applications and with common content access frameworks such as Symbian Content Access Framework (CAF), Microsoft File DRM (FDRM) API, GStreamer API and more.

Featuring an outstanding level of security, the client conforms to the stringent security requirements set down by mobile operators and content providers. Discretix Multi-Scheme Content Protection Client is compliant with robustness requirements set by CMLA, Microsoft, 4C Entity and OMTP. Where available the client utilizes the hardware-based security sub-systems, trusted execution environments, hardware cryptographic accelerators, and the secure database mechanism to protect licenses and device keys. In addition, the solution uses the OS application security framework to ensure that only trusted applications can access the protected content.

### Multi-Scheme Content Protection





## ■ Multi OS

---

The Discretix Multi-Scheme Content Protection Client has been ported to a large number of operating systems including Android, Windows Mobile, Symbian, Linux-based systems and multiple RTOSs. The client relies on a limited number of OS services and hardware device drivers accelerating the implementation and deployment process, significantly reducing time to market. The client is fully compliant with operators' requirements and all OMA DRM use-cases.

### Android Support



- Ported to all versions of the Android platform
- Minimal integration and maintenance costs
- Utilizes existing Android components
- Reference code provided to ensure applications are DRM-aware

### Symbian Support



- Ported to multiple versions of Symbian
- Integrated with Symbian Content Access Framework (CAF)
- Seamless integration with different applications

### Windows Mobile Support



- Ported to multiple versions of Windows Mobile
- Client accessible by Microsoft File DRM (FDRM) and file system APIs
- Seamless integration with existing applications
- Based on the Discretix FDRM engine and a file system filter

### RTOS and Linux Support



- Ported to multiple RTOSs (Nucleus, BREW, Rex)
- Ported to embedded Linux (Moblin, Limo and others)
- Integration using the Discretix DRM API
- Single interface to multiple content protection schemes and applications
- Includes GStreamer plug-in

# Content Protection

## ■ OMA DRM V1.0 and V2.1

---

Discretix Multi-Scheme DRM Client fully complies with the different mobile-operators' requirements regarding OMA DRM, including Vodafone, T-Mobile and Orange. The solution is deployed on a large number of platforms, and in certain cases fully integrated with the application framework. Discretix OMA DRM Client enables a broad range of business models, including forward lock, subscription, time and usage limit, P2P distribution, preview, domains (read on multiple devices), advertizing, metering and content backup and recovery. For some operating systems such as Windows Mobile a download agent compliant with OMA DL OTA V2 specifications is provided in order to handle OMA DRM content objects and licenses.

The DRM client supports the set of requirements and use-cases that are needed for Video on Demand (VOD) including download to own, subscription and renting business models, as well as OMA DRM V2.1 domains, preview and metering features.

The client supports the highest level of security and robustness required by CMLA. Content Management License Administrator (CMLA) defines a set of security and robustness requirements for data flows, secure time and the methods used to ensure the integrity and confidentiality of DRM sensitive information. Discretix OMA DRM Client uses both SW based tools (e.g. obfuscation) and HW based security tools (whenever available) to ensure full compliance with CMLA requirements.

## ■ Windows Media DRM

---

Discretix Multi-Scheme Content Protection Client supports Windows Media DRM 10 specifications for portable devices. The client supports protected Windows Media Audio (WMA) and Windows Media Video (WMV) files that are encapsulated in a protected advanced system format (ASF). The client supports all Microsoft use-cases including content purchase (download-to-own), content subscription and content rental. These models can be applied for both downloadable content objects and streamed content.

Discretix Windows Media DRM Client supports both indirect and direct license acquisition methods (ILA and DLA). Subscribers can download content directly to their PCs and then transfer it to the mobile device, or they can acquire the license directly from the content service provider. To support DLA, Discretix provides APIs that are used in the license acquisition process along with a reference code for the WMDRM DLA helper function which is a key component in the DLA process. The MTP (media transfer protocol) stack (available from various vendors) required to support the ILA model has been integrated with the Discretix client.

Discretix fully complies with Microsoft's compliance & robustness (C&R) rules. The solution is based on Discretix' security middleware to ensure the highest level of robustness. Discretix Windows Media DRM Client uses both software-based tools (e.g. obfuscation) and hardware-based security tools (whenever available) to ensure full compliance with Microsoft requirements regarding storing sensitive information.



