Updating supporting documents for composite product evaluation

for CC V3

7th ICCC Lanzarote – 19-21 September 2006

ISCI-WG1

speaker: Françoise Forge

Presentation overview

- ISCI a Eurosmart Initiative
- ICSI contribution to CC V3
- Composite product evaluation
  - History
  - Why composite product evaluation is beyond ACO
  - Composite evaluation steps
  - Composite evaluation document overview
  - ETR for composite product (ETR_COMP)
- Conclusion

ISCI a Eurosmart initiative

- Created to continue e-Europe Trail Blazer 3 work on smart card evaluation
- Provide supporting documents to guide smart cards evaluation
- Improve methodology of smart card CC evaluations
- Involve all actors of the evaluation process,
- linked to JIL through Evaluation Authorities
- Two working groups
  - WG1 for methodology
  - WG2 for technical issues

ISCI-WG1 contributors

- Eurosmart members, laboratories, Evaluation Authorities
- Smart card manufacturers (hardware and software)
  - Gemalto, G&D, OCS, ATMEL, Infineon, Philips, Renesas, STMicroelectronics, Trusted Labs, Aspects
- Smart Cards issuers :Banking cards and e-Purse
  - Cartes Bancaires, BMS
- Evaluation laboratories
  - CEA-Leti, Serma, T-System
- Evaluation authorities
  - BSI, CCN, DCSSI, TNO

ISCI Contribution to CC V3

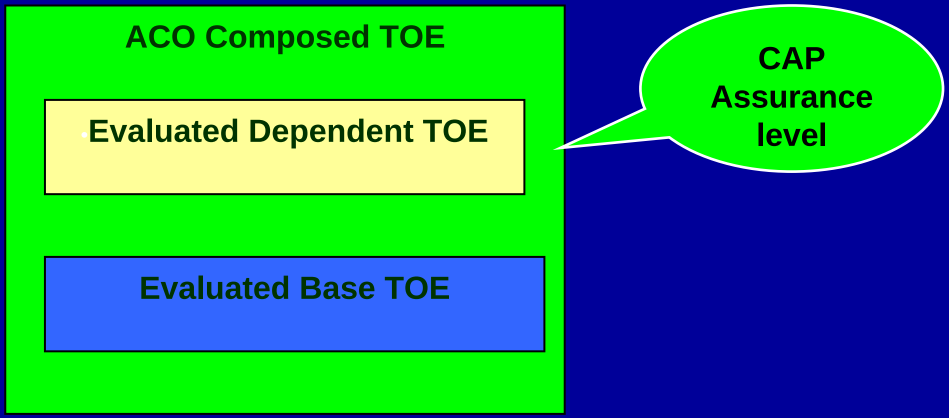
- Achievements
  - Support CC Site security evaluation process (WG1)
  - Commenting the CC V3.0 drafts with the ‘Smart Cards eye’ (WG1)
  - Updating the Attack quotation Table for Smart Cards (WG2)
  - Updating the Attack methods catalogue for Smart Cards (WG2)
- Current work plan
  - Updating of Smart Cards supporting documents
    - Composite Product evaluation
    - Guidance for Smart Card Evaluation
  - Continue to support Smart Card industry with methodology, tools with aim to reduce evaluation time and cost

Composite product evaluation: history

- Methodology was needed for smart card evaluations
  - Smart card composed of two parts from different manufacturers
  - An evaluated platform on which a software is embedded or loaded
  - The smart card is the final product on which security is challenged
- JIL supporting documents were issued
  - Produced by e-Europe Smart Cards TB3 group
  - Gathering all smart Card actors (industries, services, evaluators, CBs)
  - ETR-lite for composition : Version 1.1 July 2002,
  - ETR-lite for composition: Annex A Composite smartcard evaluation : Recommended best practice : version 1.2 March 2002
- Most smart cards evaluated with this methodology
  - First composite evaluation in 2002 (Ottawa 3rd ICCC May 2002)
  - Updated for CC V3 and improved methods after 4 years of experience

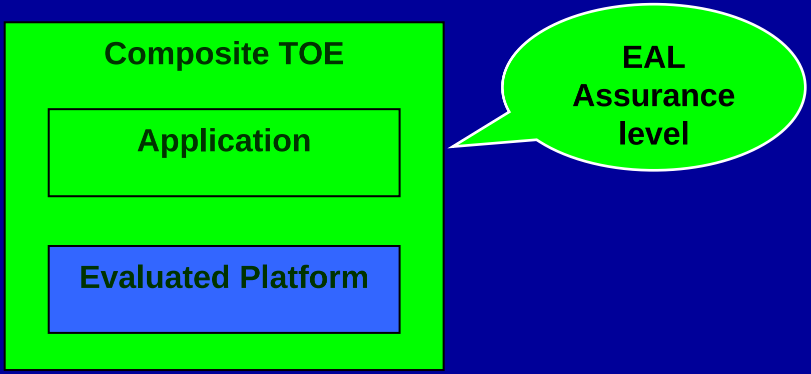
Composite product evaluation: beyond ACO (1)

