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

ICCC 2008, Korea, Jiju

Septembre 2008

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

Project Background

- 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

Business Needs

- 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

Scheme Requirements

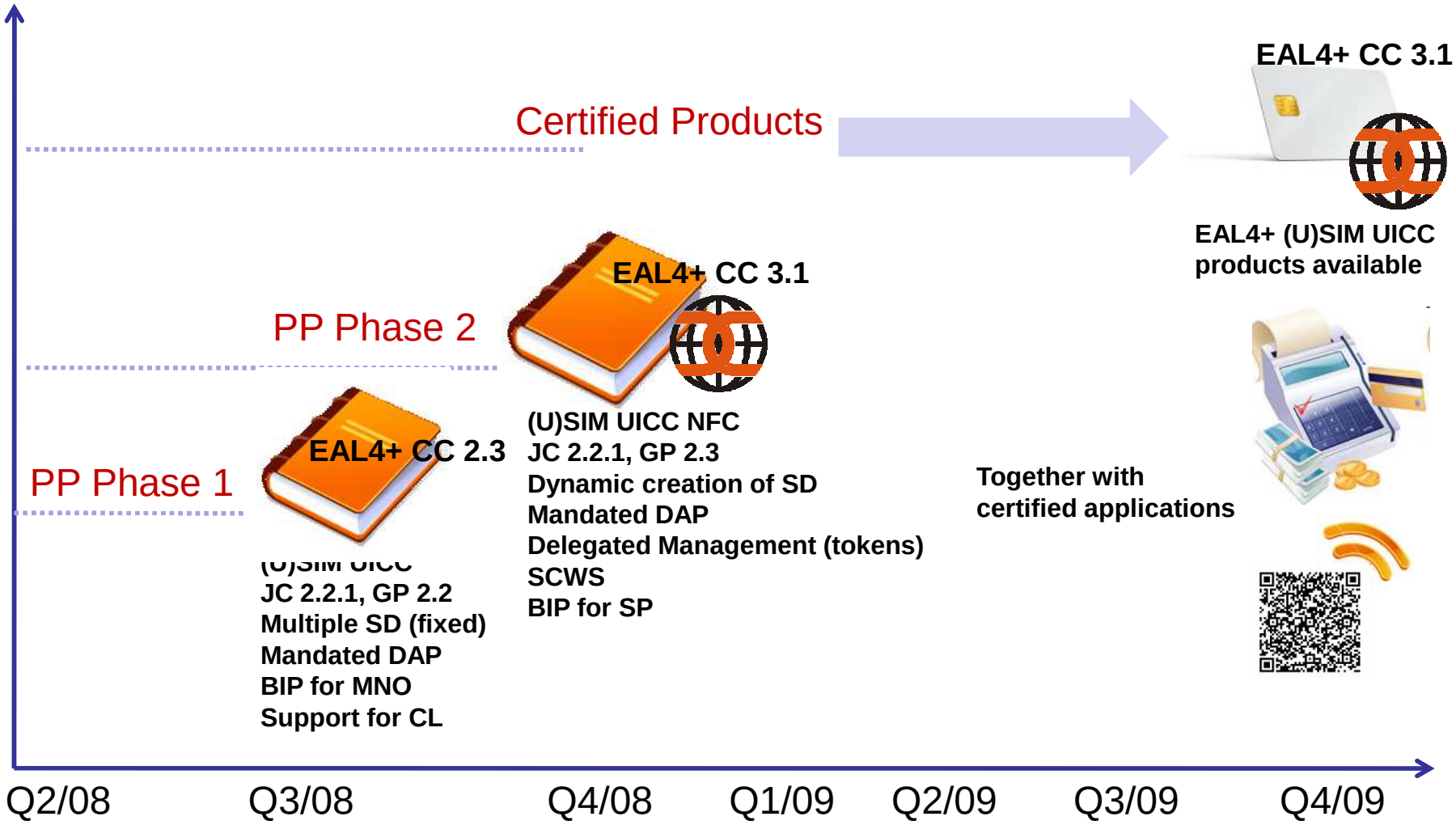
Standard & Secure Applications shall coexist on a multi-applicative (U)SIM UICC card in accordance with Mobile Operators and Service Providers security requirements.

