# MULTOS™

PIV Endpoint SP 800-73 fully compliant Solution

**AVAILABLE NOW** (Thank You - Mobile Mind)

**DEMONSTRATING TODAY** (Thank You - Identity Alliance)

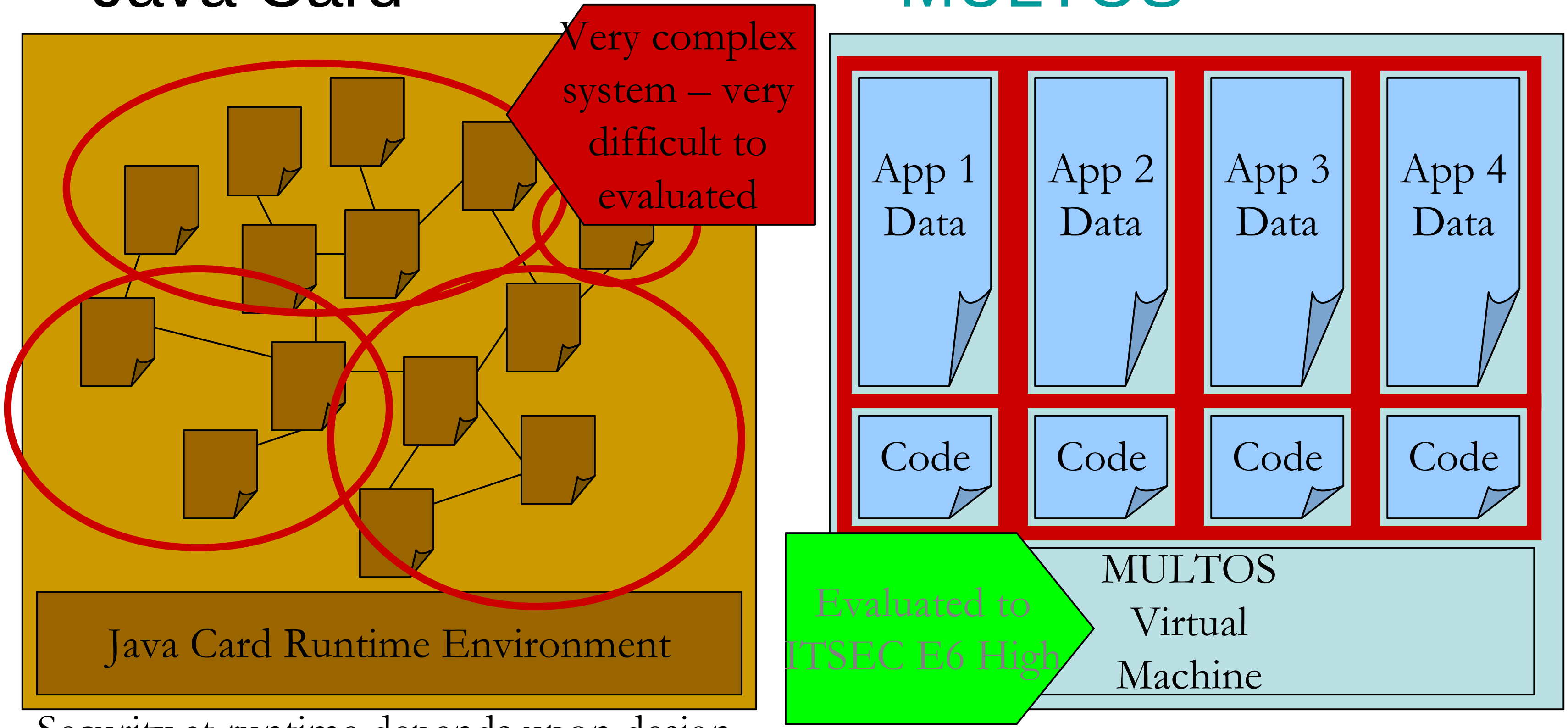
**FIPS 140 EVALUATION PROCEEDING**

# GOOD NEWS

- Substantially more secure
- Substantially lower cost of ownership
- Fully maintainable in the field – “keep the first card issued at the same state as the last”
- Multiple inter-department key management relationships
- Growing application catalog for US Govt
  - PIV Endpoint
  - TECSEC Constructive Key Management
  - Identity Alliance ID Ally
  - Precise Biometrics Match on Card

# Security and Evaluation

- Java Card
- MULTOS



Very complex system – very difficult to evaluated

Java Card Runtime Environment

App 1 Data

App 2 Data

App 3 Data

App 4 Data

Code

Code

Code

Code

MULTOS Virtual Machine

Evaluated to ITSEC E6 High

Security at runtime depends upon design of applets separating package contents of objects and methods in shared Java heap NO security is enforced within packages

