

## The GP Composition Model Maximizing the Efficiency of Security Certifications

11th ICCC

Antalya, 21-23 September 2010

Authors: Mestiri S. **Oberthur Technologies**; Chetali B. **Gemalto**; Loiseaux C. **Trusted Lab**;  
Picard P. **Orange**; Haselsteiner E. **NXP**; Gawlas F. **G&D**; Huque T. **ST**; Nahari, H. **Paypal**

- Motivation
- Applications Deployment on UICC Platforms
- Why GlobalPlatform?
- Methodology
- Next Steps

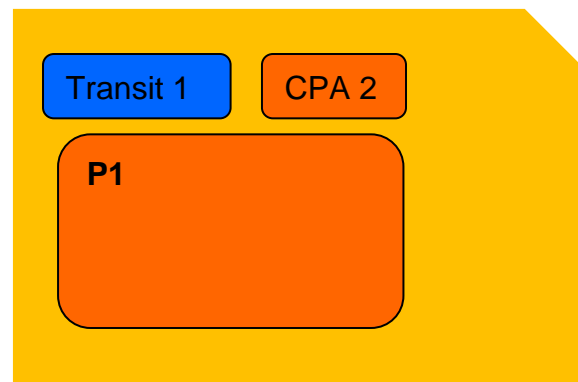
- Deployment of value added services requires security certification
  - Payment, Digital signature, Health Card, eID card, ..
- Current certification schemes are focused on **one** application or more (but from the same sector)
- Current certifications are incompatible with the business requirements of new uses cases (e.g. Mobile Banking) and not efficient when:
  - Card and application are not owned by the same actors
  - Deploying one certified application into various certified platforms

# Monolithic Certification Approach

GLOBALPLATFORM



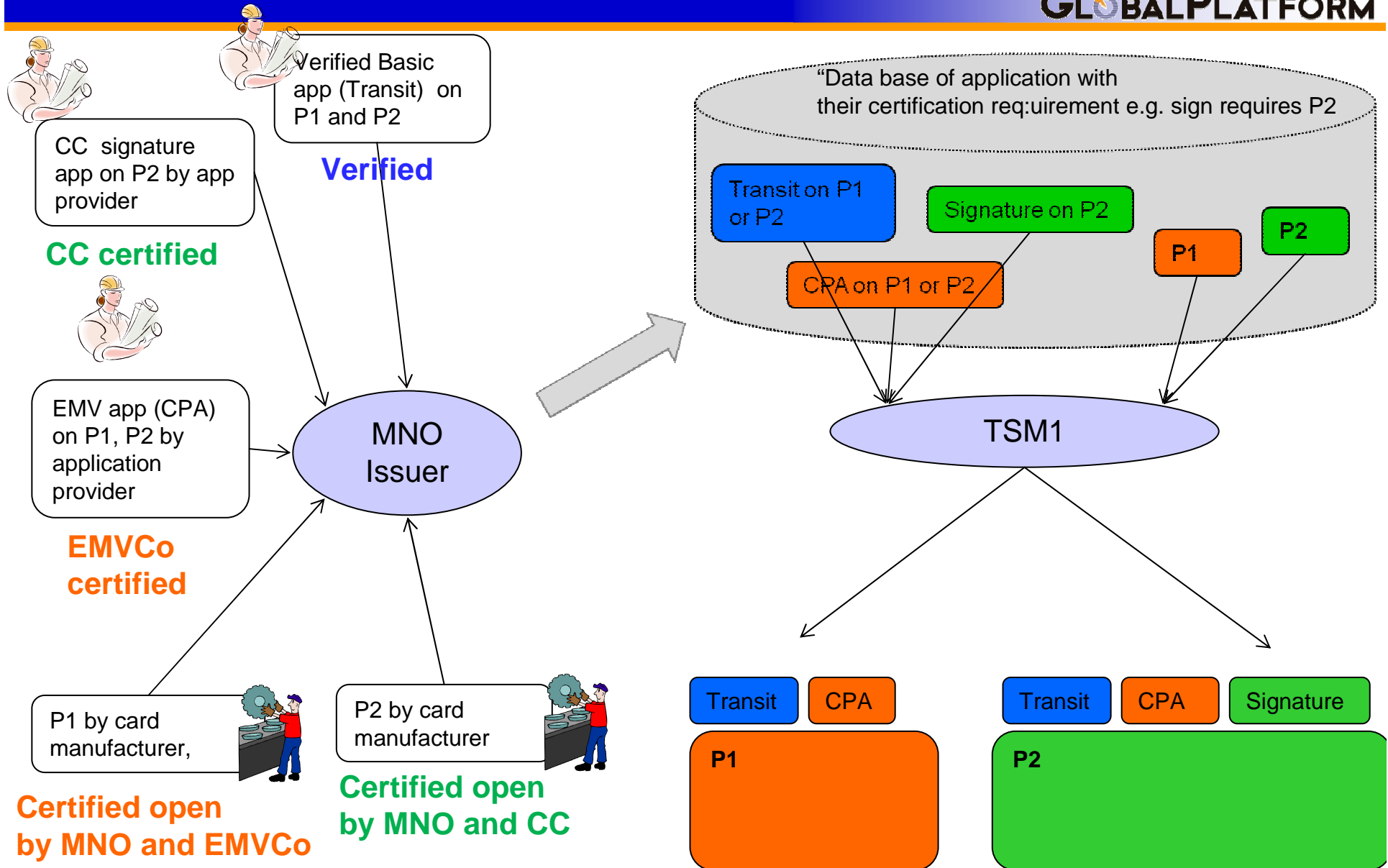
CC Certified by the card manufacturer on the requirement of the application issuer