- 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

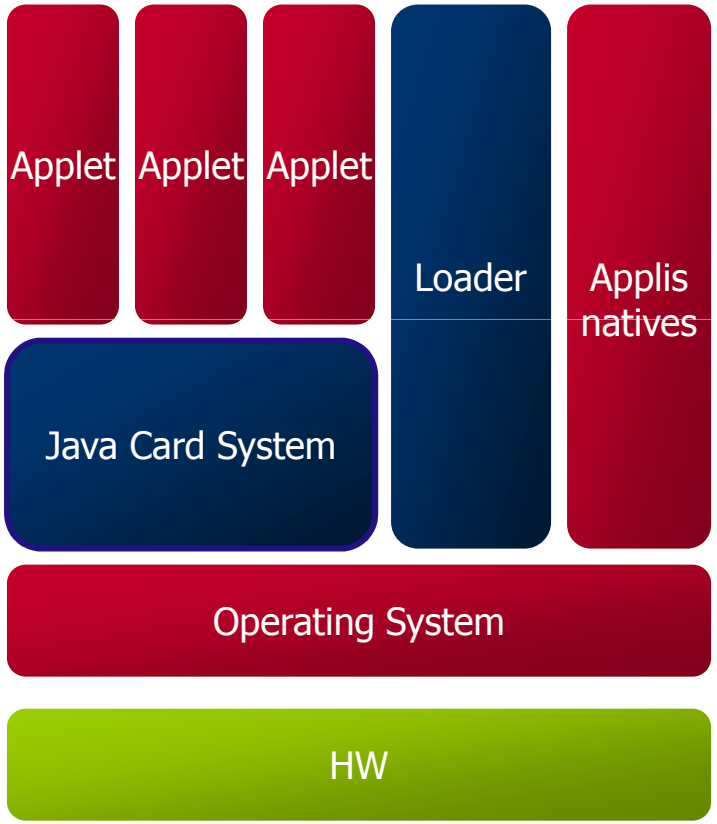
- It has been decided to develop a Common Criteria Protection Profile for the (U)SIM UICC platform that could match various security requirements

Protection Profile Project Timeline



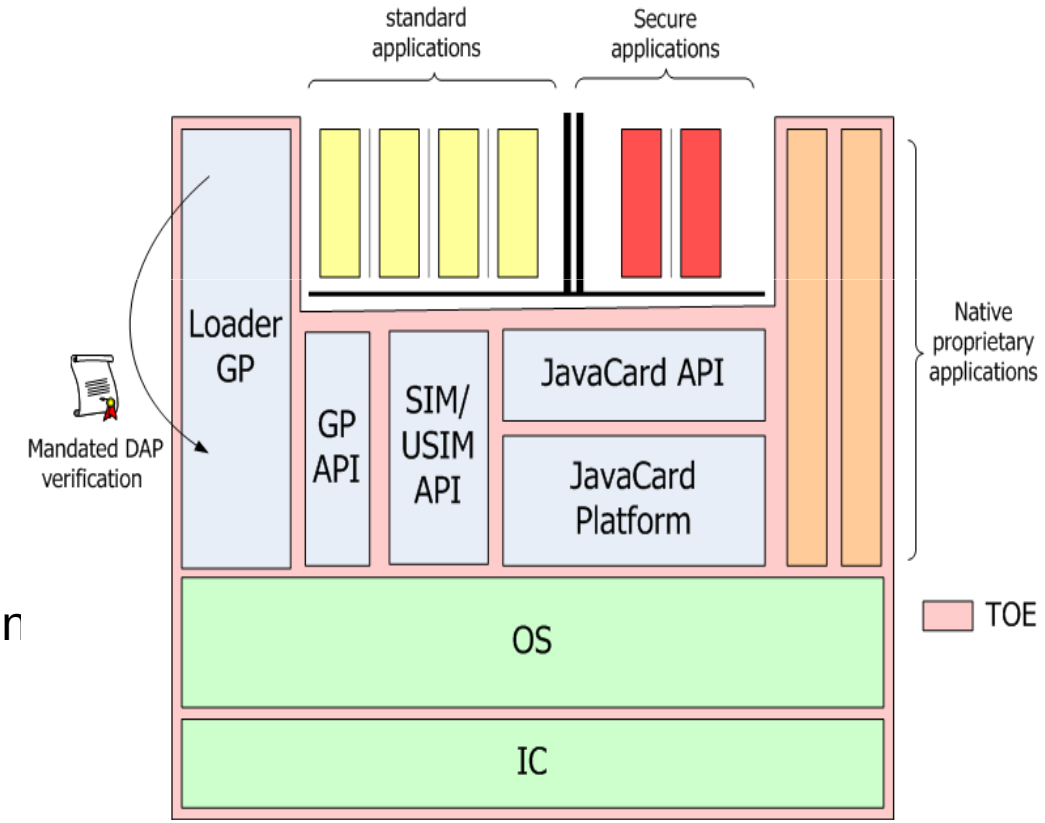
Standard & Secure Applications Chain of Trust