Security is enforced at runtime by the runtime bytecode interpreter – EVERY memory location access is checked for memory firewall violation

# The Solution

MULTOS™

- All Application separation and authentication of issuer instructions must be handled “On Card.”
- Scheme must use “Asymmetric” keys to give the Issuer full control of the card lifecycle (and to support the privacy needs of any additional department with permission to use an application space)

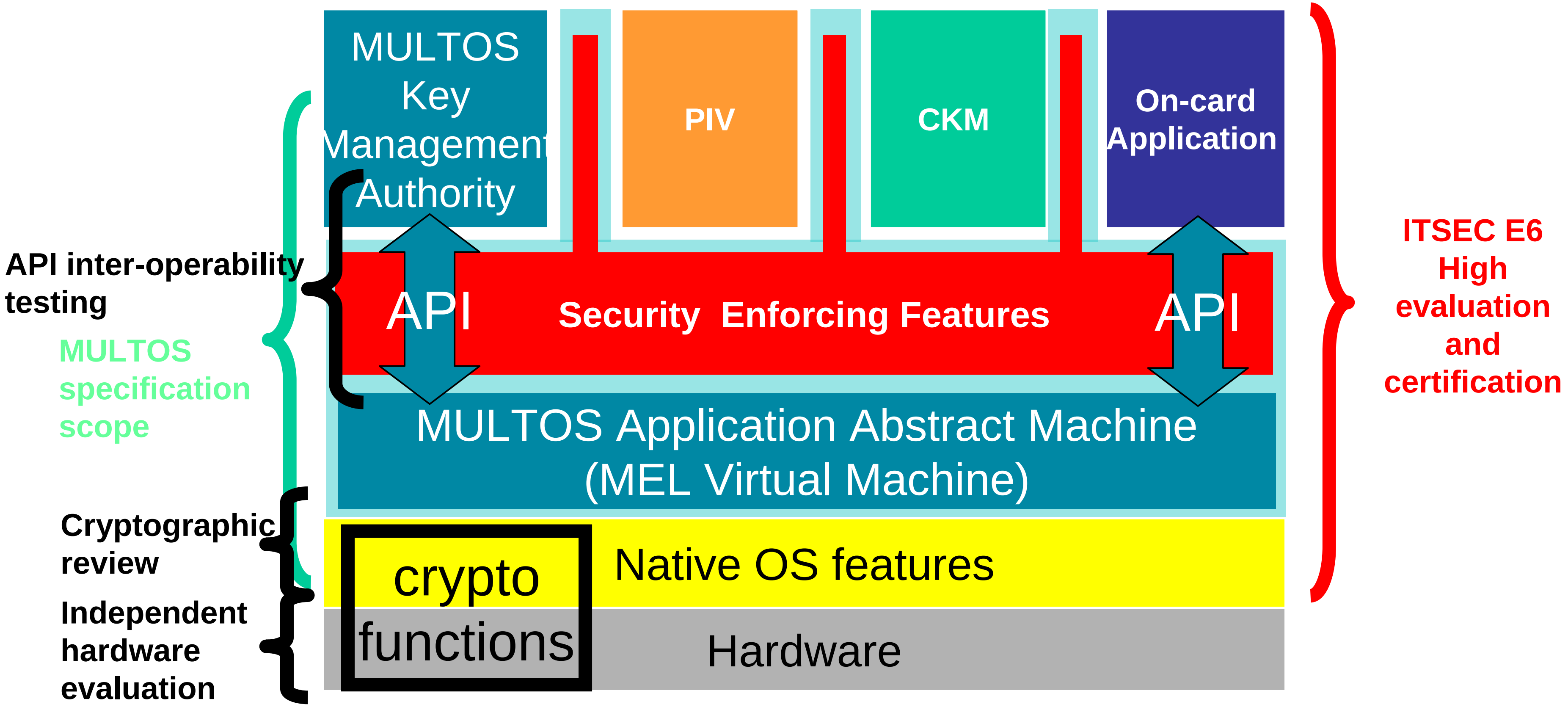
# MULTOS end-to-end security assurance.

