

## Discretix DES Cryptographic Engines



Discretix cryptographic engines are widely deployed in leading system-on-chip solutions. Discretix provides highquality, ready-to-use cryptographic engines, to support variety of applications. Included in Discretix's family of cryptographic engines are symmetric ciphers, asymmetric ciphers, Hash and random number generators.

### DxDES - General Description

The DxDES cryptographic engine fully supports the DES and Triple DES algorithms. The engine supports Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes.

DxDES has three interfaces: configuration (CPU) Data-In and Data-Out. The CPU interface is a synchronous slave bus, which allows an external processor to access the engine's configuration registers. The Data-In and Data-Out interfaces are FIFO-type interfaces, which are used to stream in cipher/plain data to be processed, and stream out plain/cipher output data. AMBA AHB interfaces for Data-In and Data-Out are also available.

### Key Applications

- Digital Right Management scheme (WMDRM)
- WLAN applications (IEEE 802.11)
- IPSec and SSL/TLS
- WiMax applications (IEEE 802.16)
- E-commerce (EMV v4.1)

### Benefits

- Silicon proven - deployed in numerous devices and platforms
- Vast experience with multiple tier-1 customers
- Mature technology from the embedded security market leader
- Fast time to market, easily integrated
- Highly optimized implementation ensures minimal gate count and reduced power consumption
- Excellent technical support

### Certifications

- FIPS ready
- Common Criteria EAL4+ ready



## Key Features

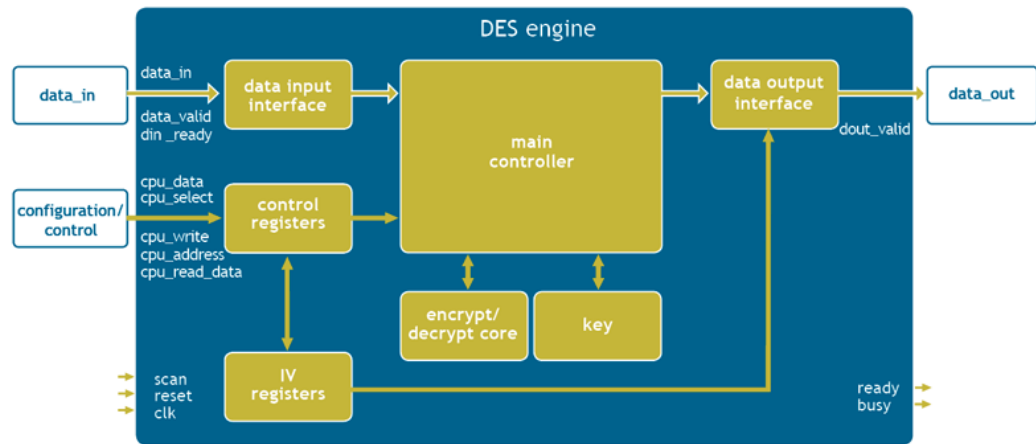
- Throughput of 1400 Mbps (480Mbps for 3DES)
- Supports DES and Triple DES (3DES)
- Supports ECB and CBC modes (according to FIPS PUB 81 and ANSI X9.52)
- Area: 7.7K ASIC gates
- Asynchronous 32bit input and 64 bit output data interface
- Two or three keys for 3DES mode
- Optional support for AMBA AHB data interface

## Deliverables

- Synthesizable Verilog RTL source code
- Synthesis script and constraints
- RTL Test Bench (test vectors and expected results)
- User Manual with hardware integration guidelines and application notes

## Block Diagram

### DES Block Diagram



## Configuration Options

Name	Keys	Configuration	Throughput		Maximum Clock Frequency	Gate' Count
			bits/cycle	Maximum (in Mbps)		
DxDES-01	56, 112, 168	DES	3.55	1400	390MHz	7.7K
		3DES	1.23	480		

1. Technology and synthesis dependent; based on the use of design compiler and slow speed 0.09 μm TSMC technology; measured at 100MHz

## About Discretix

Security lies at the heart of embedded computing, enabling a broad range of services and applications. Discretix delivers leading-edge embedded security solutions to the mobile, storage, automotive, networking, office automation and industrial markets. Discretix' suite of products includes security co-processors, security sub-systems, cryptographic cores and content protection applications. Discretix serves the needs of some of the world's best-known semiconductor and device manufacturers.