- 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



Phase 1 Protection Profile : TOE Overview

- 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

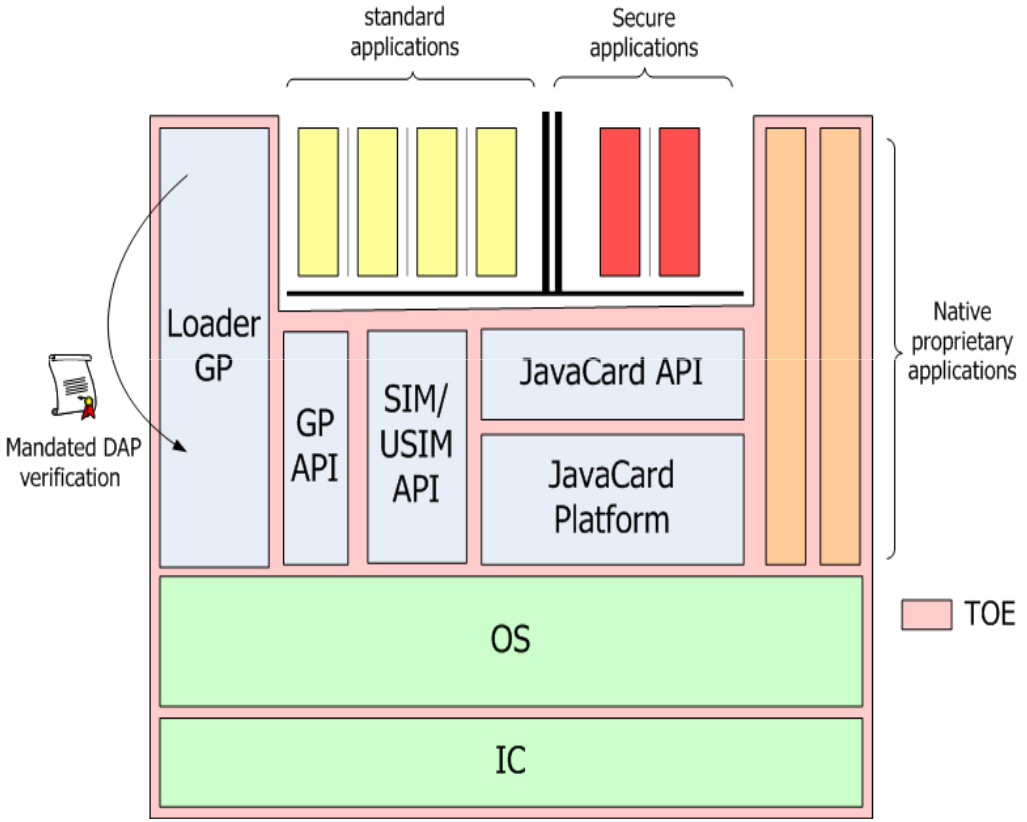


Protection Profile : Conformance claims

EAL 4 augmented by
AVA_VLA.4
AVA_MSU.3
ALC_DVS.2
ADV_IMP.2

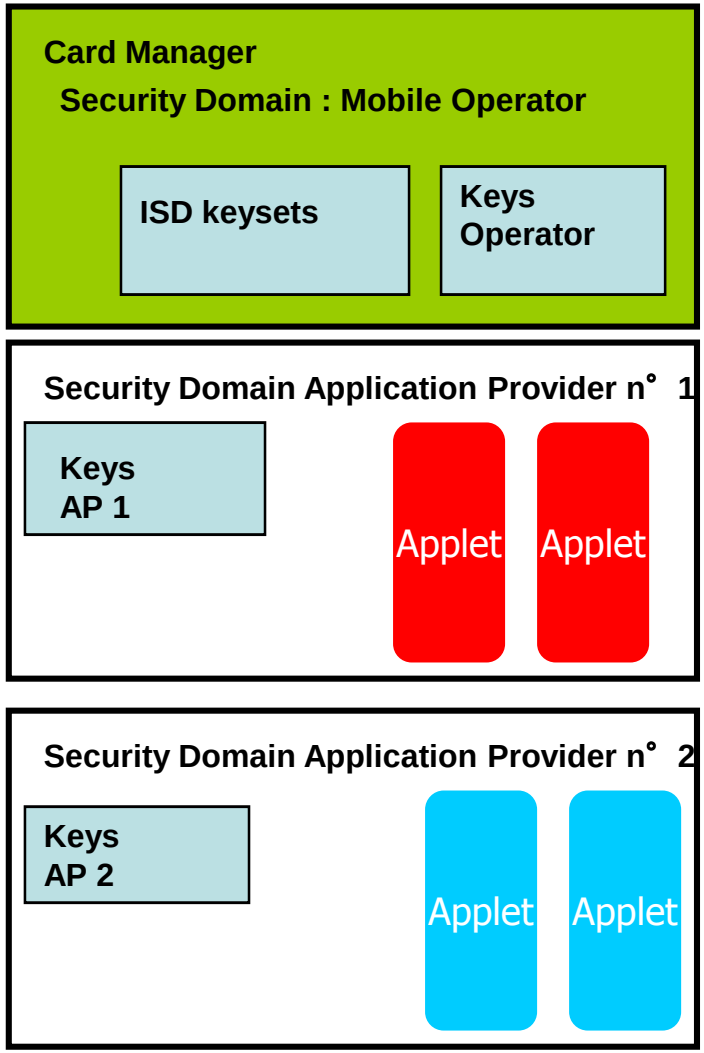
PP DCSSI-2003-05

PP BSI-2001-0002 or PP BSI-2007-0035



Protection Profile : Assumptions

- Security Domains
  - Created once
  - Limited
- Java Card System
  - No native method post-issuance
- Keys
  - APSD temporary keys
  - Key escrow



