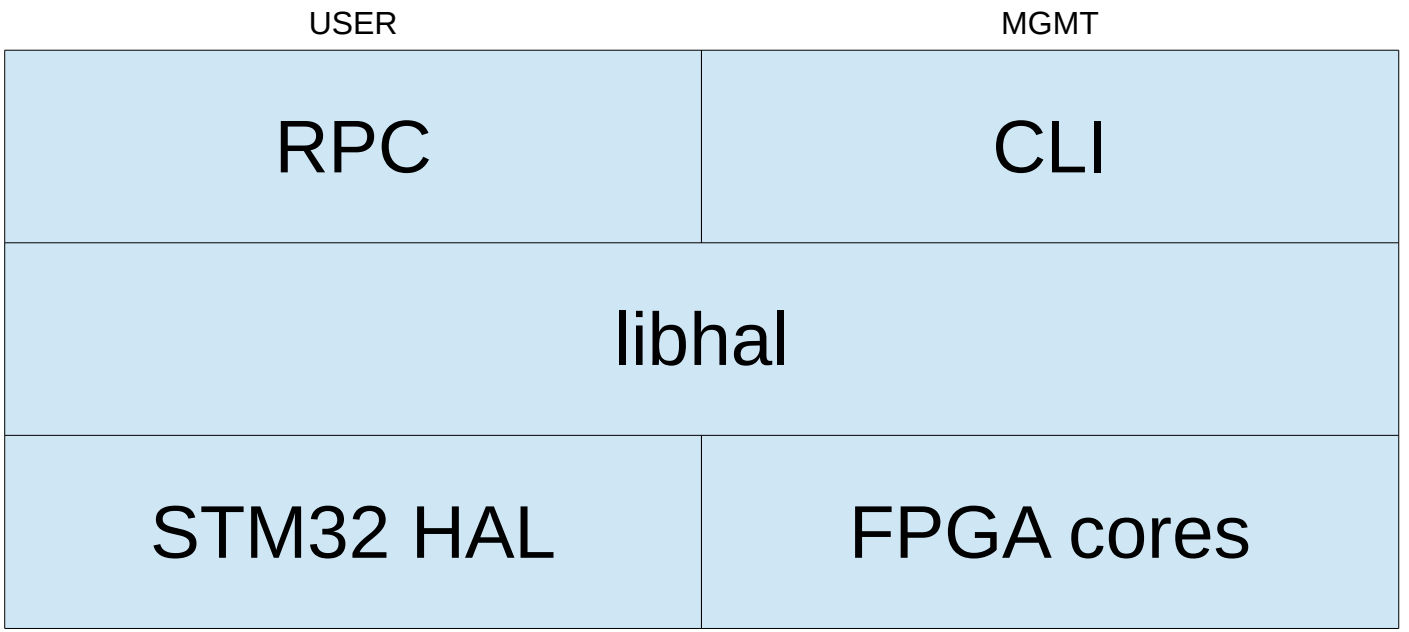
Cryptech Alpha Firmware

Paul Selkirk <paul@psgd.org>
Berlin, July 2016

Firmware Overview



Third-Party Software

- STM32 HAL, RTOS (BSD)
- Libcli (GPL, BSD re-license in the works)
- TomsFastMath (public domain)
- Sqlite3 (on host) (public domain)

RPC

- RPC wrapper around our libhal API
  - PKCS #11 builds on this
- XDR serialization, SLIP framing
- Used for some internal operations as well
  - e.g. CLI login == RPC login

CLI

- Cisco-like CLI to manage the device
- Mostly around keystore and masterkey
- Also used for upgrades
- Command set subject to change at whim...

CLI

```
cryptech> help

Commands available:
  help                          Show available commands
  quit                          Disconnect
  logout                        Disconnect
  exit                          Exit from current mode
  history                       Show a list of previously run commands
  fpga show cores               Show FPGA core names and versions
  fpga reset                    Reset FPGA (config reset)
  fpga bitstream upload         Upload new FPGA bitstream
  fpga bitstream erase          Erase FPGA config memory
  keystore set pin              Set either 'wheel', 'user' or 'so' PIN
  keystore set pin iterations   Set PBKDF2 iterations for PINs
  keystore clear pin            Clear either 'wheel', 'user' or 'so' PIN
  keystore delete key           Delete a key
  keystore rename key           Rename a key
  keystore show keys            Show what PINs and keys are in the keystore
  keystore erase                Erase the whole keystore
  masterkey status              Show status of master key in RAM/flash
  masterkey set                 Set the master key in the volatile Master Key Memory
  masterkey erase               Erase the master key from the volatile Master Key Memory
  masterkey unsecure set        Set master key in unprotected flash memory (if unsure, DON'T)
  masterkey unsecure erase      Erase master key from unprotected flash memory
  firmware upload               Upload new firmware image
  bootloader upload             Upload new bootloader image
  reboot                        Reboot the STM32
```

libhal

- Primitives talk directly to the FPGA cores
- Functional wrappers
  - Hash/HMAC
  - PBKDF2
  - AES keywrap
  - Master Key Memory
  - ModExp
  - RSA
  - ECDSA
  - CSPRNG

STM32 HAL

- Board Support Package
- RTOS
  - CLI thread
  - RPC thread
    - Designed to support multiple RPC threads
      - but needs work WRT resource management

FPGA cores

- Memory-mapped register interface
  - Name
  - Version
  - Ctrl
  - Status
  - Block data, digest, etc.