- ITSEC E6 High evaluated OS security claims common to all MULTOS Devices:
  1. Applications are only to be loaded onto a card or removed from the card with the permission of the Card Issuer
  2. Applications are to be segregated from other applications - an application may not read from or write to another application's code or data
  3. Loading or Removing an application must have no effect on the code and data of existing applications
  4. The application load process must be able to guarantee the authenticity, integrity and confidentiality of the application code and data

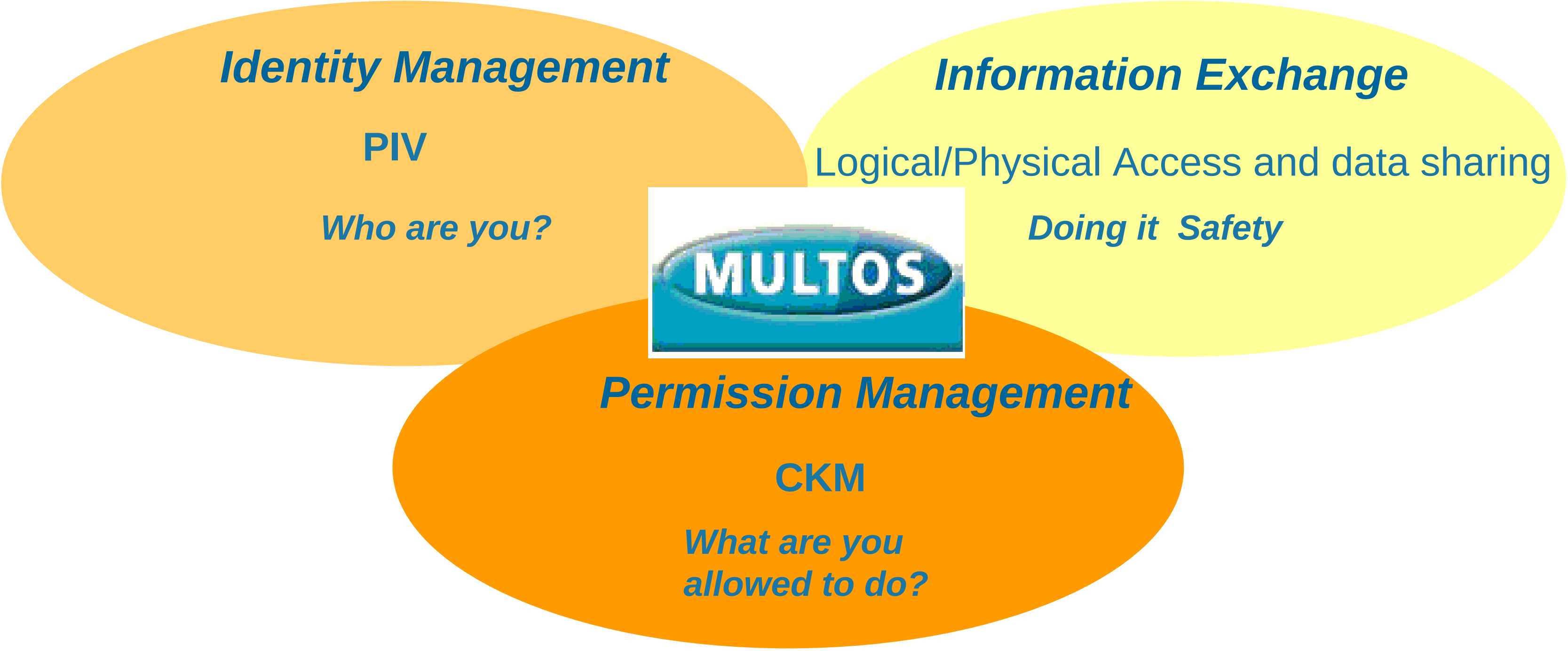
**Security Claims 2, 3 & 4 are UNIQUE to MULTOS**

# MULTOS Type Approval

- MULTOS Consortium and Secretariat defines AND TYPE APPROVES the multi-application smart card environment from end to end
  - API, Virtual Machine & Operating System (including load/delete mechanism)
- This independent third party testing that provides the assurance of interoperability of MULTOS cards – there are no vendor-to-vendor differences


MULTOS Key Management Authority
PIV
CKM
On-card Application
API inter-operability testing
MULTOS specification scope
API
Security Enforcing Features
API
MULTOS Application Abstract Machine (MEL Virtual Machine)
ITSEC E6 High evaluation and certification
Cryptographic review
crypto functions
Native OS features
Independent hardware evaluation
Hardware

# Putting It All Together



*Identity Management*

PIV

*Who are you?*

*Information Exchange*

Logical/Physical Access and data sharing

*Doing it  Safety*

*Permission Management*

CKM

*What are you allowed to do?*

**FIRST RELEASE – 64 K DUAL INTERFACE PIV II + CKM**

**AVAILABLE FOR INTEGRATION NOW**
**EVALUATION UNDERWAY**

# Contact Information

John Wood

415-563-5081

shutowood@comcast.net