

Developing a new Protection Profile for (U)SIM UICC platforms

ICCC 2008, Korea, Jiju

Septembre 2008

JP.Wary/M.Eznack/C.Loiseaux/R.Presty

- **A Protection Profile for (U)SIM Security Requirements**
 - Build a Certification Scheme for multi-application (U)SIM UICC platforms
 - Commercial products roll-out for 2009/2010 timeframe
- **MNO Security Working Group of a French NFC-Payment project (multi banks / Operators)**
 - Contribution of All the 3 french operators
 - Lead by SFR as the Sponsor
 - Reviewed and approved by Bank Members of the project
 - Trusted Labs as consulting and technical writer
- **Milestones**
 - Study : may to October 2008
 - PP edition : end 2008
 - Banks approval : Q1/2008

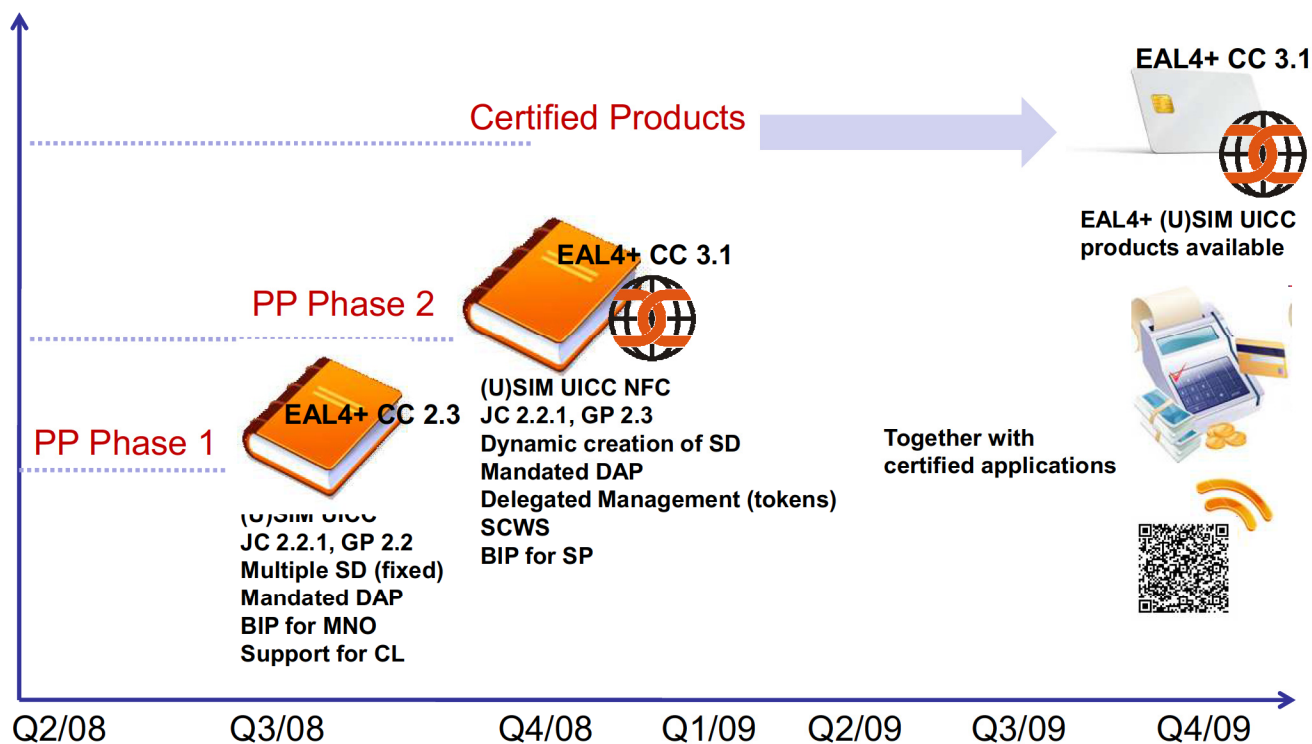
Authors SFR / TL – Restricted

- Mobile Operators wish to develop new value-added services/usages based on (U)SIM UICC platforms
 - Payment
 - Electronic Signature
 - Mobile TV
 - Identity
- This requires (U)SIM UICC security increase in accordance to Service Providers requirements
 - Multi-application isolation
 - High-level of attacks potential
- In the same time, Standard Applications (Operators Domain) are stored on (U)SIM UICC

