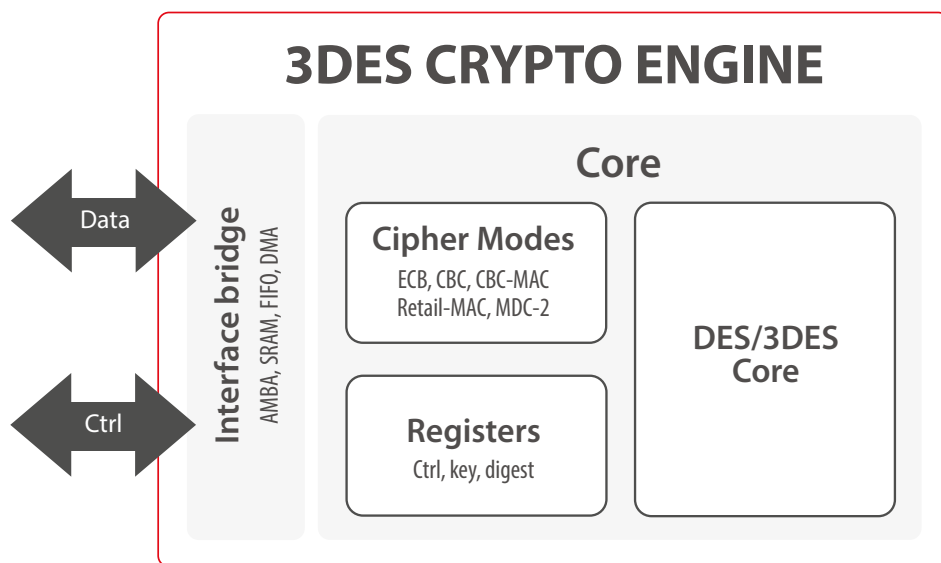# SECURE-IC
THE SECURITY SCIENCE COMPANY

Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Security IP > Tunable Crypto > Symmetric > SCZ_IP_3DES

3DES CRYPTO ENGINE

The DES/3DES crypto engine offers a hardware implementation of the Data Encryption Standard (DES) according to Federal Information Processing Standards Publication (FIPS 46-3) of the National Institute of Standards and Technology (NIST).

3DES CRYPTO ENGINE

Interface bridge
AMBA, SRAM, FIFO, DMA

Data

Ctrl

Core

Cipher Modes
ECB, CBC, CBC-MAC
Retail-MAC, MDC-2

Registers
Ctrl, key, digest

DES/3DES Core

Features

- ASIC and FPGA
- FIPS 46-3 compliant
- Supports:
  - DES
  - 3DES
- Includes:
  - Encryption
  - Decryption
- Performs key expansion
- Supports:
  - ECB
  - CBC
  - CBC-MAC
  - Retail-MAC
  - MDC-2
- Low power feature
- Data interface: AMBA (AHB/AXI) with optional DMA
- Control interface: APB/AXI4-lite

Implementation aspects

Standardized AXI-4 and AHB (optional) I/O simplifies system integration. It is easily portable to ASIC and FPGA and supports a wide range of applications on various technologies. The unique architecture enables a high level of flexibility. The throughput and features required by a specific application can be taken into account in order to select the most optimal and compact configuration.

Applications

- RFID
- Finance

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA
- Self-checking RTL test-bench on referenced vectors
- Documentation

V4.0

CONTACT US

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

TAIWAN
sales-TAIWAN@secure-ic.com

SECURE-iC
THE SECURITY SCIENCE COMPANY

HEADQUARTERS
Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com