## ■ CPRM

---

Discretix Multi-Scheme Content Protection Client includes a CPRM engine - a cost-effective alternative to a dedicated CPRM chip. The client provides a reliable, high-performance and secure CPRM solution in compliance with the requirements of the 4C Entity.

The Discretix CPRM solution is comprised of three major components:

- SD-Bind / SD-Video / SD-Audio client – User application glue layer, to facilitate the consumption and protection of content.
- CPRM engine – Implementation of SD card mounting and authentication. This includes a provisioning manager, a secure file system component and interfaces to the CPRM IP component.
- CPRM IP – Implementation of the security and cryptographic services that are required for the CPRM scheme.

The Discretix CPRM solution is fully compliant with the 4C Entity robustness requirements regarding the protection of the sensitive information. Discretix CPRM IP component can run on a hardware-based SEE (where available) and has been integrated into a large number of platforms.

The solution is highly optimized to the embedded environment, enabling high performance with low resource consumption. The Discretix SD-Bind component includes a packetized version enabling an efficient implementation of “trick-play” use-case for audio and video files.

## ■ Mobile TV Security

---

Discretix Multi-Scheme Content Protection Client includes a fully-optimized mobile TV security solution compliant with OMA BCAST specifications. The mobile TV solution supports both the SmartCard and DRM profiles of the OMA BCAST specifications. The solution meets a large number of industry specifications including those defined by the Advanced Television Systems Committee (ATSC). In addition, the Discretix solution supports unconnected devices and is integrated with dedicated mobile TV dongles.

The Discretix mobile TV solution enjoys the benefit of the general multi-scheme architecture which is common to all Discretix content protection solutions. The solution offers multi key-management support (both OMA DRM and SCP) as well multi traffic decryption schemes (ISMACryp, IPsec and SRTP). As the mobile TV market is still evolving, the client’s flexibility allowing new content protection schemes, key-management options and traffic decryption to be added.

Discretix Mobile TV Security Client has been deployed on a large number of platforms including Android, different flavors of embedded Linux, Windows Mobile, Symbian and RTOS. The solution is highly optimized to ARM based processors achieving throughput rates of 1 MBps at 400MHz.

In cases where the device manufactures cannot access the player’s source code, the Discretix Mobile TV can be integrated directly to the IP Stack providing a transparent integration with the player.

# Content Protection



Post production, downloadable, content protection device-client for service providers

## ■ Post Production Content Protection Client

---

Discretix offers content service providers and mobile operators a unique content protection client for devices already released to the market. The post production software client allows content service providers to overcome the dependency on pre-installed device applications. In so doing, service providers are able to target the large base of existing devices, accelerating the deployment of new services. Discretix' post product client supports both industry standard and proprietary content protection schemes, compliant with the requirements of the content owners.

The post production clients are available for various open operating systems such as iPhone OS, Android, Windows Mobile, Linux and Symbian.

### Highlights

- Based on standard and widely accepted DRM schemes
- Supports the majority of smartphones and devices
- Immediate access to devices already released to the market
- Secure – compliant with studios and content owners requirements
- Customizable for service provider's specific features

## ■ Link Protection

---

Discretix Link Protection is a content protection solution ideally suited for service providers requiring a rapid rollout of services based on devices already in the market (smartphones, netbooks, PCs, MIDs etc.). The solution creates a trusted link between a receiver (sink appliance) and an authorized display device enabling the distribution of protected video and/or audio streams. Using Discretix Link Protection secured content streamed to the sink appliance can be accessed and consumed by an authorized display device.

Discretix Link Protection utilizes SRTP for content encryption and decryption, as well as a sophisticated key-provisioning and key-management scheme. In addition the solution includes state-of-the-art obfuscation and device-fingerprint technologies to ensure a robustness level in line with the requirements of major studios and content owners. An optional server component - controlling the service registration process - provides an even higher level of robustness. Several renewability mechanisms can be deployed based on the service robustness requirements and the existing service provider infrastructure.

Discretix Link Protection allows content service providers to rapidly deploy services based on devices already in the market eliminating the dependency on a specific feature set in the receiving device. The rapid deployment is achieved without compromising the level of robustness that characterizes Discretix' content protection solutions.

Discretix Link Protection is available for devices based on open operating systems including iPhone OS, Android, Windows Mobile, Linux and Symbian.

# Security Modules



## Fundamental security building blocks for any device

### ■ Secure Boot

Discretix Secure Boot offers protection for code running on any device, ensuring that only authenticated code is executed when the chip powers up. A boot process based on trusted software is essential to the proper functioning of devices such as mobile handsets, DVDs and utility meters. The software loaded during the device boot controls the functionality of the device as well as any business rules.

