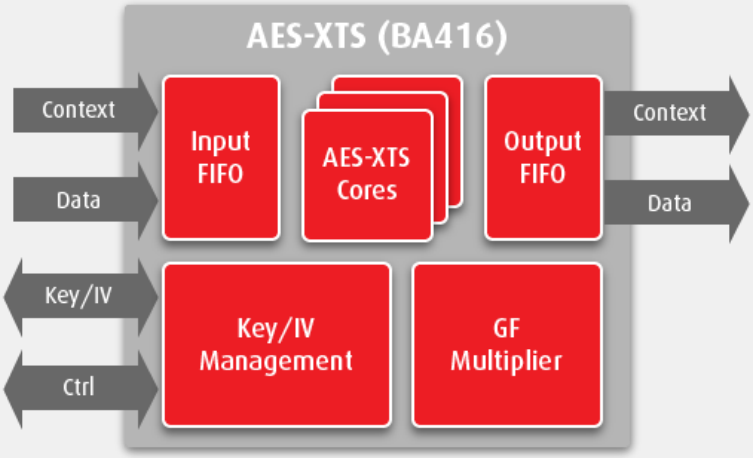
BarcoSilex

AES-XTS crypto Engine

BA416
Product sheet

The BA416 AES-XTS crypto engine includes a generic & scalable implementation of the AES algorithm making the solution suitable for a wide range of low-cost & high-end applications from 15 K-Gates (including key, IV, input and output registers and Galois field multiplier) to > 100 of GBits/s.



Implementation aspects

The BA416 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 128-bit & 256-bit key with Key Expansion
- Compliant with NIST SP800-38E
- Masking option available with excellent protection against SPA & DPA
- Data interface: AMBA (AHB/AXI) with optional DMA
- Control interface: APB or AXI4-lite
- Up to 100 GBits/s
- XTS 256 (2 keys of 128 bits)
- XTS 512 (2 keys of 256 bits)
- Cipher stealing (optional)
- Low power feature

Applications

- Encrypted disk/data storage
- SATA III