

Composite evaluation of (U)SIM applications

R. Atoui¹, G. Dufay¹, M. Eznack², C. Lavatelli¹,
C. Loiseaux¹ and J.-P. Wary²

1 Trusted Labs, 5 rue du Bailliage 78000 Versailles, France

2 SFR, 1 Place Carpeaux 92915 Paris La Défense, France

ICCC 2009
September 22nd – 24th
Tromsø, Norway



Contents



- Context and goals
- Three experiences on composite evaluation
 - PP (U)SIM
 - Signature application on top of Java Card platform
 - Generic ST for mobile payment
- Outcomes



Goals



Evaluate sensitive applications on top of deployed certified open platforms

- Reuse of certificates : composite evaluation
- Reuse of certified products : open platform, on-the-field application loading

Tackle the challenge for (U)SIM

- Solve technical issues
- Facilitate the application evaluation process



Three axes of work and derived goals



1. Protection Profile for (U)SIM open platforms
 - A step towards the security interoperability of applications

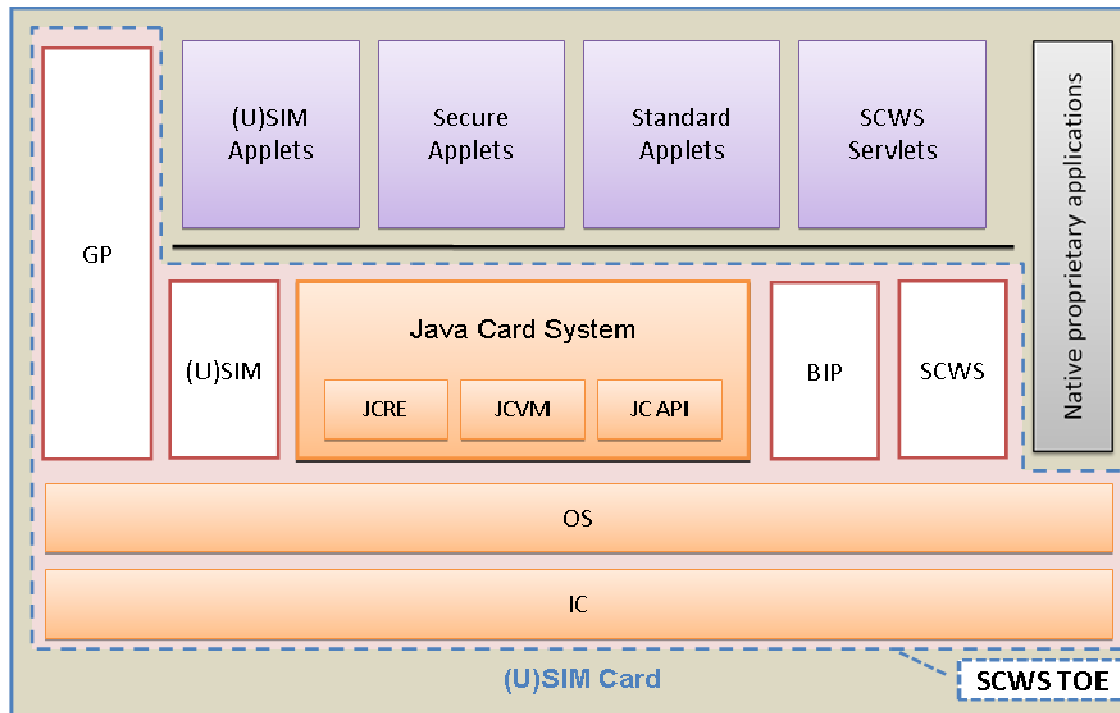
2. Composite evaluation of a signature application using [CCDB-2007-09-001]
 - Best practices for Application Providers

3. Generic security target for « Payez Mobile » Contactless Payment Application Package:
 - Extension of the composite approach to applicative Protection Profiles

[CCDB-2007-09-001] « Composite product evaluation for smartcards and similar devices »



(U)SIM Protection Profile



IC certified BSI-PP-0035

Conformant to Java Card PP

Post-issuance application loading
with DAP verification

- Under evaluation within French scheme ANSSI: expected by November 2009
- Presented to ICCC 2008