Offline software modifications attacks, aimed at modifying or bypassing the code running on the device, are the most common type of attack. Offline attacks are harder to prevent, particularly because the device is powered-off.

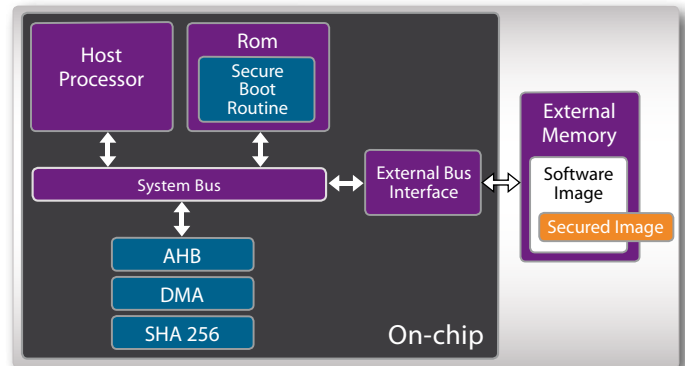
Discretix Secure Boot offers protection from hacking by identifying any modifications that have occurred once power is restored. Discretix' solution protects vulnerable elements of the device (flash memory storing the code) while the device is off. The secure boot solution verifies the public key signature embedded into the flash image, ensuring that only the owner of the private key is able to sign and authenticate code.

### Secure Boot benefits:

- Boot up with authenticated code
- Prevents hacking or patching of the code
- Minimizes device malfunction due to unauthorized software modifications

Discretix Secure Boot ensures a faster boot up process and improved user experience by providing hardware acceleration of the public key and hashing needed for code verification.

### Secure Boot Hardware Architecture



# Security Modules

## ■ Secure Debug

Typically, debugging interfaces (e.g. JTAG) are disabled as a chip leaves the factory, ensuring that access to the various part of the SoC remain closed to hackers. Discretix Secure Debug, enables the debug interface to remain active, yet protected. Using the solution, only parties authorized by the manufacturer can authenticate their debugging equipment, retaining access to the debug interface, throughout the product life-cycle. This cryptography based mechanism prevents platform SW alteration and exposure as well as leakage of sensitive information through the debug interface

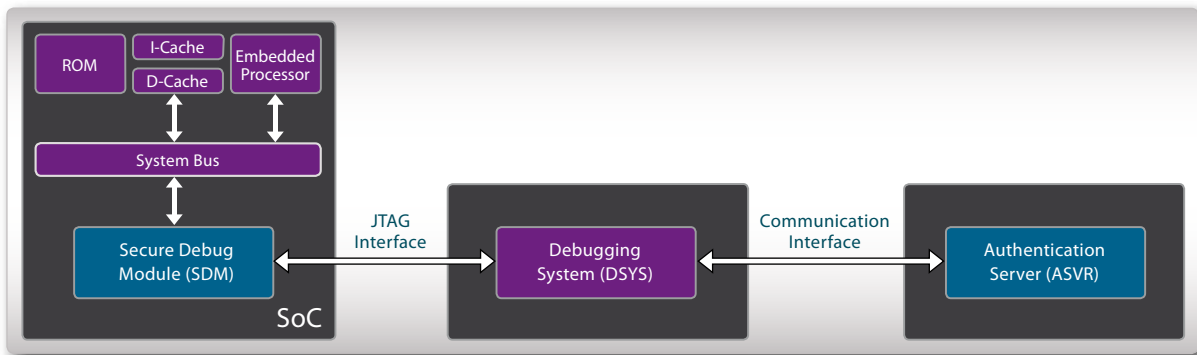
The Discretix Secure Debug is comprised of three elements:

- The secure debug module (SDM), embedded in the SoC, used to verify the authenticity of users attempting to perform debugging operations. The SDM is a hardware and firmware module provided by Discretix to the chip manufacturer.
- An authentication server installed in the OEM's premises, storing the sensitive data needed for authentication. This software module is provided as reference code.
- The debugger - operating as a relay between the previous two elements - is integrated into some of today's leading debuggers (such as Lauterbach). Reference code is provided by Discretix as well.

The flexible authentication scheme has several benefits:

- The embedded SDM can control multiple test access ports and debug interfaces on the SoC, allowing access to different areas of the SoC and the formulation of different access policies.
- Flexible access policy, defined per debugging entity (e.g., OEM).