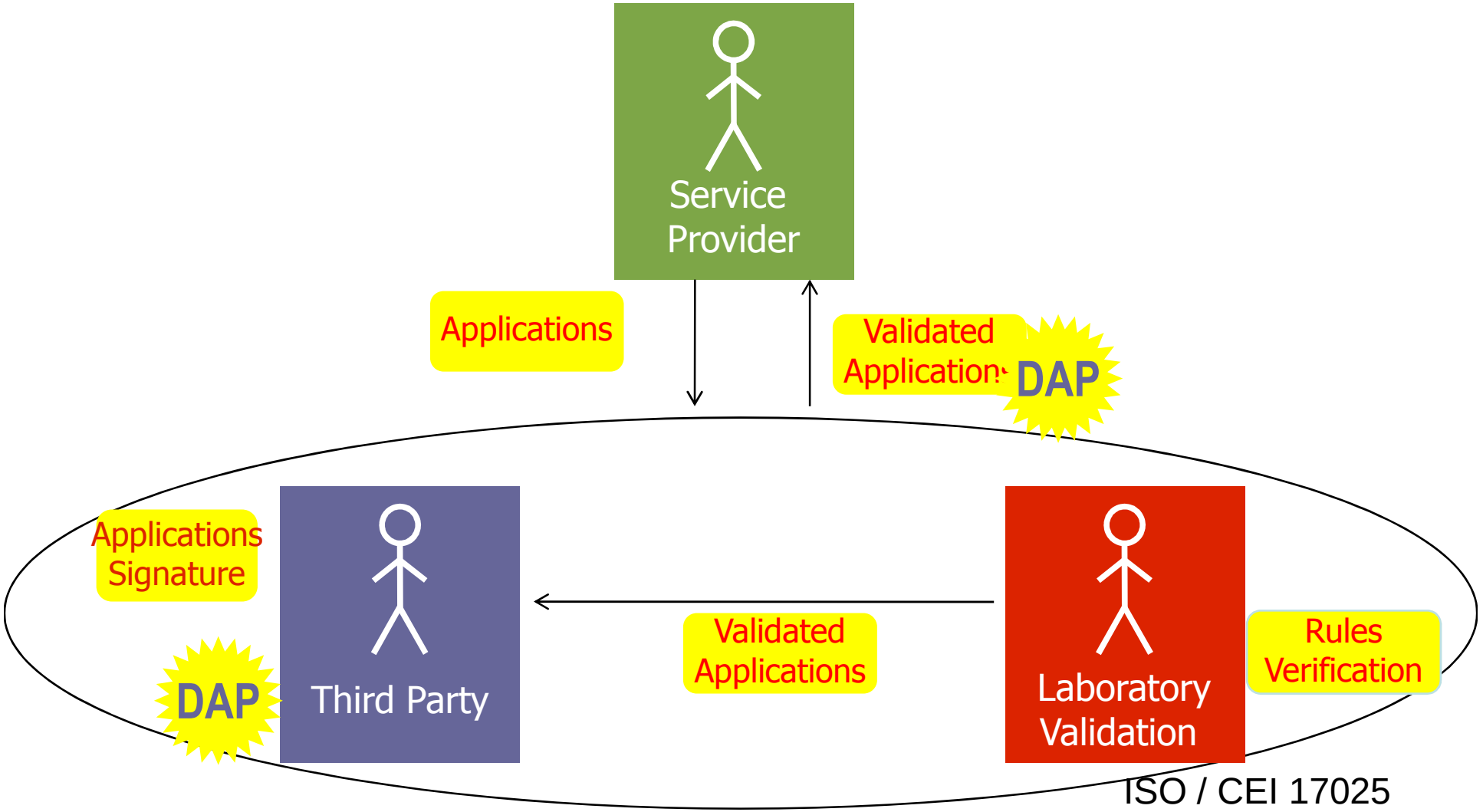
- Applications
  - Validation or Certification
  - Mandated DAP signature (Verification authority)
- OTA platforms
  - Secure administration
  - Applets download using OTA security
  - BIP protocol on for Mobile operators

