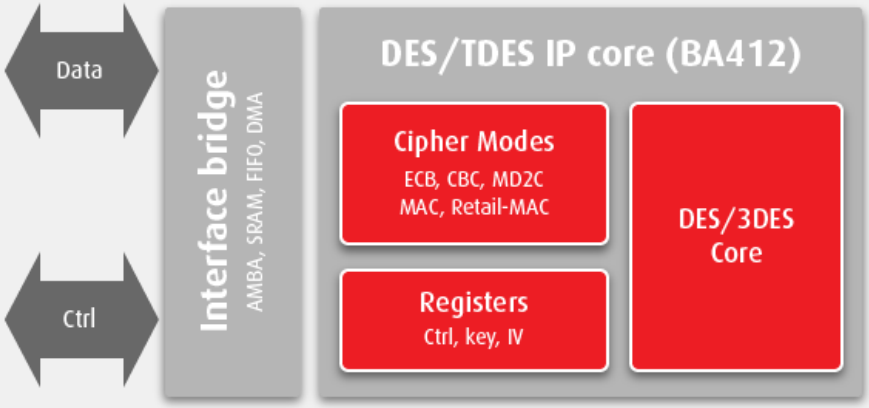
BarcoSilex
DES/3DES

BA412
Product sheet

The BA412 DES / 3-DES IP core is developed validated and licensed by Barco Silex.

The BA412 offers an 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

The BA412 core is easily portable to ASIC and FPGA (Altera, Xilinx, Microsemi). It 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.

Deliverables

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

FEATURES

- Supports DES and 3DES
- Supports encryption and decryption
- Performs key expansion
- Masking option available for protection against SPA & DPA
- Supports ECB, CBC, MAC and Retail-MAC
- Low power feature
- Data interface: Slave, FIFO:AXI4-Stram, AHB, DMA
- Control interface: APB or AXI4-lite

APPLICATIONS

- Secure mobile communications
- RFID
- Finance