EMVCo Certified by the card manufacturer for the banks

# Application Deployment in Mobile Market

GLOBALPLATFORM



- Maintaining the level of security of the products
- Avoid the creation of a new certification scheme
- Base the model on existing schemes (CC and EMVCo)
- Allow for multi actor ecosystem
- Allow for multi sector products
- Management of heterogeneous set of applications

# GP Security Working Group

GLOBALPLATFORM

- GlobalPlatform is a cross-industry organization regrouping the main actors of the UICC\* business model.
- The GP Security Working Group (GPSWG) is the interface between actors and facilitates the adoption of the composition model
  - Hardware Manufacturers
  - OS & Card Manufacturers
  - Labs
  - Applications providers
  - Mobile Network operators



GLOBALPLATFORM



**AFOM**  
ASSOCIATION FRANÇAISE  
DES OPÉRATEURS MOBILES



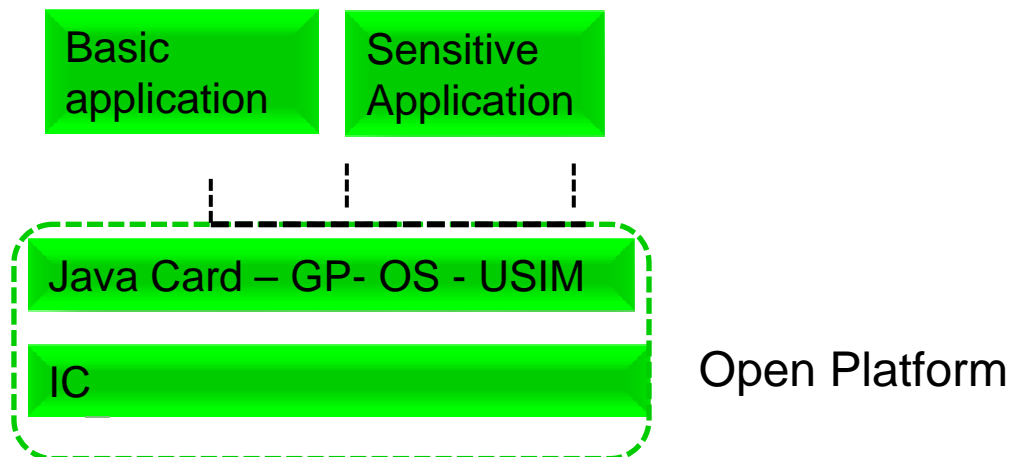
UICC : Universal integrated circuit card