Secure Debug Hardware Architecture





## ■ Secure Database

All applications - ranging from those with copyright enforcement to personal applications containing sensitive user information - need to be protected from prying eyes.

Protecting the information involves strict access control and data encryption. Stored passwords, credentials and keys are protected for secrecy and from unauthorized changes.

Discretix Secure Database provides a robust secure storage solution for:

- security key material
- rights objects
- certificates
- any other sensitive information

Discretix Secure Database ensures the strongest security for diverse applications ranging from enterprise to multi-user data. The secure module employs different authorization mechanisms to protect different types of data.

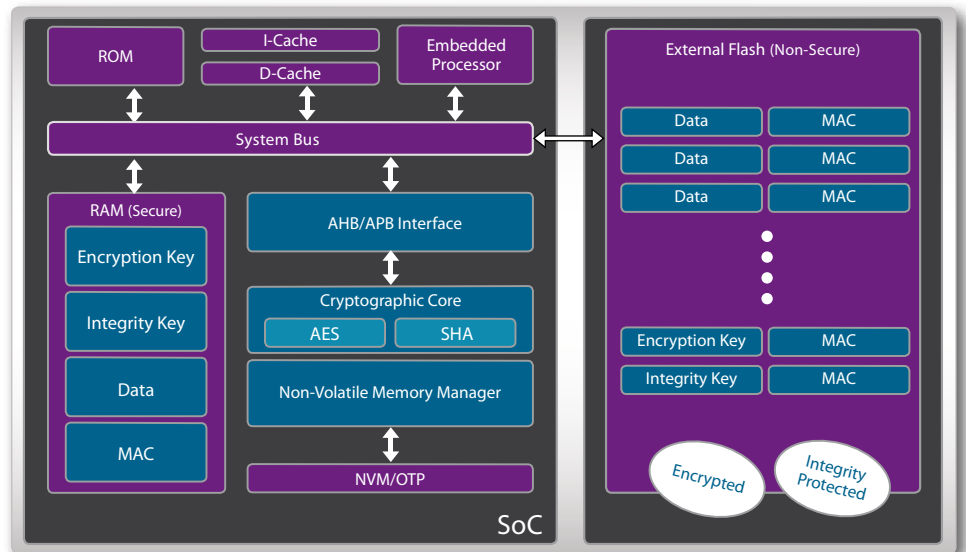
The Secure Database protects confidentiality and integrity of data items in off-chip non-volatile memory. This data is securely stored on external flash memory, with full confidentiality provided by AES encryption, and data integrity provided using cryptographic hash functions. Access to items in the secure database is protected by several authentication methods, each with specific access policies. The Secure Database is fault tolerant, and employs several methods to mitigate re-flash attacks.

The Secure Database offers a unique approach to dealing with protected cryptographic keys. The Secure Database mechanism allows application to use the cryptographic keys, yet limits the application from directly accessing the keys. This ensures that the cryptographic keys are never exposed outside the secure environment.

### Highlights

- Robust encryption (AES-128/256)
- HASH integrity protection
- Multiple authentication methods
- Re-flash attacks protection
- Fault tolerant
- Unlimited database size
- Fast and efficient search capabilities
- Easy to use API

### Secure Database Hardware Architecture



# Cryptographic Libraries

Building blocks for embedding security into applications.

## ■ Hardware Cryptographic Engines

Discretix' hardware libraries provide a variety of symmetric ciphers, cryptographic hash functions and asymmetric ciphers.

All of the engines are highly configurable, allowing easy removal or addition of cipher modes. The implementation offers an excellent tradeoff between performance and power consumption (area). The libraries are suitable for all types of applications – ranging from SmartCard-grade ciphers with small footprint and low power consumption up to storage and networking applications that require extremely high throughputs.

All of the Discretix engines are silicon-proven across many different devices and platforms. Thanks to Discretix' technology maturity, ease-of-integration along with comprehensive documentation and support, the time-to-market is reduced substantially.

The cores are FIPS-140 and Common Criteria EAL4+ ready. The cores also offer optional countermeasures for side-channel attacks (such as power analysis attacks).

