

Tamper-Resistant Envelope

Crypto Engine

Cryptographic Hashing

Random Number Gen

Asymmetric Key Gen

Public Key Encryption

Symmetric Encryption

Endorsement
Certificate

Key Store

Persistent Store

Non-Volatile Memory

Proof Verifier

Execution Engine

SECpack Loader

Virtual Machine

Communication Interface