Power Matters™

Microsemi Security Solutions

Security on Chip, in Transit, and at Rest
October 2014

Secure Execution

Enhancing Microsemi SmartFusion2/Igloo2 Security

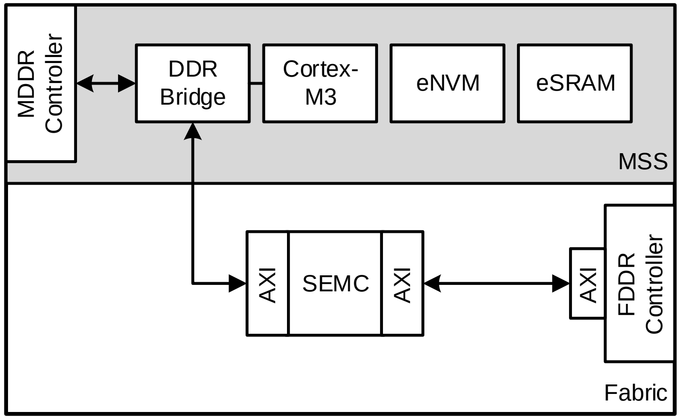
SmartFusion2 Secure Execution

Augmenting the SmartFusion2 with security IP

- Leverage SmartFusion2 security capabilities to provide a secure runtime execution environment

- Fabric Protection
  - Protected using SmartFusion2 built-in security
  - Configuration file encrypted with built-in FPGA key
  - EnforcIT Security Monitor

- ARM Cortex-M3 Software Protection
  - Bootloader stored in eNVM
  - User application encrypted and stored externally
    - Keys stored in internal eNVM
    - User level application performs encryption wrapping
  - DDR access bridged through inline encryptor
    - AES-XTS with integrated cache
    - Ephemeral keys generated using SF2 RNG

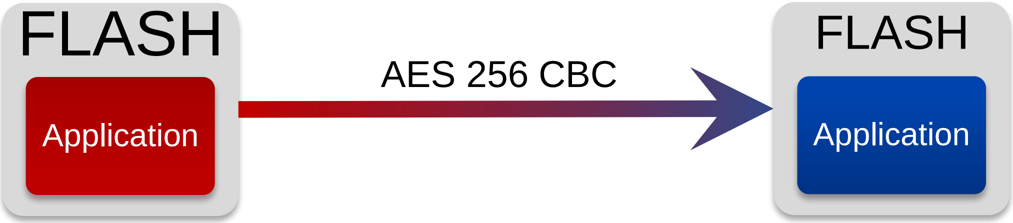


Application Protection

Securing Software at Rest

- General Principles
  - Encrypt all software and data outside of the FPGA boundary
  - Use a secure bootloader to decrypt/authenticate the application
- Software and Tools
  - Secure Bootloader (Microsemi run-time software)
    - Supports encrypted load of application
    - Basic file system and SPI controller
    - Supports execution of bare-metal and uClinux applications
  - File Encryptor (Microsemi tool)
    - Performs AES-CBC with ciphertext stealing encryption

```
fencrypt --keyfile key.dat --binfile application.bin
```