Composite evaluation of application



- Signature application on top of certified Java Card open platform
 - Product reference: jTOPv27-ASEv1 v1.0
 - Developers: Trusted Labs, Trusted Logic, Infineon Technologies AG
 - Sponsor: SFR
- Evaluation (EAL4+) in the framework of French scheme ANSSI
 - ITSEF Serma Technologies
 - 3 months long
 - Certificate DCSSI-2009/02
 - Presented at Cartes 2008
- Based on [CCDB-2007-09-001]
 - Interpretation of ASE_COMP for ST writing



ASE_COMP: generic approach (1)

- Non-contradiction assessment between Composite-ST and Platform-ST
- Hints for Composite-ST writing
 - Composite-ST independent of the platform using « standard practice »
 - Statement of compatibility of Composite-ST and Platform-ST
- Consequences
 - Composite-ST contains Platform-ST elements at all levels (threats, objectives, SFRs)
 - TSFI derived from the Composite-ST larger than required for evaluation
 - Statement of compatibility used to restrict the evaluation scope



ASE_COMP: generic approach (2)

- Scenarios that justify the generic approach
 1. Platform (type) unknown (eg Composite-ST developed both for native and JC platforms)
 2. Platform and Application of different nature, hence (almost) empty intersection (eg software layer on top of IC)
 3. Compliance to PP required (if PP is platform-agnostic)
- Application on top of certified (U)SIM or JC platform
 - Does not fall into categories 1 or 2
 - Dedicated Composite-ST approach
 - Category 3 is not a fatality
 - Composite-PP approach for platform-aware PP

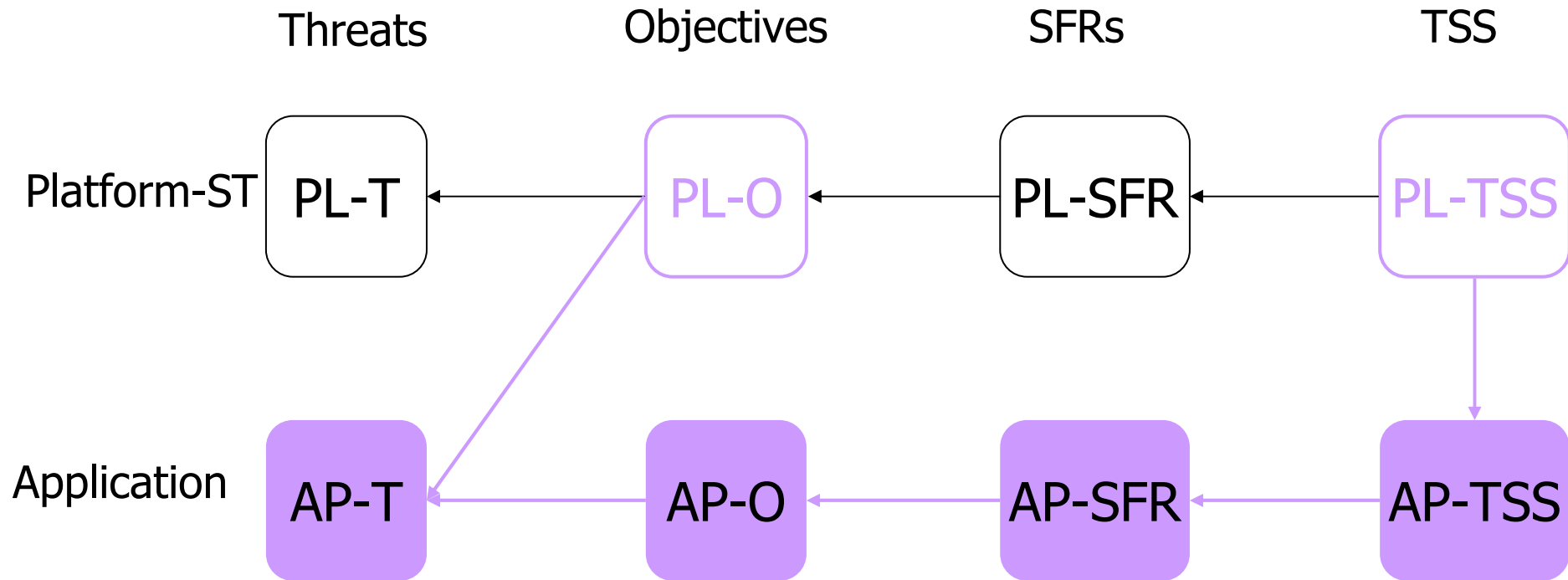


ASE_COMP: dedicated approach (1)

