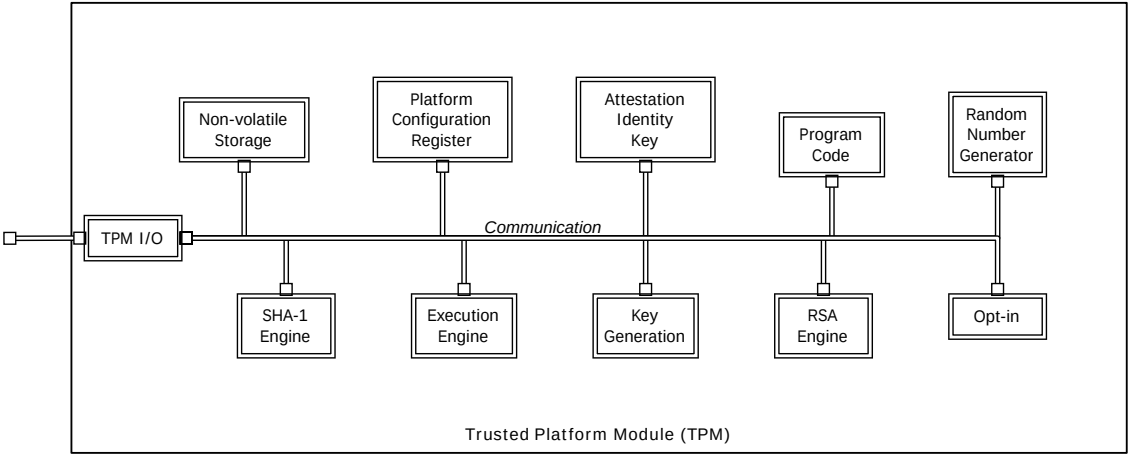
Non-volatile Storage
Platform Configuration Register
Attestation Identity Key
Program Code
Random Number Generator
TPM I/O
Communication
SHA-1 Engine
Execution Engine
Key Generation
RSA Engine
Opt-in
Trusted Platform Module (TPM)