Standard & Secure Applications shall coexist on a multi-applicative (U)SIM UICC card in accordance with Mobile Operators and Service Providers security requirements.

- Standard applications : transport, Loyalty, phonebook, geolocalization, sim tool kit apps ...
- Secure applications : payment, electronic signature, identity, health, Conditional access ...
- This requires an evaluation standard that could match different types of applications, and different Service Providers requirements
- It has been decided to develop a Common Criteria Protection Profile for the (U)SIM UICC platform that could match various security requirements

Protection Profile Project Timeline



Authors SFR / TL – Restricted

■ A certified and secure platform (U)SIM UICC

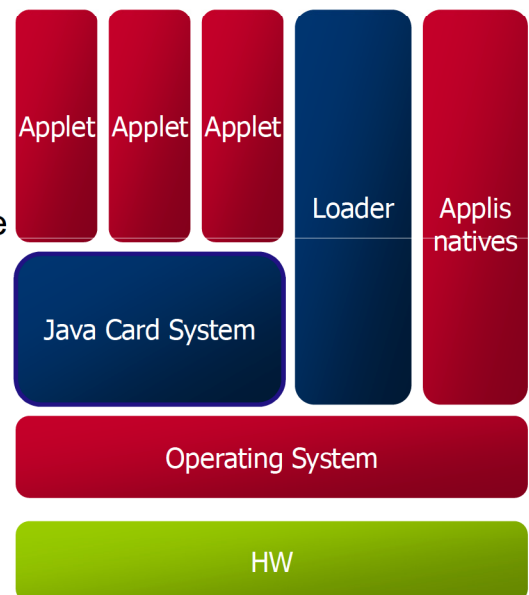
- SIM/USIM JavaCard semi-open & secure
- EAL4 augmented by AVA_VLA.4 certified

■ Host secure applications

- Application Security Level according to Service Providers Risk Assessment
- Common Criteria Certification according to requirements (Banking, SSCD, Identity)

■ Load “non sensitive” standard applications

- No particular assets to protect
- Validated Applications
- (U)SIM UICC platform certificate still valid



■ TOE : a (U)SIM UICC JavaCard platform

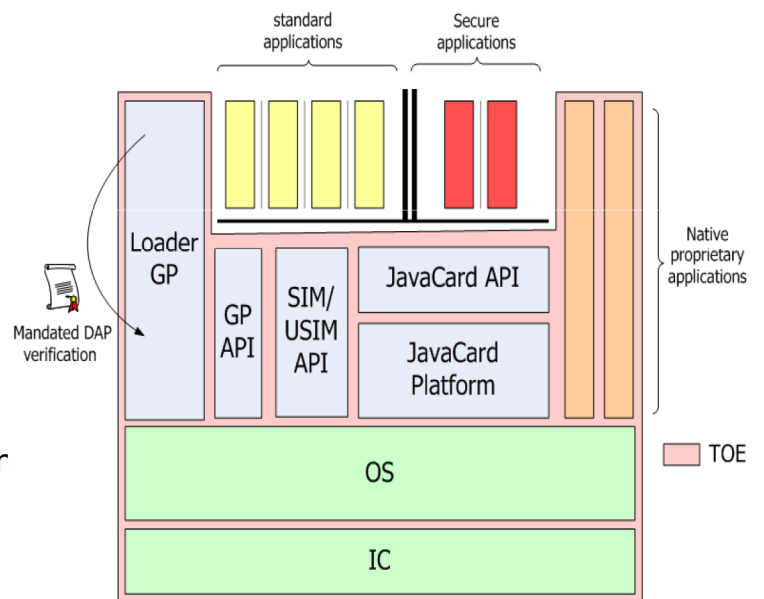
- Security IC + OS + JavaCard System 2.2.1 + Global Platform 2.2 + APIs
- Post issuance downloading of applications

