Product Spec

Company Overview

jNet Technology is in the business of developing JavaCard & Global Platform Operating Systems under contract with silicon manufacturers, Government Departments and Agencies and Commercial Businesses both foreign and domestic.

Java Card / Global Platform OS

From its inception, jNet's JavaOS family was developed as highly secure and scalable card operating system that meets the stringent requirements of Government ID and ePassport, medical, banking, secure token and other vertical smart card sectors. Its portable Java VM execution engine has been optimized for 16-bit processors. Its internal data structures break Java Card's 16-bit limitations in addressing modes to support extended memories above 64KB. Coupled with streamlined method invocation, applet loading & linking, exception processing and persistent memory caching sub-systems, its run-time performance is often faster than other interpreter-based Java Cards. A typical jNet's JavaCard / Global Platform mask includes Java Card Virtual Machine (JCVM), Java Card Runtime Environment (JCRE), Java Card API class libraries, Crypto library, Global Platform implementation and any optional applets integrated in ROM. The advanced cryptographic and vertical market accelerators provide the "unfair competitive advantage" to system solution providers because they offer near native performance for their deployed applets yet minimize their size and complexity by providing the needed functionality built-into the JavaOS itself. The silicon provider's crypto library implementation for its DES, RSA, AES and ECC operations include the built-in countermeasures and protection profile(s) for FIPS 140-2 Level 3 and Common Criteria EAL4+ certifications.

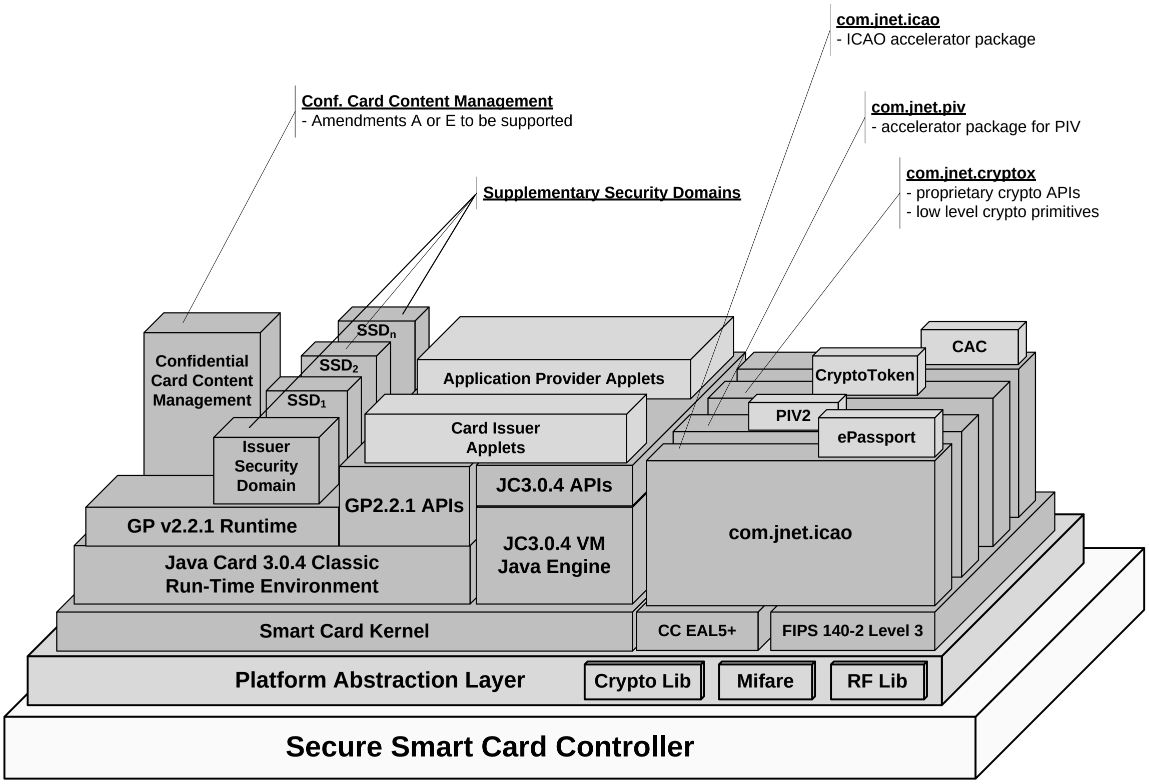
com.jnet.icao
- ICAO accelerator package
Conf. Card Content Management
- Amendments A or E to be supported
com.jnet.piv
- accelerator package for PIV
com.jnet.cryptox
- proprietary crypto APIs
- low level crypto primitives
Supplementary Security Domains
SSDn
SSD2
SSD1
Confidential Card Content Management
Application Provider Applets
CAC
CryptoToken
PIV2
ePassport
Issuer Security Domain
Card Issuer Applets
JC3.0.4 APIs
GP2.2.1 APIs
GP v2.2.1 Runtime
JC3.0.4 VM Java Engine
com.jnet.icao
Java Card 3.0.4 Classic Run-Time Environment
Smart Card Kernel
CC EAL5+
FIPS 140-2 Level 3
Platform Abstraction Layer
Crypto Lib
Mifare
RF Lib
Secure Smart Card Controller

