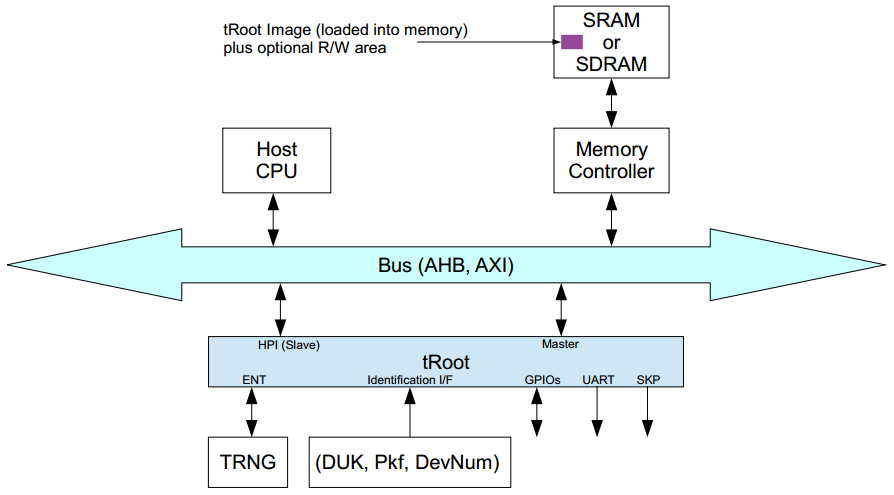
## Secure Subsystem Feature

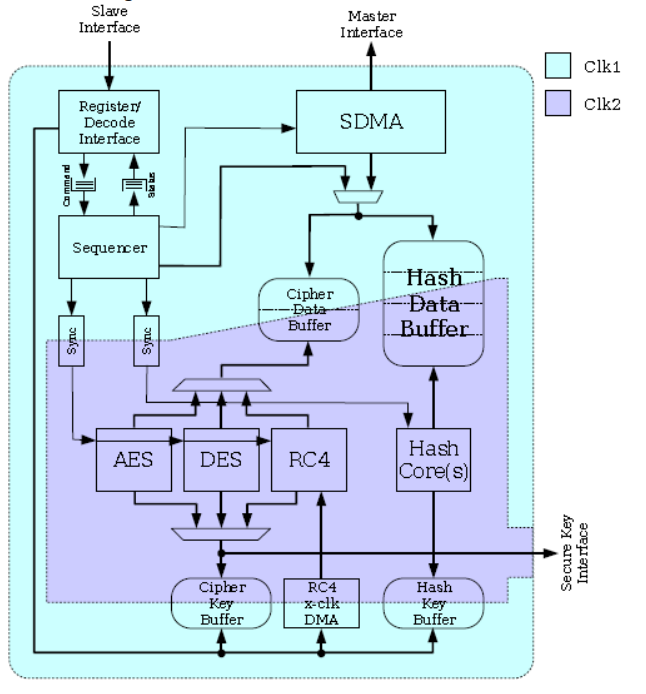
All the engines is work at 150MHz.

### tRoot



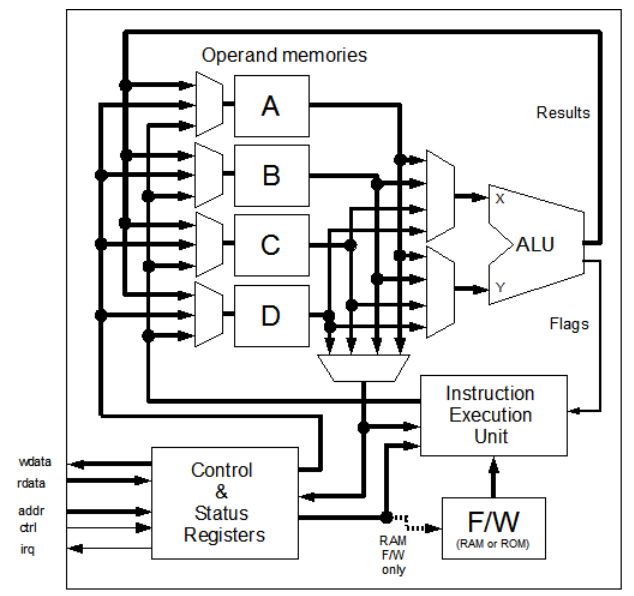
* tRoot contains an embedded microprocessor. As such, it requires access on a bus to fetch instructions from memory which is then stored in a local secure cache and occurs over the master interface
* Support secure boot and secure storage

### Security Protocol Accelerator(SPACC)



* Cipher algorithms: AES, DES
* Cipher modes: ECB, CBC, CTR, OFB, CFB, f8, XTS, CCM, GCM
* Hash (MAC) algorithms: MD5, SHA-1, SHA-256, SHA-512, SHA-512/256, AES-XCBC-MAC, AES-CMAC, CRC-32-IEEE 802.3
* Hash modes: Raw, SSLMAC, HMAC
* DDT packet descriptors
* Multiple cryptographic context support. The number of contexts supported is a configurable parameter
* AXI bus interfaces
* Full DMA master capabilities to bring data into the core and write back. Packet data traverses the bus only twice per packet (once for the read operation, once for the write operation)
* Endian support is configurable to either big-endian or little-endian via an external pin
* Support for secure key area for block cipher algorithms (AES)
* Secure bus available to securely operate in systems which differentiate between secure and normal processing modes

### Public Key Accelerator(PKA)



* RSA (with or without CRT): 256, 512, 768, 1024, 1536, 2048, 3072, and 4096-bit
* ECC-GF(p): 160, 192, 224, 256, 320, 384, 512bit

### True Random Number Generator(TRNG)

* Internal random (re)seed operation
* 256-bit random number generation
* Two separate reseed reminder schedules provide autonomous background reseeding (build-time configuration option)
* Shift register compatible output stream for auxiliary uses such as, DPA, TA, IPsec, and so on (for TRNG product only)
* Status/control I/O for allowing external monitoring of internal actions and states (for TRNG product only)
* Glue-less interface to ESM family entropy port (TRNG for ESM product only)

### Secure UART



* Work at 150MHz
* Simple UART without DMA feature
* For all UART, 16-byte depth transmit and receive FIFO
* 16550 compatible function
  + 5-8 data bits per charater
  + Optional parity bit
  + 1/1.5/2-bit stop bit
* Programmable serial data baud rate as calculated by the following:

Buadrate = sclk/(16xdivisor)

### Secure Timer



* 32-bit APB bus interface, compliance with AMBA 2.0 specification
* Up to 8 programmable timers
* Supports for two operation modes: free-running and user-defined count
* Supports interrupt generation

### Secure Watchdog



* 32-bit APB bus interface, compliance with AMBA 2.0 specification
* Configurable APB data bus widths of 32 bits
* Configurable watchdog counter width of 16 to 32 bits
* Counter counts down from a preset value to 0 to indicate the occurrence of a timeout
* If a timeout occurs watchdog timer can perform one of the following operations:
  + Generate a system reset
  + Generate an interrupt, restarts the timer, and if the timer is not cleared before a second timeout occurs, generate a system reset
* Test mode signal to decrease the time required during functional test