■ TOE Actors

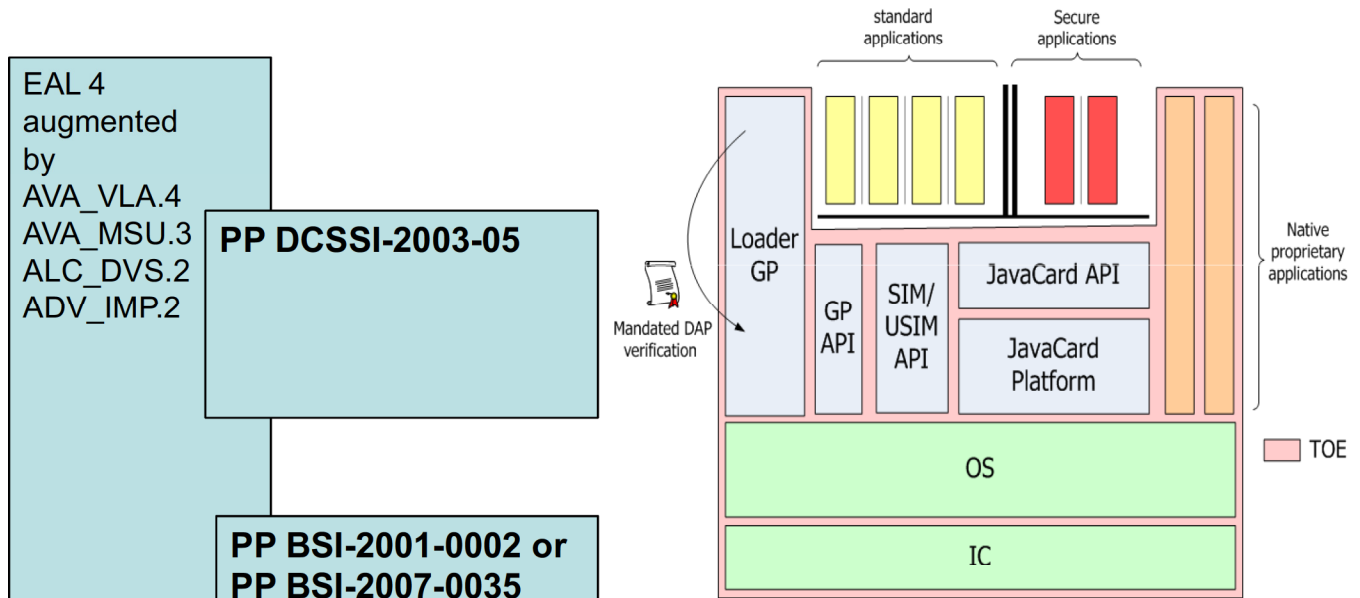
- Mobile Operators
- Service Providers
- Trusted Third Party or verification authority