Figure 1. Internal representation of jNet's JC304/GP2.2.1 offering.

Technical Specifications (Advanced Information)

Java Card VM v3.0.4 Classic:

- Certified with Oracle (TCK v304 kit)
- FIPS 140-2 Level 3, configurable FIPS-approved mode
- JavaCard Protection Profile for CC EAL4+
- Garbage Collection
  - Compliant with Java Card VM requirements.
  - 100% recovery of all packages and objects
- Optional JC packages supported:
  - RMI, TLV, External (Mifare), Math, Integer, Util, Biometry with match-on-card native library
- Configurable JavaOS components:
  - Persistent Java Heap
  - Transient Java Heap (RAM)
  - Transaction Buffer
  - Java Stack
  - APDU Buffer Size (up to 2K)

Global Platform v2.2.1:

- Physical delete supported for applets and packages.
- Up to 20 logical channels supported
- Full lifecycles implementation
- CVM plug-ins supported
- Multiple Supplementary Security Domains with Delegated Management, Extradition, DAP, Tokens Verify & Receipts Generation\
- Amendment-A: Confidential Content Management
- Global Services
- Secure Chanel Protocols:
- SCP-01
- SCP-02
- SCP-03

Persistent Memory Cache:

- Caches NVM pages in RAM during Java applet loading & linking phase to eliminate unnecessary writes into NVM and speed up loading process.
- Object fields cache (lazy write) to reduce NVM wear

Personalizaton:

- Advanced manufacturing features available (cloning, high speed personalization, keysets injection)
- Proprietary production features integrated per user requirements.

Communication Protocols:

- ISO 7816 with T=0 & T=1 with configurable baud rates
- ISO14443 Type A & B, up to 848kbits/sec data rates
- Fast, asymmetric personalization baud rates supported. Extended APDUs and chaining.

Cipher Algorithms:

DES CBC/ECB: NOPAD, ISO9797_M1, ISO9797_M2
AES: CBC and ECB BLOCK128_NOPAD
SEED: Korean SEED with CBC and ECB _NOPAD
RSA: NOPAD, PKCS1, PKCS3

Signature Algorithms:

DES MAC8/MAC4: NOPAD, ISO9797_M1 & _M2
AES MAC128: NOPAD
RSA: SHA_ISO9796, SHA_PKCS1, MD5_PKCS1
ECC: ECC over GF(p) & GF(2m), Brainpool or NIST

Key Agreement:

DH & ECDH: supported

Random Number Algorithms:

PSEUDO_RANDOM, SECURE_RANDOM

Message Digest & Initialized Message Digest Algorithms:

SHA-1, SHA-224/256/384/512
MD5, RIPEMD160 (deprecated, optional)

Key Sizes:

DES: 64/128/192 bits
AES: 128/192/256 bits
RSA: 1024 – 4096
ECC: up to 521-bit for GF(p), up to 409-bit for GF(2m)

Key Types (includes all JC3.0.x transient keys):
DES, AES, SEED: PERSISTENT, TRANSIENT
RSA: PUBLIC, PRIVATE, CRT_PRIVATE
ECC: PUBLIC, PRIVATE

JavaCard Acceleration Packages:

- ICAO: BAC, AA, BSI EAC, PACE
- PIV2 FIPS-201:
- Opacity – all features supported:
- com.jnet.cryptox – low level primitives & proprietary services providing direct mapping to crypto processor

Applets Integrated in ROM (optional):

- Banking: VSDC and/or MChip/PayPass
- ePassport (ICAO 9303 with BAC, AA and EAC)
- v2 CAC (US Government version only)
- PIV2 (FIPS-201)
- Opacity (ICC and SAM roles)