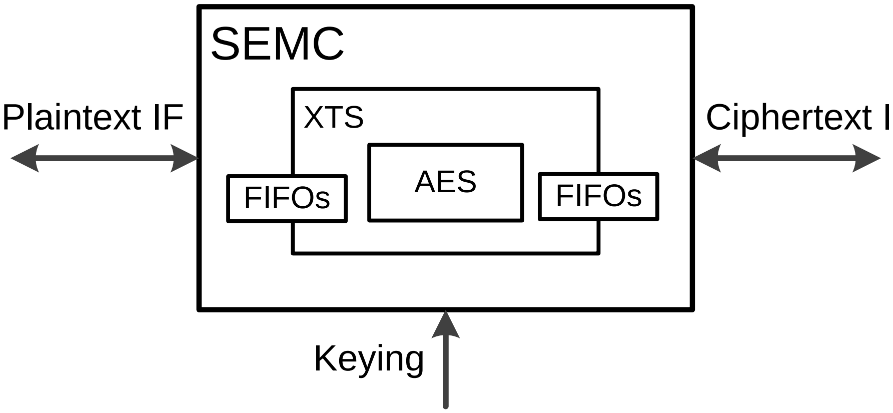


External Memory Protection

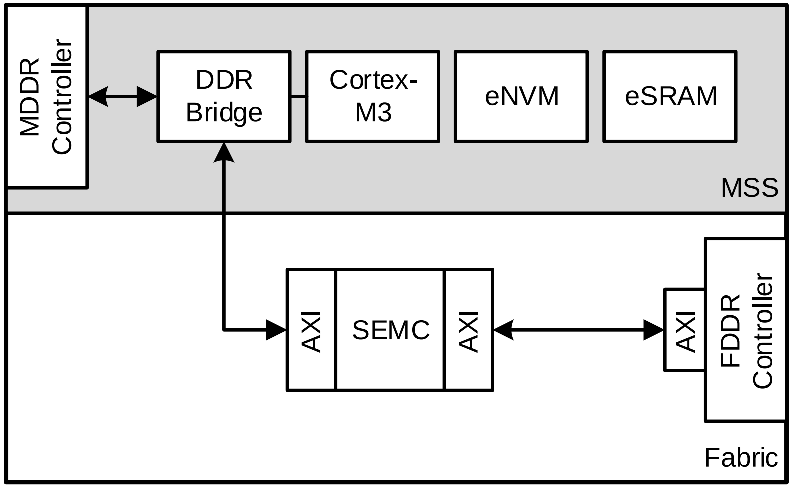
In-line AES-XTS Memory Encryption

- Protect DDR with ephemeral inline memory encryption
- Secure External Memory Controller (SEMC)
  - AES-XTS encryption with 128, 192, and 256 bit keys for data and tweak
    - Transparent encryption with configurable number of blocks-per-sector
  - Module design with internal, highly-configurable AES core
    - Supports high-throughput configuration with up to 400 MB/s of sustained bandwidth
  - Single port RAM-style interface for bridging to internal bus logic
  - FPGA-agnostic IP

High-Level Block Diagram

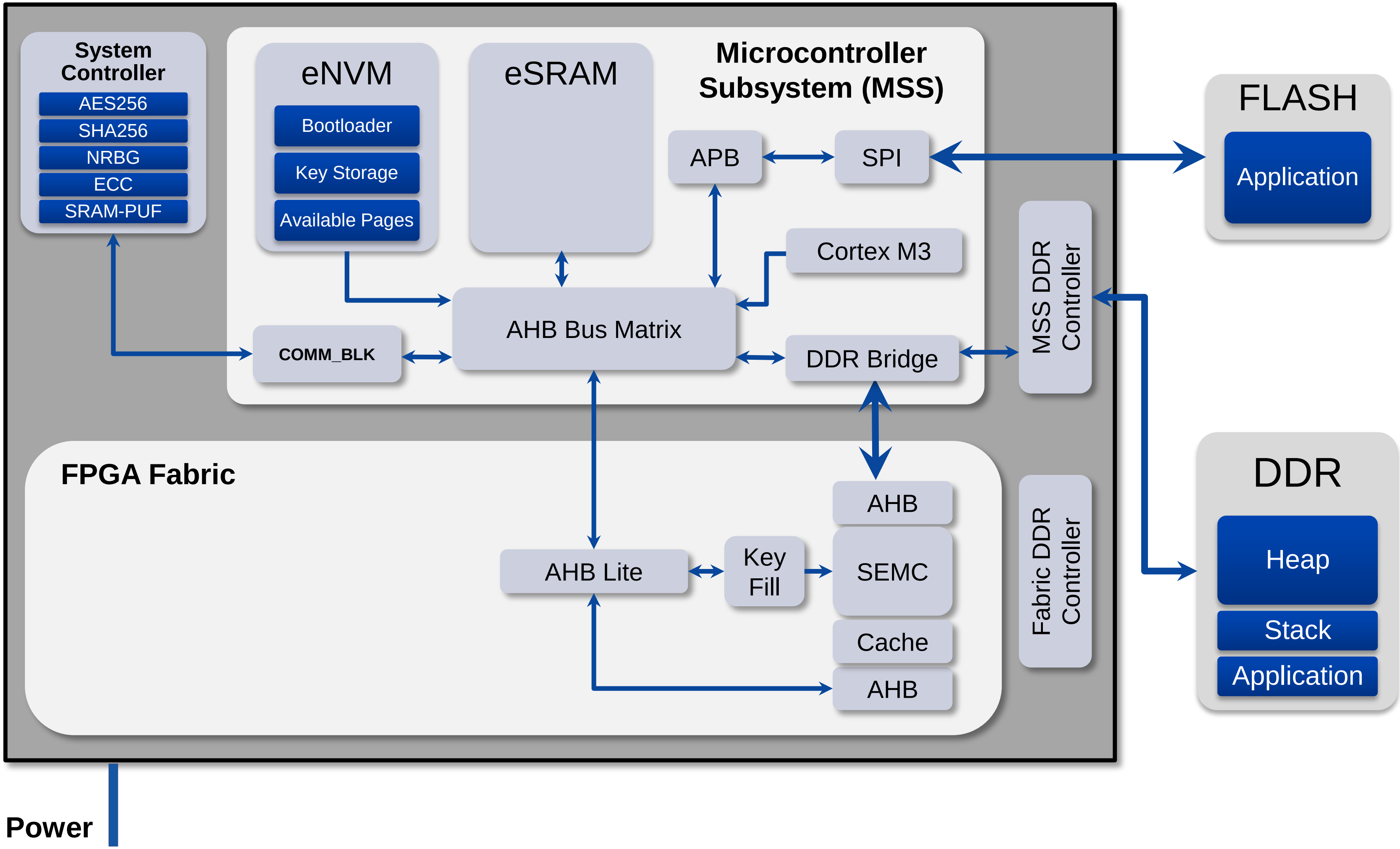


SmartFusion2 Application Example



SmartFusion2 SoC

SmartFusion2 Starter Kit Secure Execution Alternate Architecture



Security Solutions | info@microsemi-wl.com | 765.775.1800 | www.microsemi.com