iChip®

Credential Operating System
A Trusted Platform for

Digital Identity Systems

Low Cost-High Performance
Credential Operating Systems for eID Applications

The iChip® Credential Operating System can be configured for a number of business environments. Based on the export laws of many countries our team can remove or restrict specific algorithms as required. The operating system supports many applications such as National eID, electronic driver's license, Voter ID eHealth, Digital social security, ePassport, VISA etc. These are all available as standard profiles.

The iChip Credential Operating System enables the system integrator to use a variety of authentication algorithms to prove the validity of who an individual is, within each network. Optional on-chip biometric matching is also available for additional binding of a credential to an individual. the privacy and transmission of of data is secured by utilizing ECC, RSA, AES and encryption,. iChip guarantees transaction integrity through FIPS 197 symmetric and asymmetric electronic signatures.

Full lifecycle support is built in and supports 3rd part manufacturing and personalization without any loss of security.

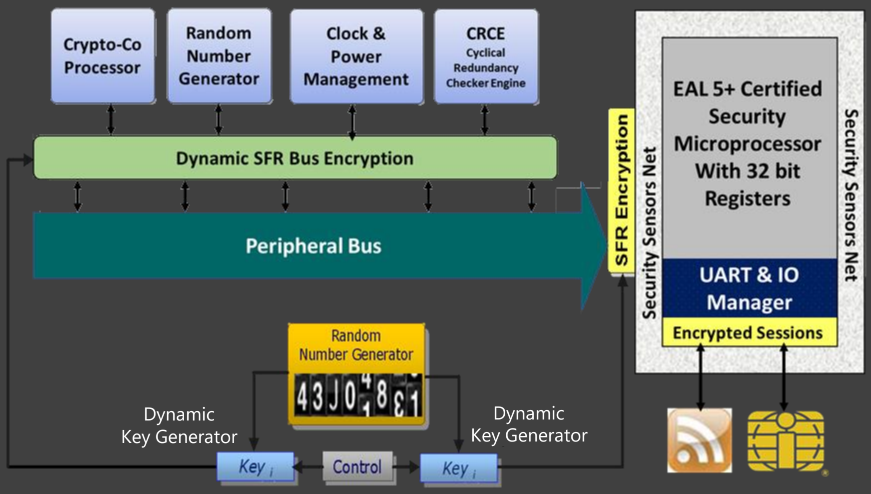
- Integrity Guard based EAL6+ hardware on with Credential OS @ EAL 5+ (high), FIPS 140-2 L3
- Type A & Type B ISO 14443 contactless communication, T=0 & T=1 ISO 7816 contact communication (in dual Interface card option)
- ECC 521, RSA 2048 (RSA 4096 waiting on certification), AES 256, AES192, SEED, SHA256 SHA512 , (TDES2K for BAC only)
- BAC/SAC/AA/EAC support compliant to ICAO 9303 and BSI TR-03110 /
- Multiple security domains and secure post-issuance download
- 20 Byte global unique identifiers (GUID)
- Configurable 7 Byte UID for NFC
- Global PIN with block and unblock features
- Special transport keys for lifecycle management
- Forensic information commands
- Full ISO TLV file support for cyclical, purse, and linear files
- Optional E-Purse / E-Payment functionality

Security by Design- In every iChip® is World Class Certified Protection

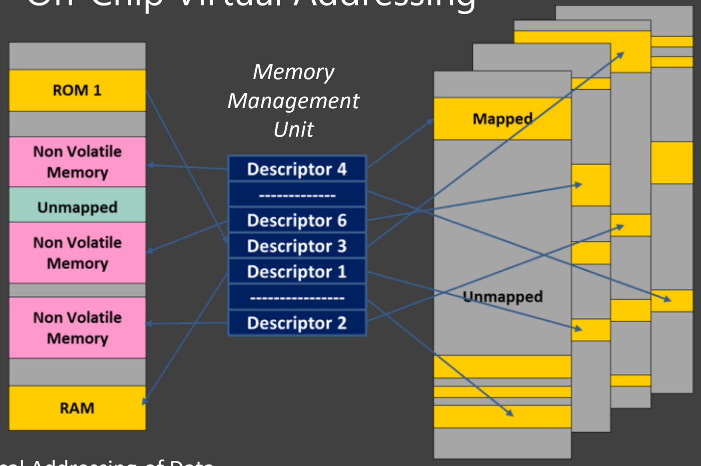
The iChip CPU, Crypto-Coprocessor and embedded crypto libraries are hardened against all known types of side channel attacks this includes SPA, DPA and DFA.