■ TOE environment

- Standard applications
- Secure applications



Authors SFR / TL – Restricted



Authors SFR / TL – Restricted

■ Security Domains

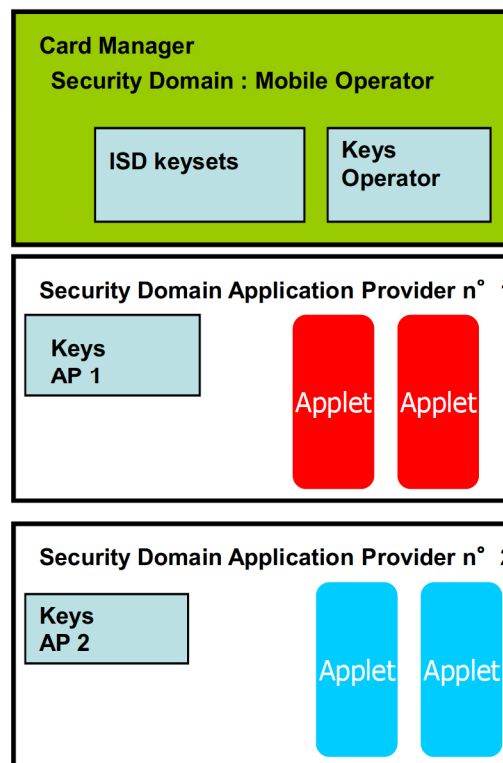
- Created once
- Limited

■ Java Card System

- No native method post-issuance

■ Keys

- APSD temporary keys
- Key escrow



■ Applications

- Validation or Certification
- Mandated DAP signature (Verification authority)

■ OTA platforms

- Secure administration
- Applets download using OTA security
- BIP protocol on for Mobile operators

Authors SFR / TL – Restricted

■ OSP. Standard Applications

- Development following guidance
- Application Verification by approved third party labs:
 - CAP file analysis
 - Byte-code verification
- Mandated DAP signature (Verification authority)

