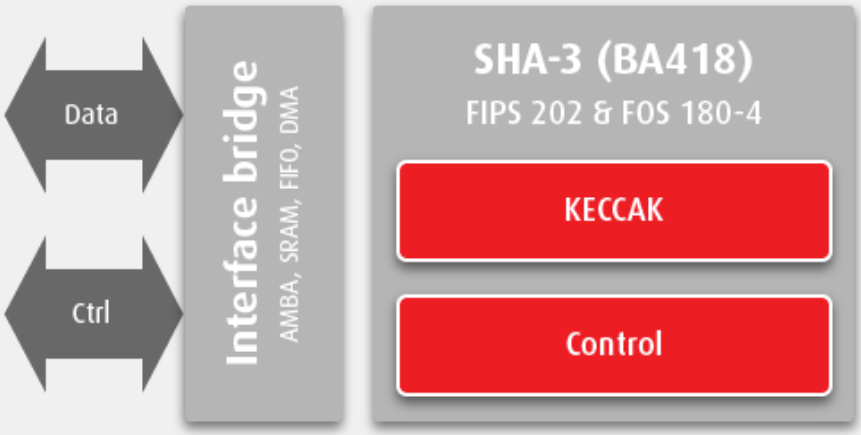
BarcoSilex

SHA-3

BA418
Product sheet

The BA418 is a crypto engine IP core for SHA-3 hashing functions compliant to NISTS's FIPS 180-4 and FIPS 202 standards.



The SHA-3 core has integrated flexibility and scalability to allow for high throughput and a configurable number of hashing rounds to optimize the silicon resource/performance ratio.

The SHA-3 IP core is available for ASIC and FPGA devices (Altera, Xilinx, Microsemi.

Implementation aspects

Standardized AXI-4 I/O simplifies system integration. All our IP cores are delivered with software drivers to simplify ASIC or FPGA integration.

FEATURES

- FIPS 202 and FOS 180-4 compliant
- Supported fixed-length functions:
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
- Supported XOF functions:
  - SHAKE-128
  - SHAKE-256
- Throughput over 20 Gb/s
- Low power feature
- Compact solution
- Control interface
  - APB
  - AXI4-lite
- Data interface:
  - AMBA (AXI, AHB)

APPLICATIONS

- Encrypted data storage
- Secure communications
- Secure processing
- IPsec acceleration
- E-commerce
- VPN
- Financial Transactions