Protection Profile : Organisational Security Policies

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

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

Functional Scheme for standard applications



ISO / CEI 17025

Functional scheme for Standard Applications

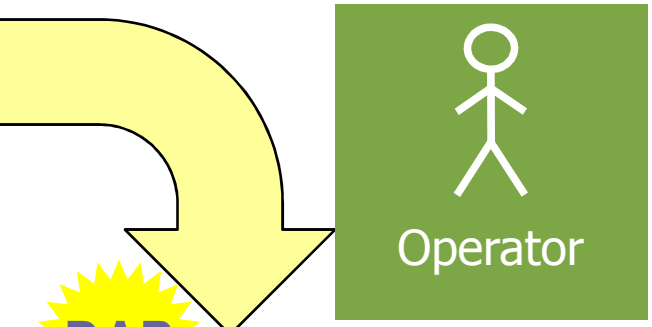
Bytecode Verification

- Java card correctness

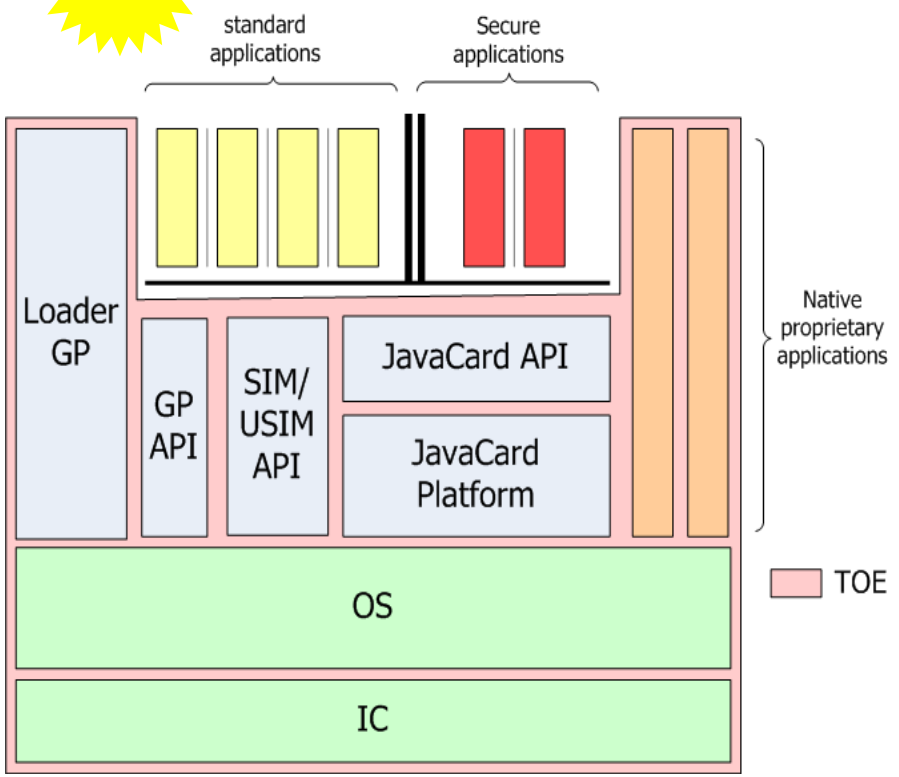
CAP File ➔ DAP

Verification Rules

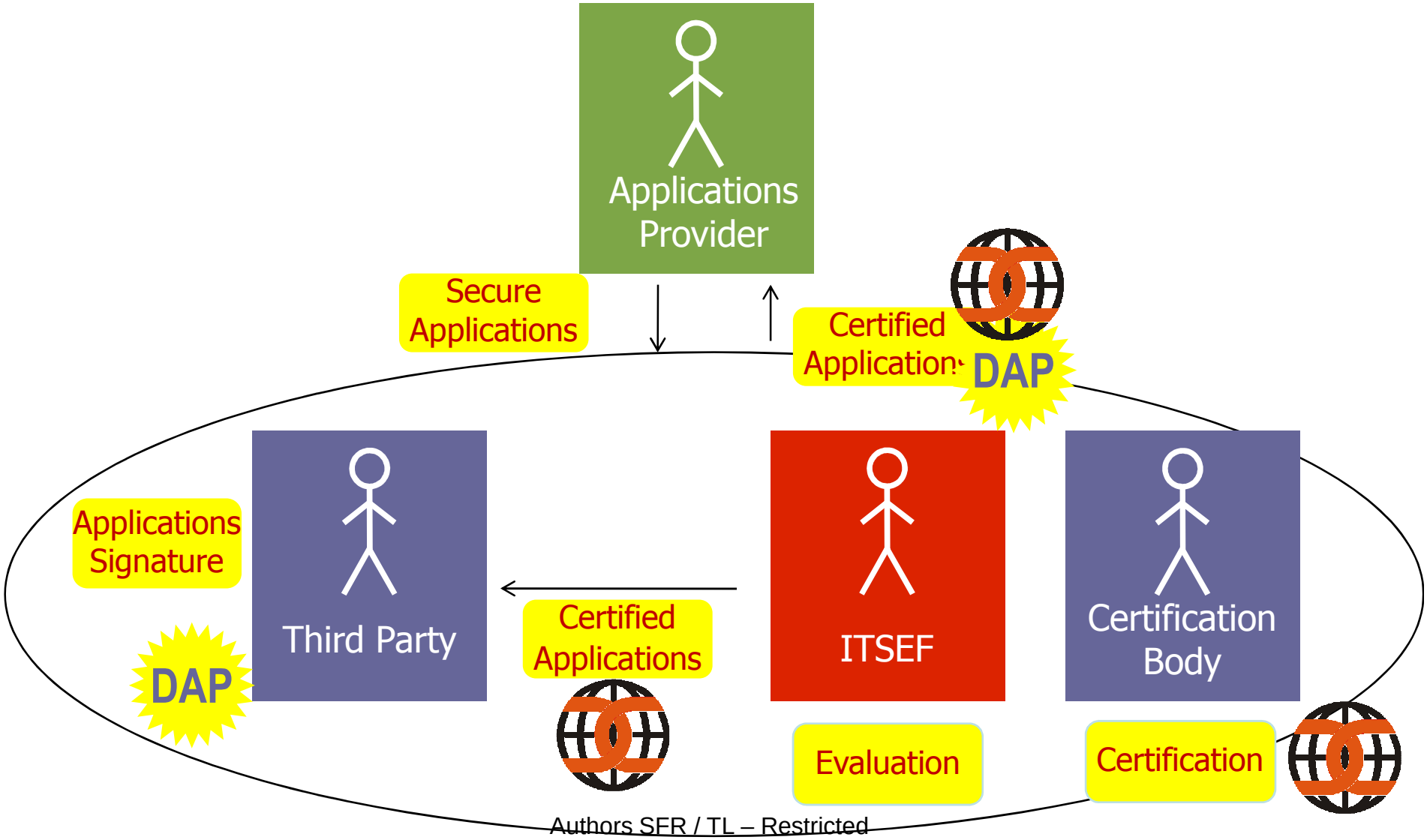
- Platform guides
- Rules Standard Applications
- Rules Operators if any