- Composite-ST complementary to Platform-ST
- TSFI derived from the Composite-ST required for evaluation
- Statement of compatibility by construction (split in rationales)
- Why:
 - Operational guidelines for Applications Providers
 - Simplify the definition of the actual evaluation scope
- How:
 - Define application-specific elements only (threats, objectives, SFRs)
 - Use platform elements to fulfill coverage rationales



ASE_COMP: dedicated approach (2)



AP-* Fully defined in Composite-ST

PL-* Referenced in Composite-ST

PL-* Outside Composite-ST



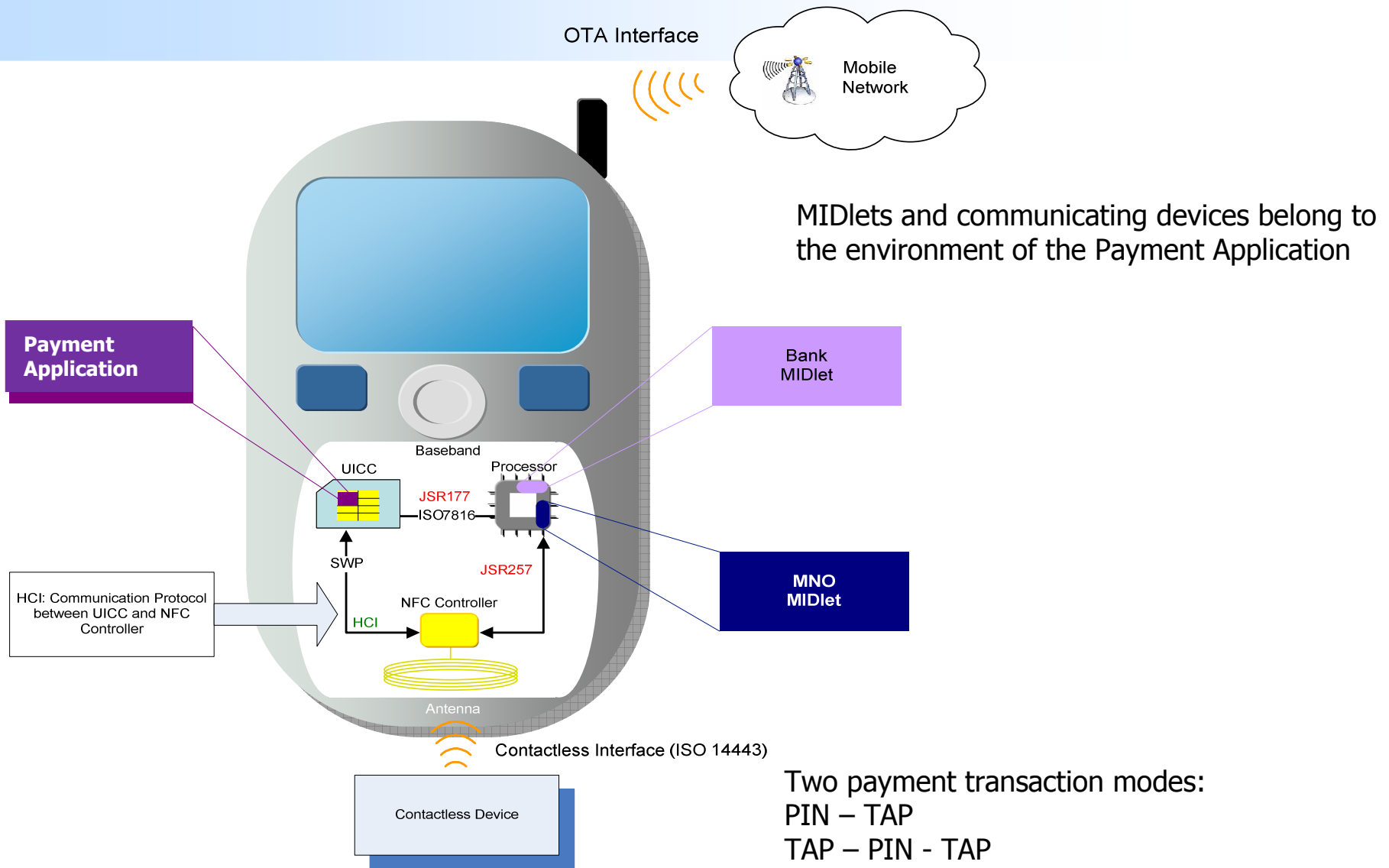
Generic security target for « Payez Mobile » Contactless Payment Application Package