## ■ Software Cryptographic Engines

The Discretix software cryptographic libraries offers a variety of optimized software only of cryptographic algorithms. These field-proven implementations of cryptographic algorithms are deployed in numerous SoCs and other devices that support a wide variety of applications. The libraries include the following cryptographic algorithms:

- AES – ECB, CBC, CTR, MAC, XTS, CCM, XEX,CMAC, XCBC
- DES/TDES – ECB, CBC
- HASH – MD5, SHA1, SHA256, SHA384, SHA512, HMAC
- RC4
- C2 – ECB, CBC
- RSA – Encrypt, Decrypt, Sign, Verify, Key generation
- ECC – Gf(p), Encrypt, Decrypt, Sign, Verify, Key generation
- Diffie-Hellman
- PRNG

The cryptographic libraries are rigorously tested and certified by tier-1 customers assuring short time-to-market and ease-of-integration.



## ■ AES

AES is the most widely used symmetric cipher. The Discretix AES engine supports all key sizes defined within the standard. The AES engine supports multiple modes including ECB, CBC, CTR, CCM, GCM and XTS for encryption and CBC-MAC, XCBC (and variants) for authentication. The engine avoids multiple data fetches by supporting a dual-tunnel configuration; decryption with one key is concatenated by encryption with another key.

## ■ HASH

The Discretix hash cryptographic engine supports the combination of the MD5 algorithm and the secure hash algorithm (SHA) including SHA-1, SHA-256 and SHA-512. The hash engine handles message padding and generates a digest for data streams and objects. The engine is configurable and enables varying tradeoffs between performance and power consumption (area). Support for hardware-based and hash-based message authentication codes (HMAC) is also optional. If chosen, the engine generates a digest based on the FIPS PUB 198 standard.

## ■ PKA

The public key accelerator (PKA) is a general-purpose acceleration engine for mathematical operations involving significantly long operands. The PKA connects as a peripheral and offloads processor-intensive functions. The Discretix PKA performs a variety of arithmetical and logical operations along with modular arithmetic operations over long operands, used in asymmetric cryptography. The PKA significantly improves performance of computationally-intensive public key algorithms such as RSA, Diffie-Hellman (D-H) and elliptic curve cryptography (ECC). The Discretix PKA supports standard and non-standard key operations from 128 bits to 2112 bits in increments of 32 bits.

## ■ DES

The Discretix DES cryptographic engine fully supports the DES and triple-DES algorithms. The engine supports electronic code book (ECB) and cipher block chaining (CBC) modes. DES is now considered to be insecure, however, its successor – triple-DES – is still used in many applications. Like the Discretix AES, the DES engine offers optional countermeasures for side-channel attacks such as power analysis.

## ■ RNG

The Discretix random number generator (RNG) includes a true RNG (TRNG) hardware component and a pseudo RNG. Random numbers are used for many purposes (cipher key generation, nonce generation etc.). The TRNG core collects entropy, performs self-testing and provides a random seed. The PRNG core provides generation of a pseudo-random bit stream based on a random seed. The seed is provided either directly from the TRNG core or through a register interface by the host processor. Both components easily integrate with each other to provide a complete RNG solution. Alternatively, they can be used as standalone modules.

# Market Traction

## Customers



## Partners



## Standards



# About Discretix

Discretix is dedicated to delivering innovative security solutions to the complex and ever-changing embedded computing markets. This specialized expertise has allowed the company to provide chipset, device vendors and service providers with complete security platforms that are easily integrated, field proven and future-proof.

Discretix' solutions make security transparent to the end-user, while protecting sensitive information and applications from malicious attacks, viruses, fraud and theft. Discretix solutions include both hardware and software technologies, that are deployed in SoCs, platforms and devices. The Discretix suite of products includes co-processors, sub-systems, modules, cryptographic accelerators and content protection applications.

Discretix' products are licensed by the world's leading semiconductor, platform, device manufacturers and service providers. The company is also active in developing an embedded security ecosystem. To this end the company works closely with leading technology and service providers across the entire value chain to deliver fully-integrated and secure end-user applications. Comprised of companies from around the world, the ecosystem includes hardware manufacturers, IP vendors as well as application and OS vendors.

#### Headquarters

Discretix Technologies Ltd.

Tel: +972 73 255 8800

#### USA

Discretix Inc.

Tel: +1 408 969 9991

#### Japan

Discretix Technologies Ltd.

Tel: +81 3 5148 2053

#### Taiwan

Discretix Technologies Ltd.

Tel: +886 2 8792 9423

#### Korea

ACETRONIX

Tel: +82 2 364 6080

#### China

Commtone Solution Co. Ltd.

Tel: +86 21 2926 4120



discretix.com

