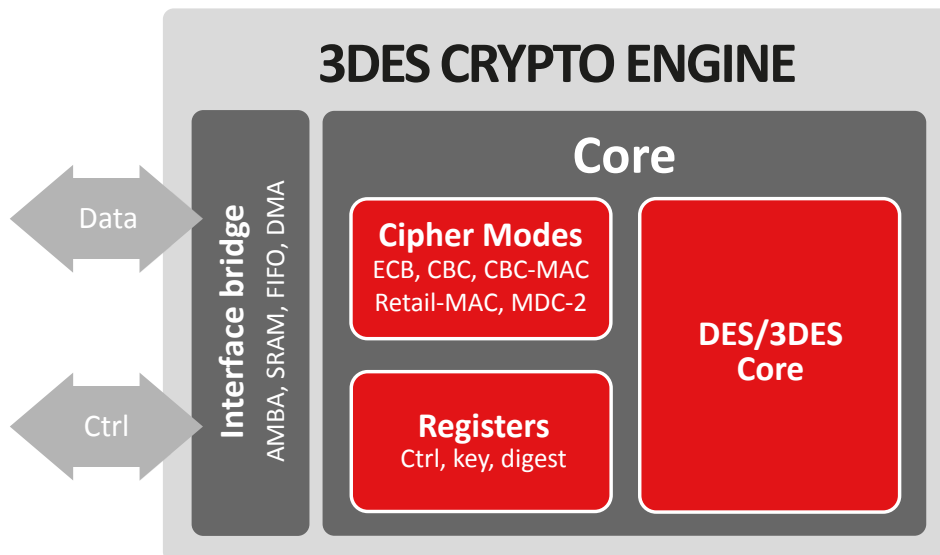




3DES CRYPTO ENGINE

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).



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.

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

Applications

- ✓ RFID
- ✓ Finance

Deliverables

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

V1.1

Silex Insight

Rue Emile Francqui 11,
1435 Mont-Saint-Guibert, Belgium

Tel: +32 10 45 49 04

E-mail: contact@silexinsight.com

Web: www.silexinsight.com