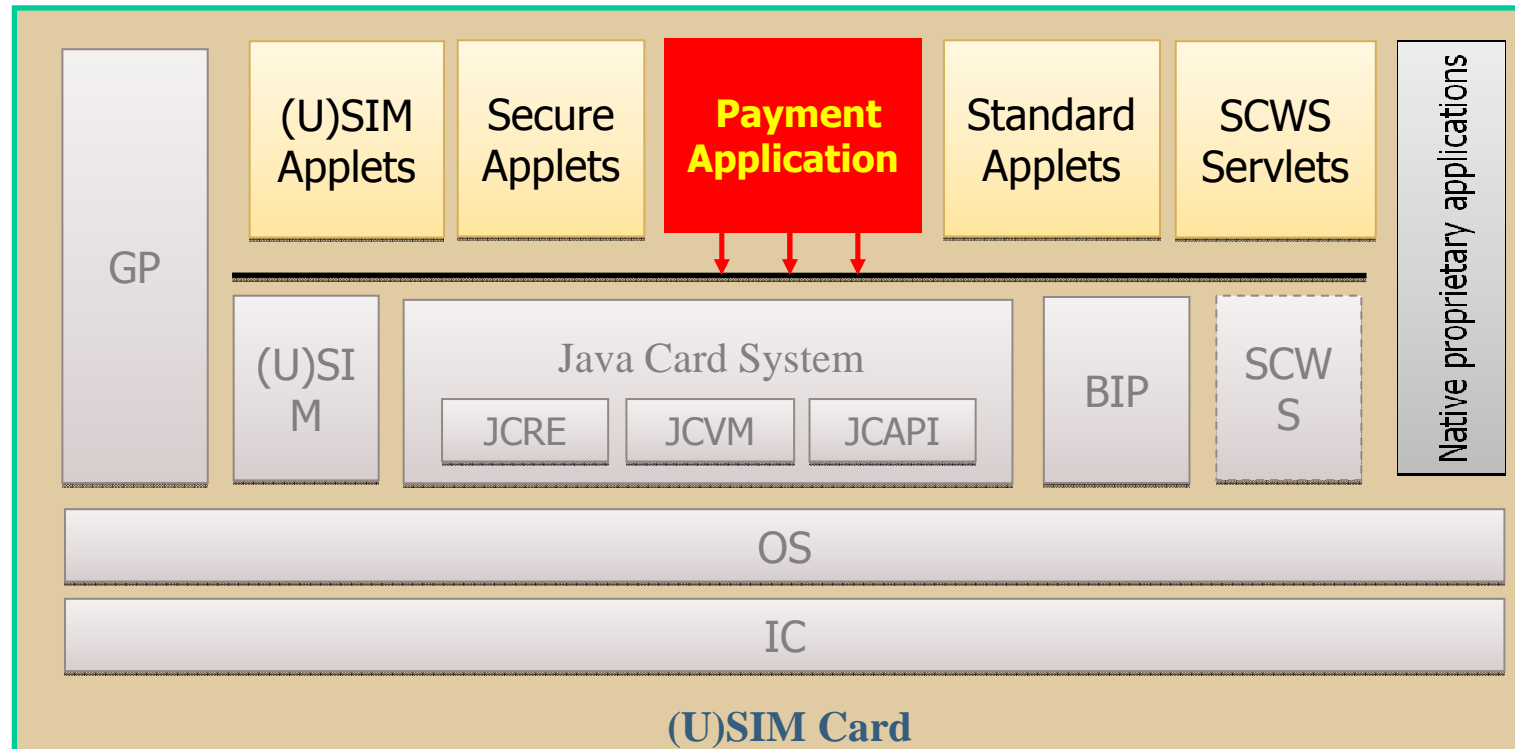
- Association Européenne Payez Mobile (AEPM) initiative
 - BNP Paribas, Crédit Agricole, Groupe Caisse d'Épargne, Groupe Banque Populaire, Groupe Crédit Mutuel-CIC, La Banque Postale, Société Générale, Bouygues Telecom, Orange and SFR
- Mobile proximity payment solution
 - Payment function located on the (U)SIM of a NFC mobile handset,
 - Compliant with payment scheme specifications:
 - MasterCard PayPass specifications (MCHIP/MagStripe), or
 - Visa specifications (qVSDC/MSD), or
 - Local scheme specifications
- Generic ST
 - Much like a protection profile
 - Internal version released July 17th 2009



