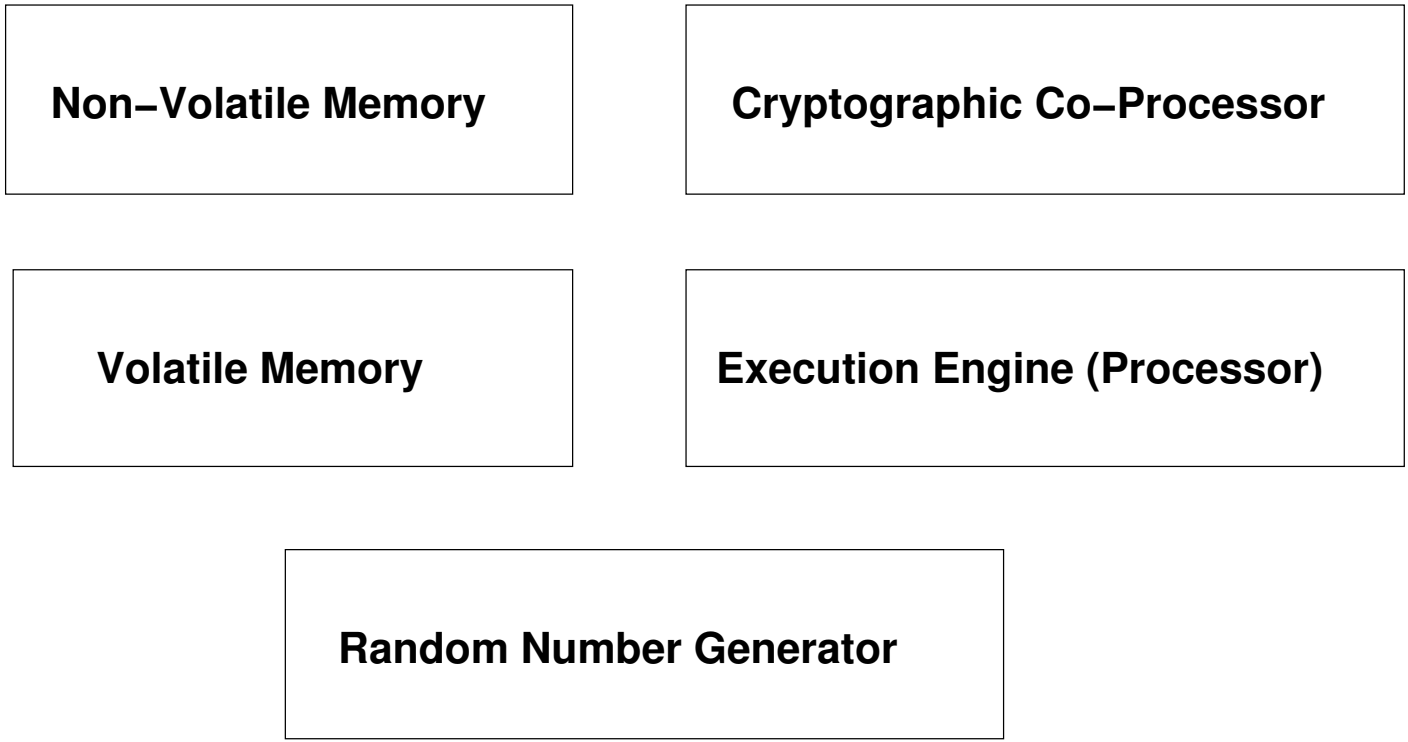
TPM


Non–Volatile Memory
Cryptographic Co–Processor
Volatile Memory
Execution Engine (Processor)
Random Number Generator