Configuration memory contains
the FPGA bitstream (code)

Client interface
for HSM management
and for communicating
with applications
(e.g., USB to SPI)

Applications connect
via the Cryptech
PKCS#11 provider

Interface for connecting
Security Officer authenticators and
storage devices for master key backup
(e.g., USB Host, Smartcard)

At least one external entropy
source connected to the FPGA

Tamper switch to
simulate tamper
during development

PKCS#11
provider in host

JTAG port(s) for
testing and debugging

JTAG

Entropy
Sources

Config
Memory

JTAG

USB Host
Interface

USB AuthN/
Backup Interface

Tamper
Switch

Spy-
Bi-
Wire

Temperature

Keystore contains
encrypted application keys
(not connected for alpha)

Keystore

FPGA

ARM

status(serial)

Tamper
Detection
MSP430

Accelerometer

Exterior Shield

RAM-based Master Key Memory
contains the symmetric key
used to encrypt the Keystore
(~ 1024 bit) power supply
controlled by tamper circuit

Master Key
Memory

RTC

External
RAM

External
Flash (SD)

C-4

Battery

Optional tamper
inputs/outputs

Security Boundary

Tamper detection circuit
responsible for erasing Master
Key Memory upon tamper