Bytecode verification

- Spec compliance

CAP File → DAP

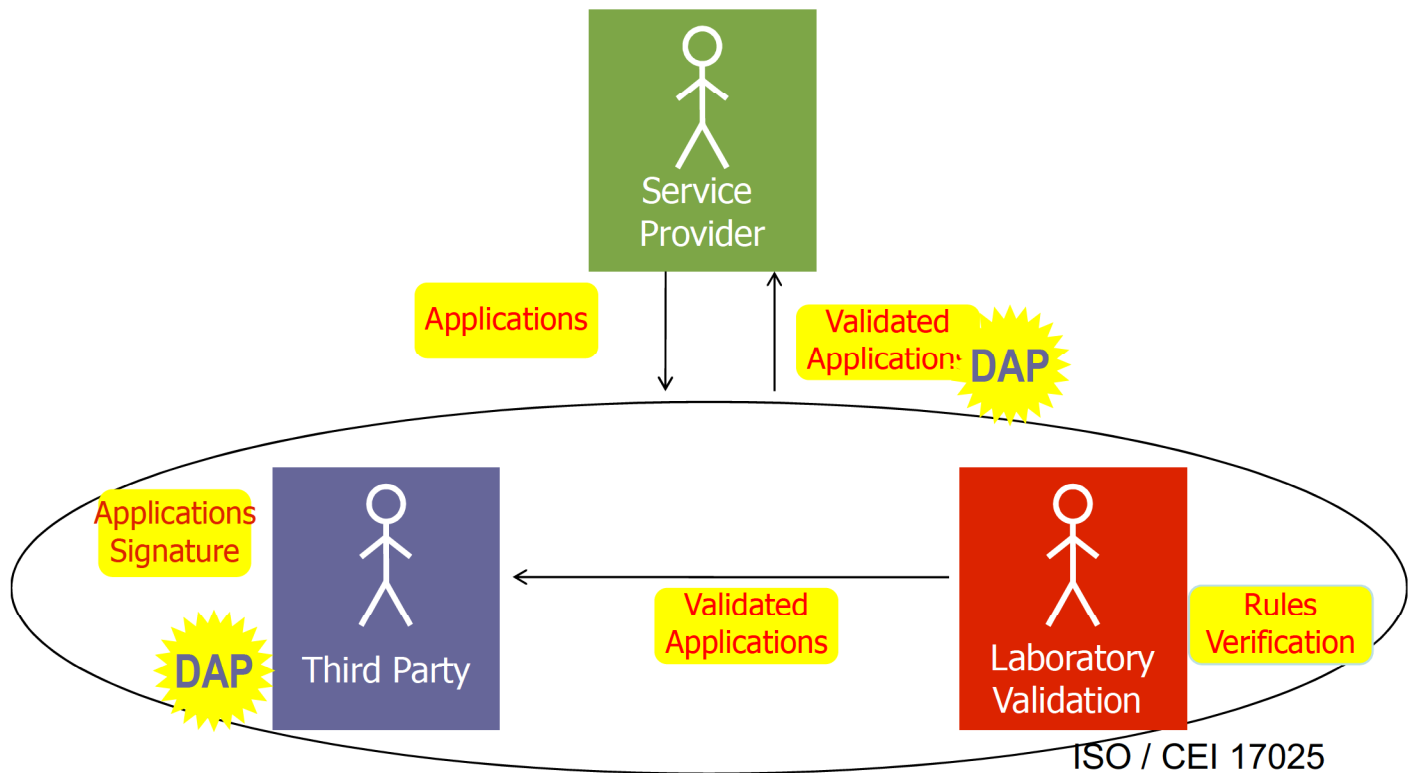
■ OSP. Secure Applications

- Development following guidance
- CC Evaluation & composition with platform according to Service Providers Requirements
- Mandated DAP signature (Verification authority)