# Identified Cases for GP composition

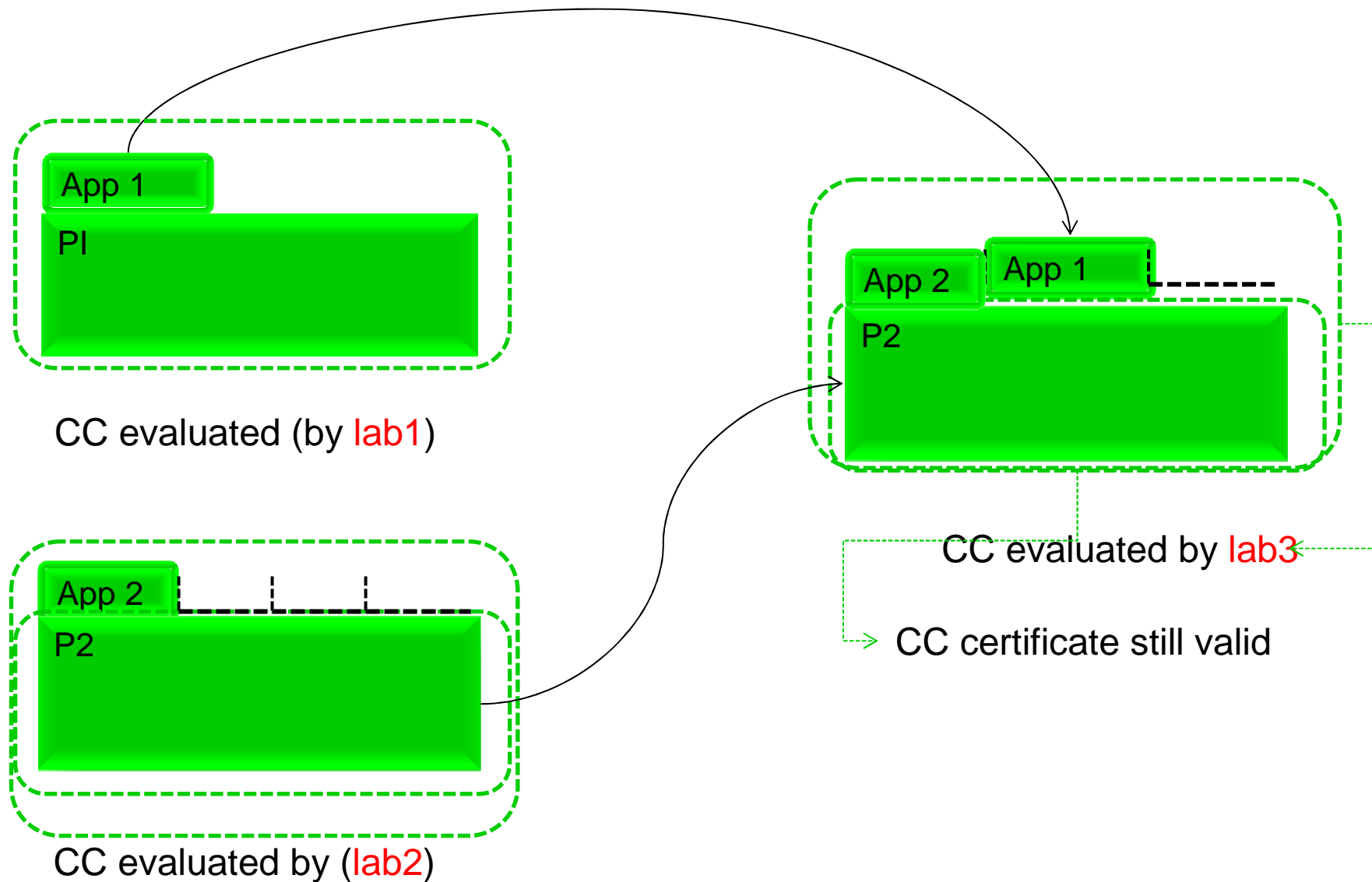
## Reuse of already certified components

- UICC platform (IC+OS+JC+GP + USIM)
- Sensitive Application : requiring certification
- Basic application: application with no certification requirement

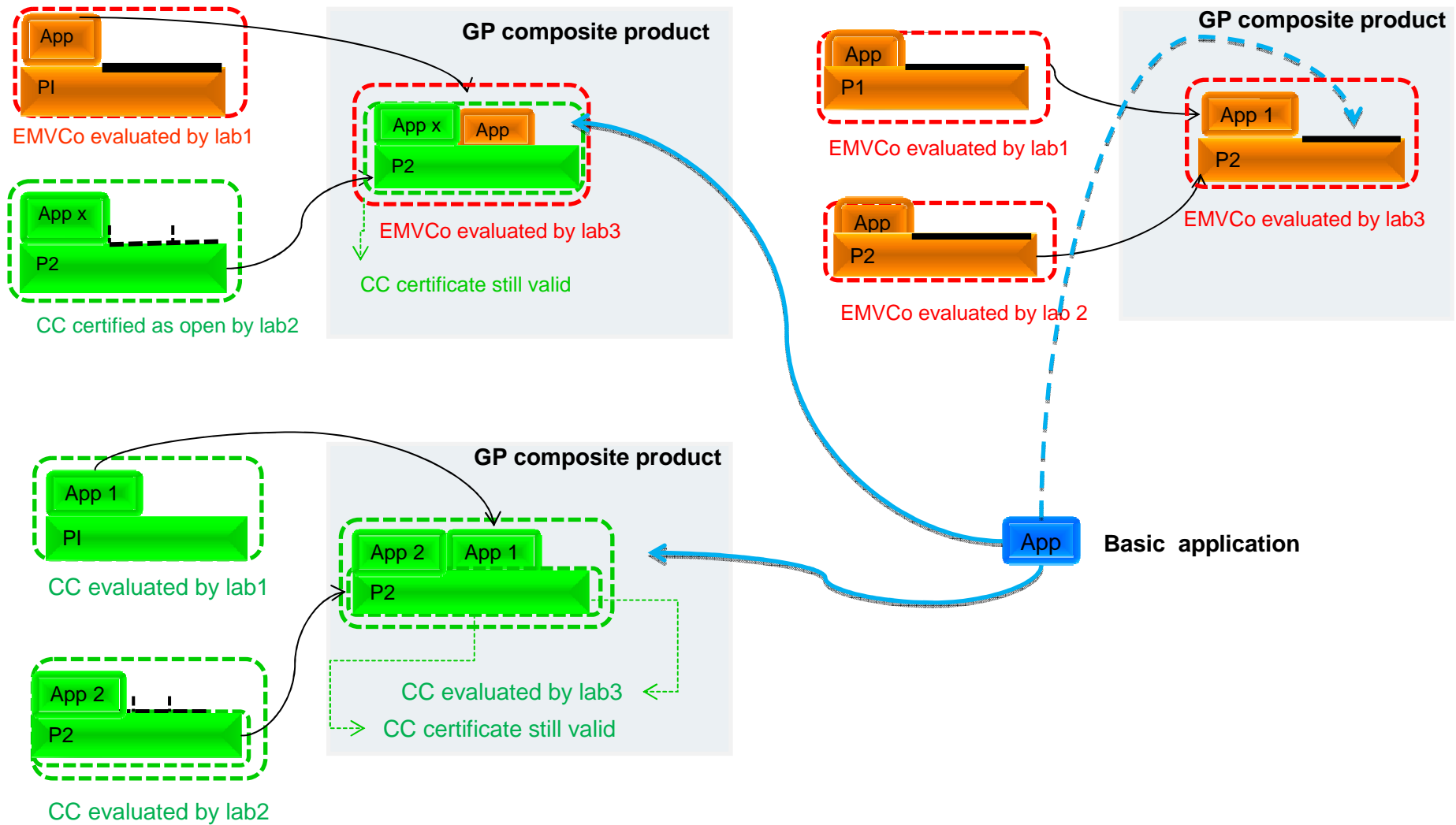
in the Common Criteria and the EMVCo schemes