DAP



Functional Scheme for Secure Applications



Functional Scheme for Secure Applications

SFR

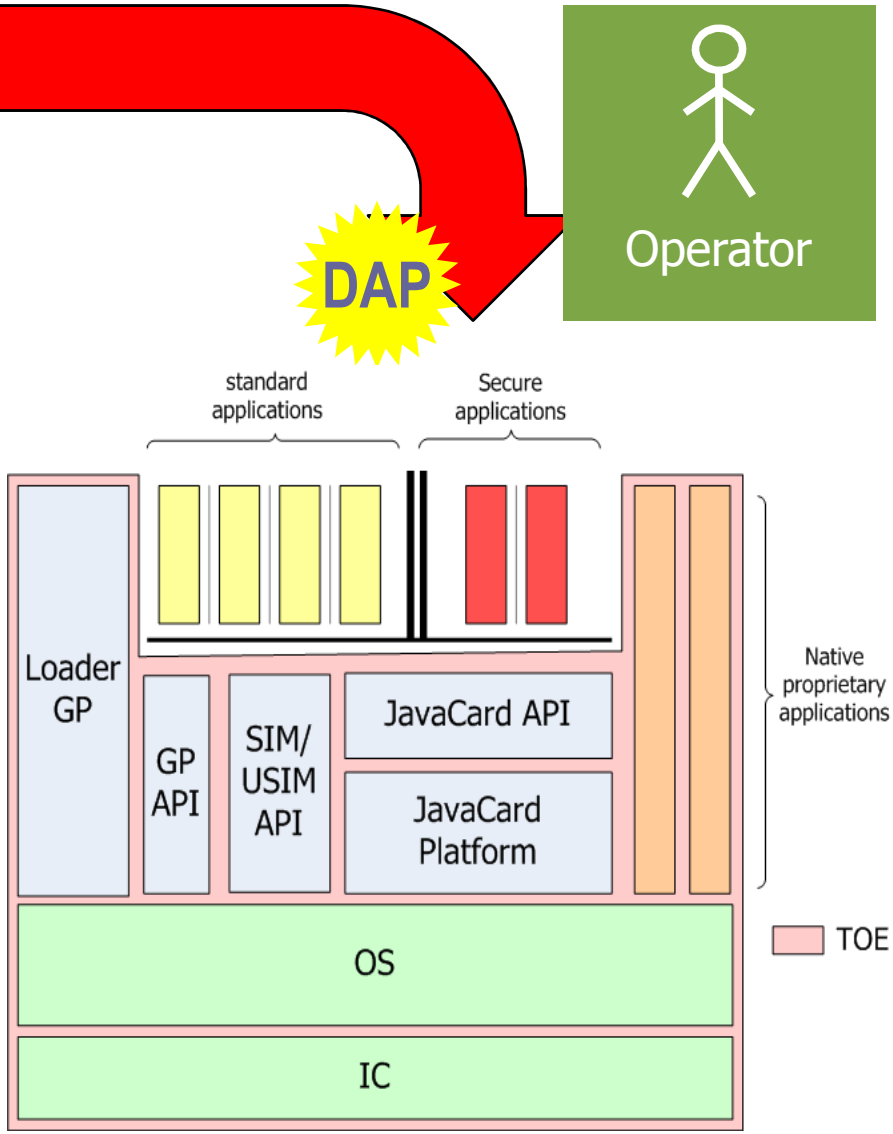
Bytecode Verification

- Java Card correctness

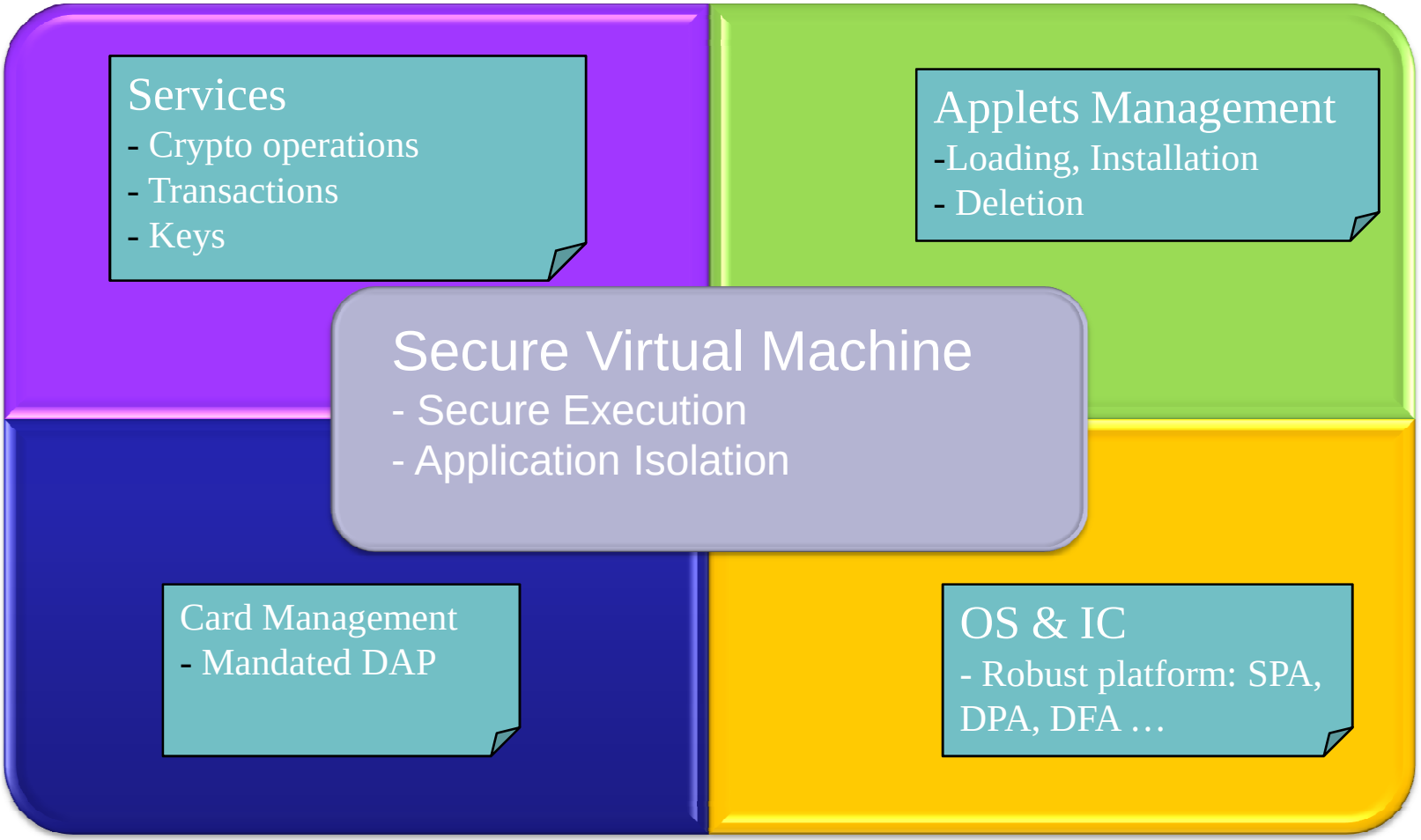
CAP File ➔ DAP

CC E[illegible]4+ Evaluation

- Platform Guides
- CC EAL4+ evaluation in composition



Protection Profile : main Security Objectives



Standard Applications Validation Rules

- 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)

Phase 2 Protection Profile Next Steps

- 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