Policy compliance

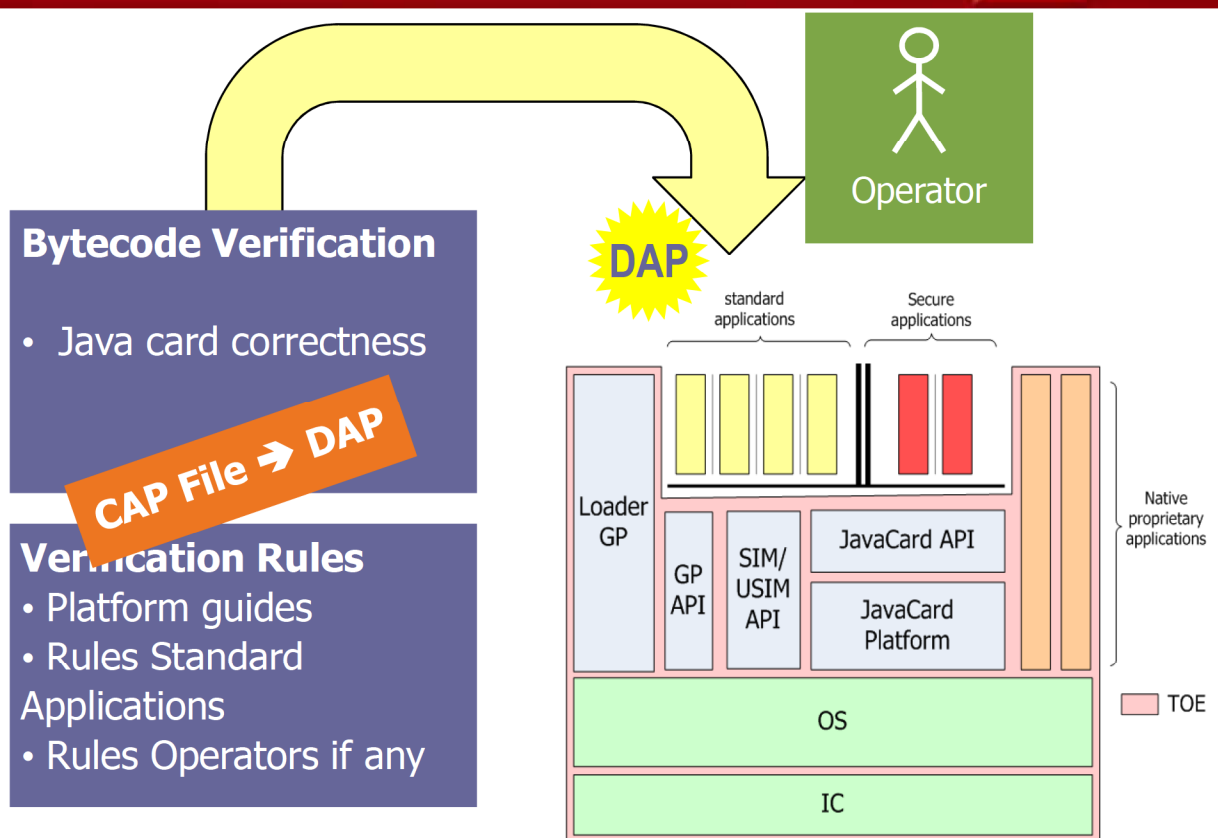
- Guidelines compliance

Authors SFR / TL – Restricted

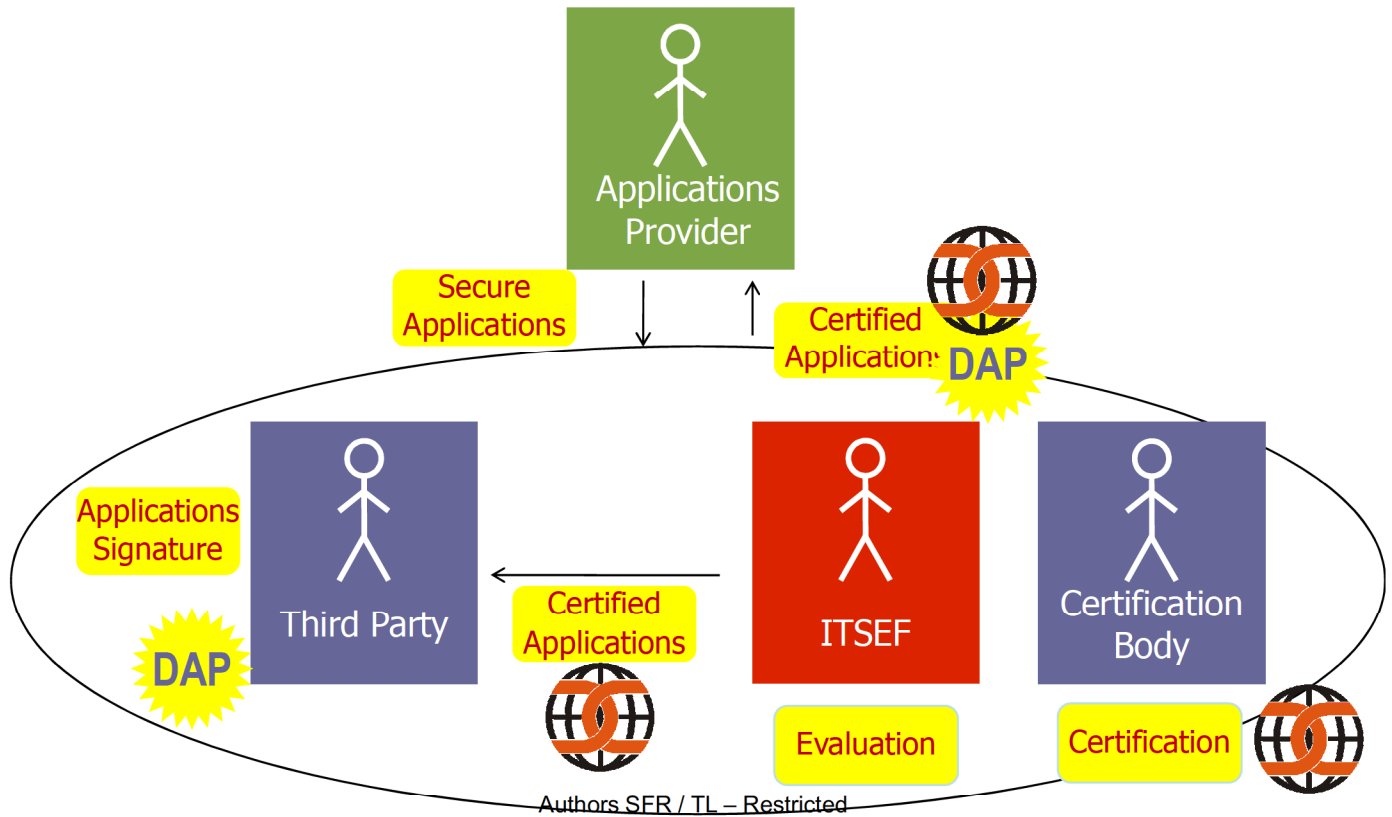


Functional scheme for Standard Applications

SFR



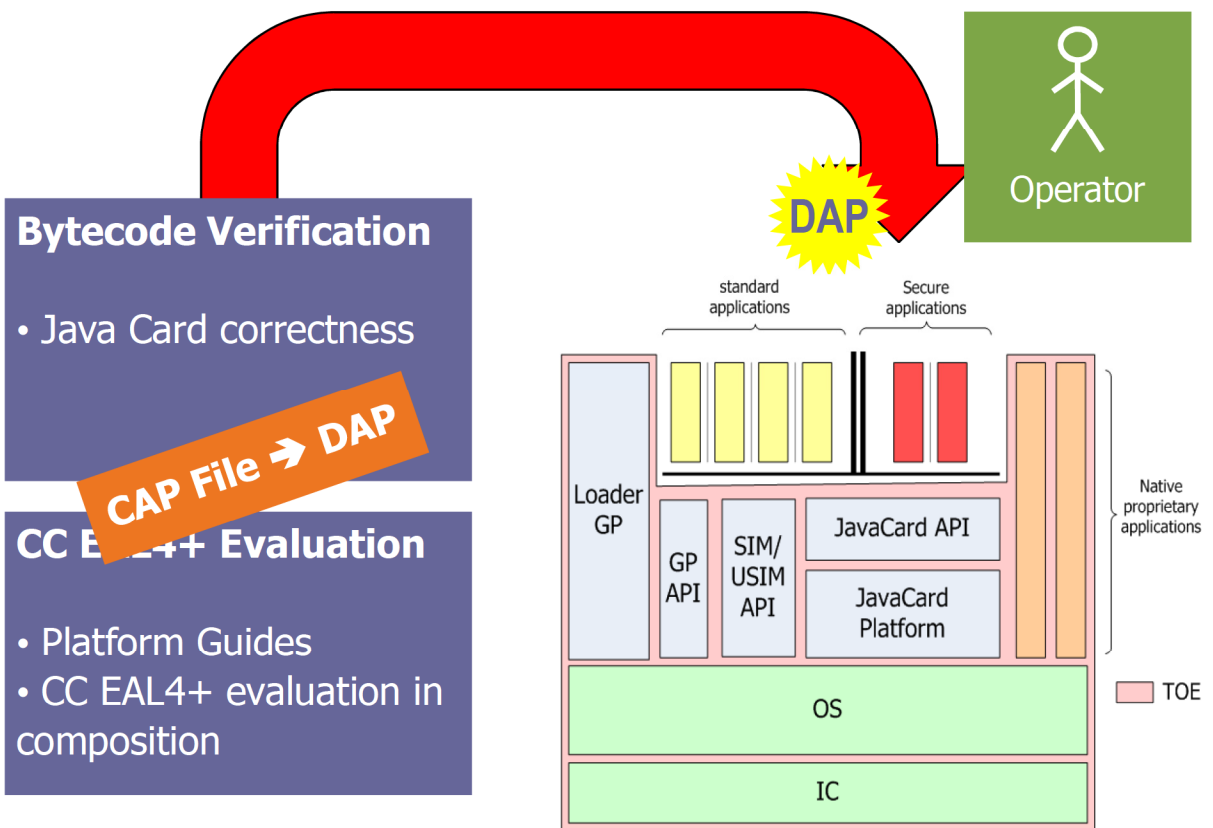
Authors SFR / TL – Restricted



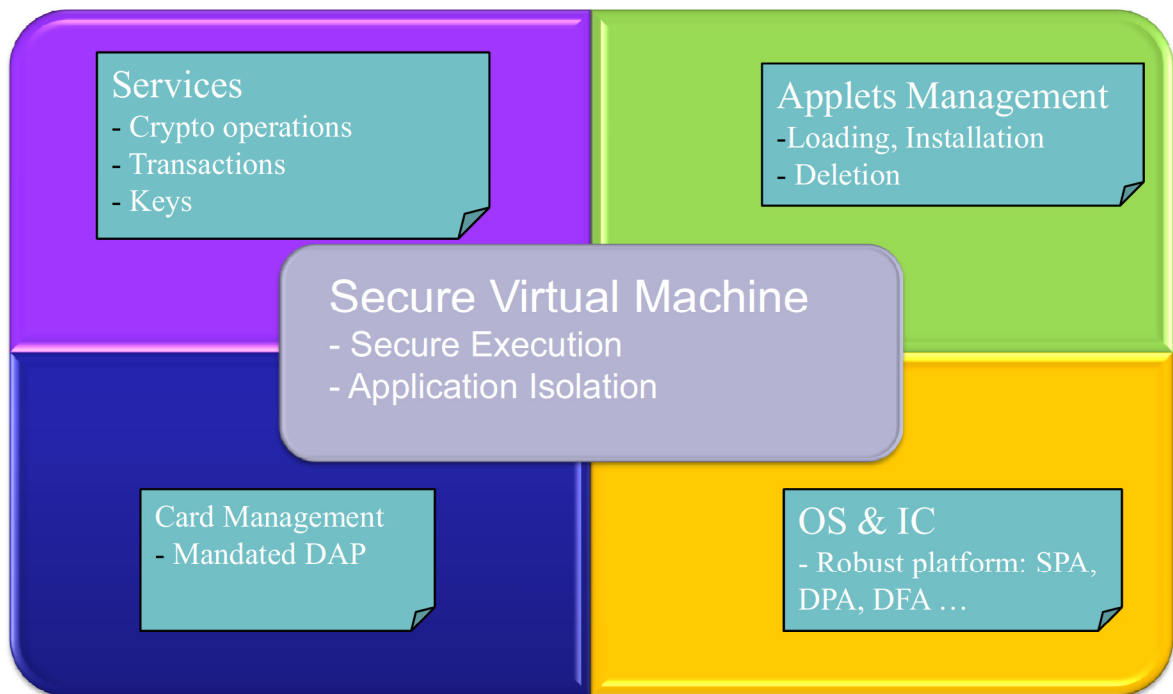
Authors SFR / TL – Restricted

Functional Scheme for Secure Applications

SFR



Authors SFR / TL – Restricted



Authors SFR / TL – Restricted

■ Code Correctness

- Code of applications must strictly comply with JavaCard Virtual Machine specification

■ Collaboration restrictions

- Forbid definition and use of user-defined libraries to standard applications
- It should only use system libraries (included in the TOE)
- Standard applications must not use sharing with any other application
- No RMI

■ Declaration Obligations

- It is important to identify applications for newly identified vulnerabilities
- For such purpose, standard applications must use constants as arguments to some methods

■ Portability rules

- Standard applications only use APIs providing interoperability

■ Platform-specific rules

- Follow platform-specific Development guidance (AGD documents)

Authors SFR / TL – Restricted

- Phase 2 Protection Profile work has already started
- Additional Features
 - Dynamic SD creation and secure keys export (to financial institutions for the management of sensitive assets)
 - BIP communication between applets and SP
 - Smart Card Web Server (tentatively)
 - Delegated management (token)
- Timeline
 - Availability : Q4/2008
 - PP APE evaluation : H1/2009

Questions ?

Comments to:

maryline.eznack@sfr.com

jean-philippe.wary@sfr.com

claire.loiseaux@trusted-labs.fr

renaud.presty@trusted-labs.fr

eric.vetillard@trusted-labs.fr

Authors SFR / TL – Restricted