# A CC certified GP composite product using CC open products



# More Complex Cases



- Application APP has been already certified on Platform P1
- Platform P2 has been certified as open (allow post issuance application download)
- Build a product [ APP + P2 ] and certify it by (GP) composition using previous certified building blocks
- Let Lab1, Lab2 and Lab\_Comp be the three evaluation labs involved
  1. List all the activities performed by Lab\_Comp
  2. Identify the required inputs for the task evaluation according to the CC
  3. Identify all available information from the previous evaluation
  4. Propose a reuse and provide the rational for this reuse

# List of activities for GP composition

	Activity to be performed by LAB_COMP	Required Input	Information of previous certifications (Reuse)	Rational for Reuse (reuse maximum)
ASE	Check security requirements for Composite Product	Security Target of App with references to P2	<p>P2 ST lite</p> <p>App on P1 ST Lite</p> <p>Certificate report of P2</p> <p>Certificate report of App on P1</p> <p>ASE work items performed for evaluation of App on P1.</p> <p>ASE work items performed for evaluation of P2.</p>	<p>App related work items for App on P2 can rely on the certificate (recognition of results of work items) of App on P1 without having access to App on P1 ASE ETR.</p> <p>P2 related work items for App on P2 rely on the certificate (recognition of results of work items) of P2 without having access to P2 ASE ETR.</p> <p>The CC composition related work items (ASE_COMP) have to be done. For example it must be checked that P2 fulfills the requirements of App (P2 fulfills the same requirements than P1).</p>
ADV	.....	.....	.....	.....
.....	.....	.....	.....	.....
AVA	Vulnerability analysis and penetration testing of Composite Product	<p>Samples</p> <p>Security architecture of the Composite Product</p>	<p>P2 ETR for Composition</p> <p>App ETR for Composition</p> <p><b>Note:</b> this Application ETR for Composition is a “new” CC document</p>	<p>P2 ETR for Composition and App ETR for Composition have to be used as input for the penetration testing.</p> <p>It is assumed that besides these documents, <b>the intellectual property</b> of penetration testing is too sensitive to be shared.</p> <p>The penetration testing plan shall be derived from the work done by the <b>JHAS group</b>.</p>

# Maximizing Reuse

- List the Assumptions on the platforms
  - Functional and security compatible
    - e.g Java Card protection profile,
    - e.g. State of the art reference for the attack potential
- Identify the roles involved: different labs and different CBs involved
- At the level of CC work items
  - Has the work item been performed already?
  - Does it need to be redone?
  - Try to find as many work items as possible which can be « done » by simply referring to previous certification

# Next Steps

- GP SWG provided a skeleton that must be challenged with
- ISCI
  - Formalize the content of the exchanges
  - Propose extension of exchange if any
  - Update of the Composite JIL document to integrate applications
- JHAS: definition of test robustness for open platform including application isolation
- Public version 1.0

Questions ?