- Chip architecture - Integrity Guard CPU
- Anti-Tearing (Atomic) transaction mechanisms in the OS and chip hardware
- All data at rest is encrypted
- External chip attack detection
- Virtualization of the data across the non-volatile memory
- Consistent load level returns regardless of operations through secure a (Memory Management Unit MMU)
- Active on-chip rotating encryption for all memory and buffers
- All data on bus is dynamically encrypted
- Masked key transfer (half key load)
- Corruption check for data transfers
- Secure lifecycle and key management

High Security Design

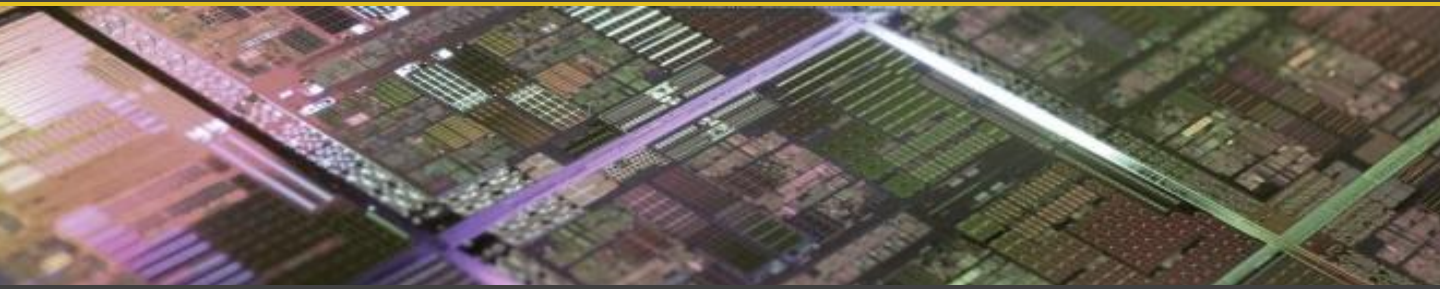


On-Chip Virtual Addressing



Physical Addressing of Data

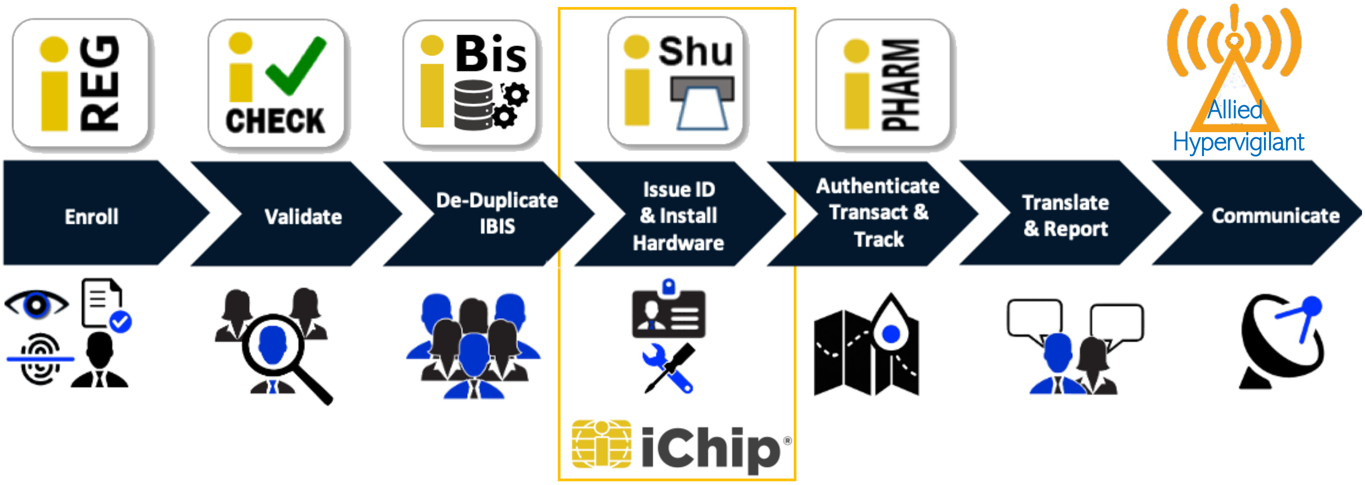
Virtual Addressing of Data



iChip®

Call us today +1 747-215-9200

The iChip® Credential Operating System is an Integral Part of a Full ID Platform



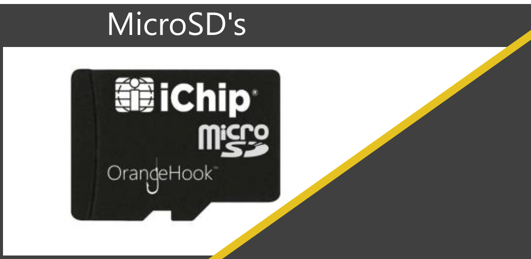
iChip® is built to these standards

FIPS VALIDATED 140-2 · Common Criteria · INTEGRITY GUARD

ePassports

Cards

MicroSD's



NFC Tags

Inlays

Call us today +1 747-215-9200

ALLIED IDENTITY