Mobile proximity payment solution



The Payment Application in the (U)SIM

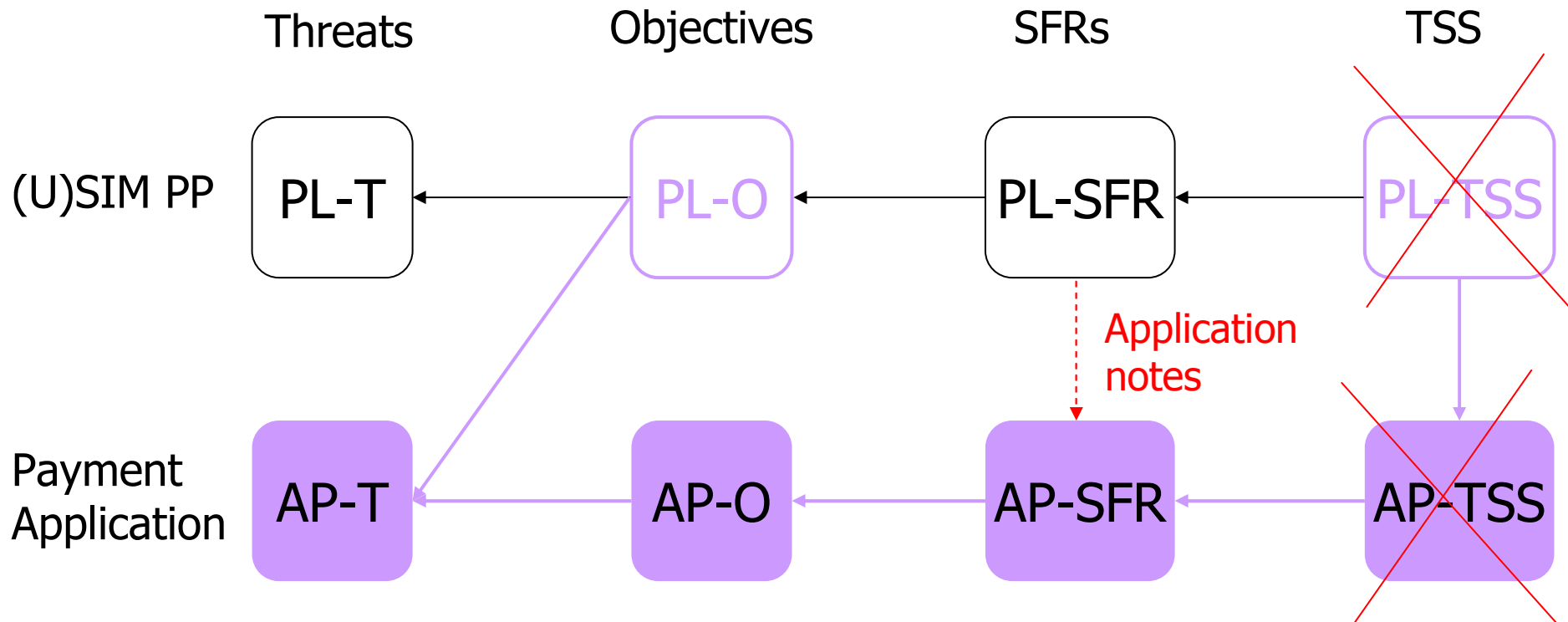


- Certified (U)SIM Java Card platform conformant to [PP-USIM]
- The generic ST addresses the Payment Application "Payez Mobile"
- Payment Application loaded/installed/personalised pre- or post-issuance



Generic ST for Payment Application

Adaptation of the ST approach



Outcomes



- Composite evaluation facilitators
 - Guidelines for Composite-ST (ASE_COMP) specific to application evaluation
 - Definition of the notion of Composite-PP (APE_COMP)
 - (U)SIM PP and Generic ST for « Payez Mobile »

- The next challenge on security interoperability:
 - « Reuse » of application's certificate across different platforms
 - Main idea: enforce adherence to PPs