- CC V3.1 introduces Class ACO: Composition
  - Addresses combination of 2 or more successfully evaluated TOEs
  - Reuses evaluation results
  - Concentrates on interfaces between TOEs
  - Defines Composed Assurance Packages (CAP) for the composed resulting TOE
  - Limited to Extended basic



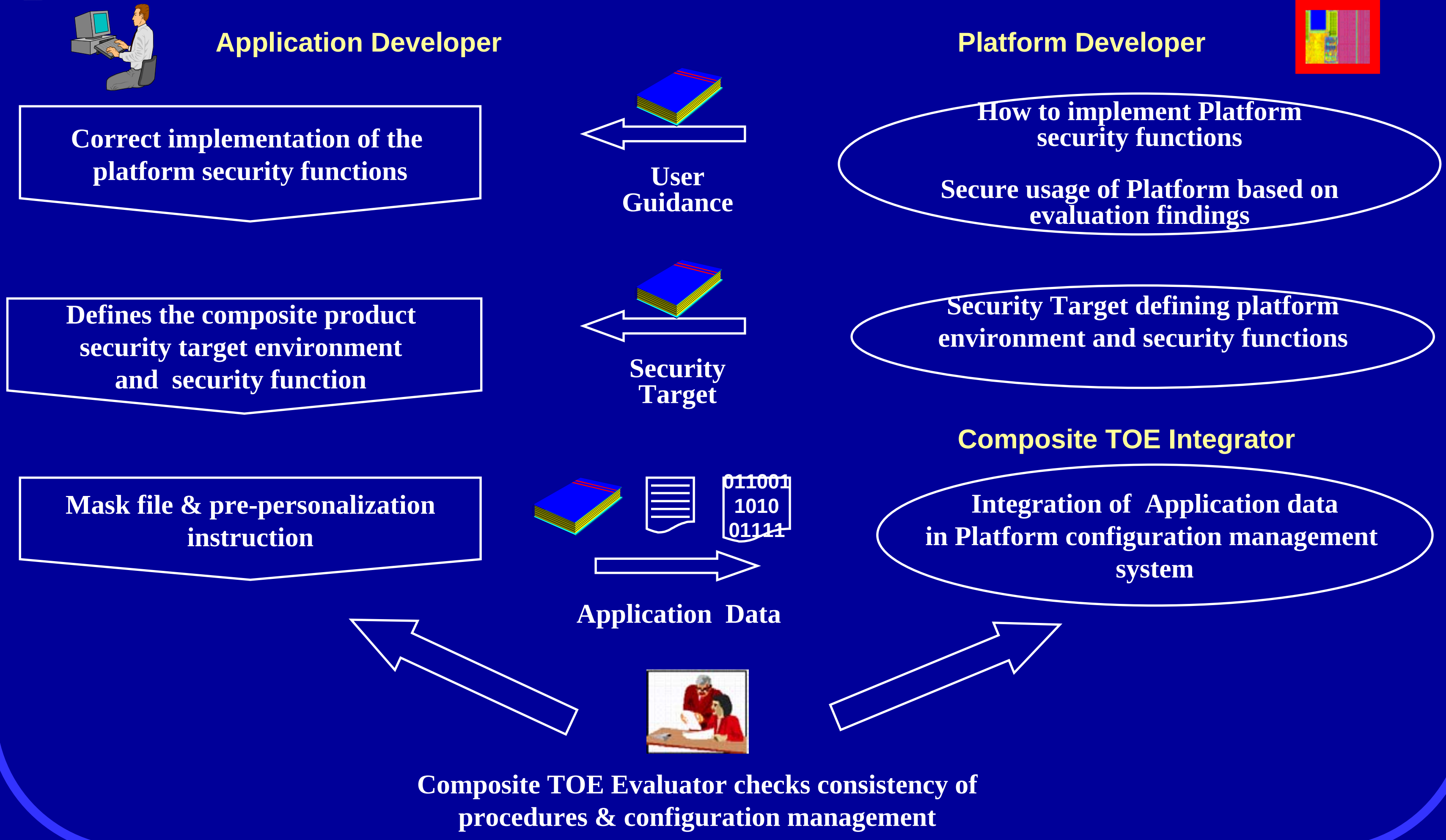
Composite product evaluation: beyond ACO (2)

- Smart cards composite product evaluation
  - Evaluation of a new TOE built with an application and an ‘underlying’ evaluated platform TOE
  - Application is not individually evaluated
  - Reuse platform evaluation results
  - Evaluation up to to EAL4+, with resistance to attackers possessing a high attack potential (VLA4/VAN5)
  - Platform provides security mechanisms for the application (ASE, AGD, AVA)
  - Composite TOE integration (mask/loading) implies information exchange management (ALC_CMS, ALC_DEL)



ISCI - International Security Certification Initiative

Composite evaluation steps(1)



Application Developer

Platform Developer

Correct implementation of the platform security functions

User Guidance

How to implement Platform security functions

Secure usage of Platform based on evaluation findings

Defines the composite product security target environment and security function

Security Target

Security Target defining platform environment and security functions

Composite TOE Integrator

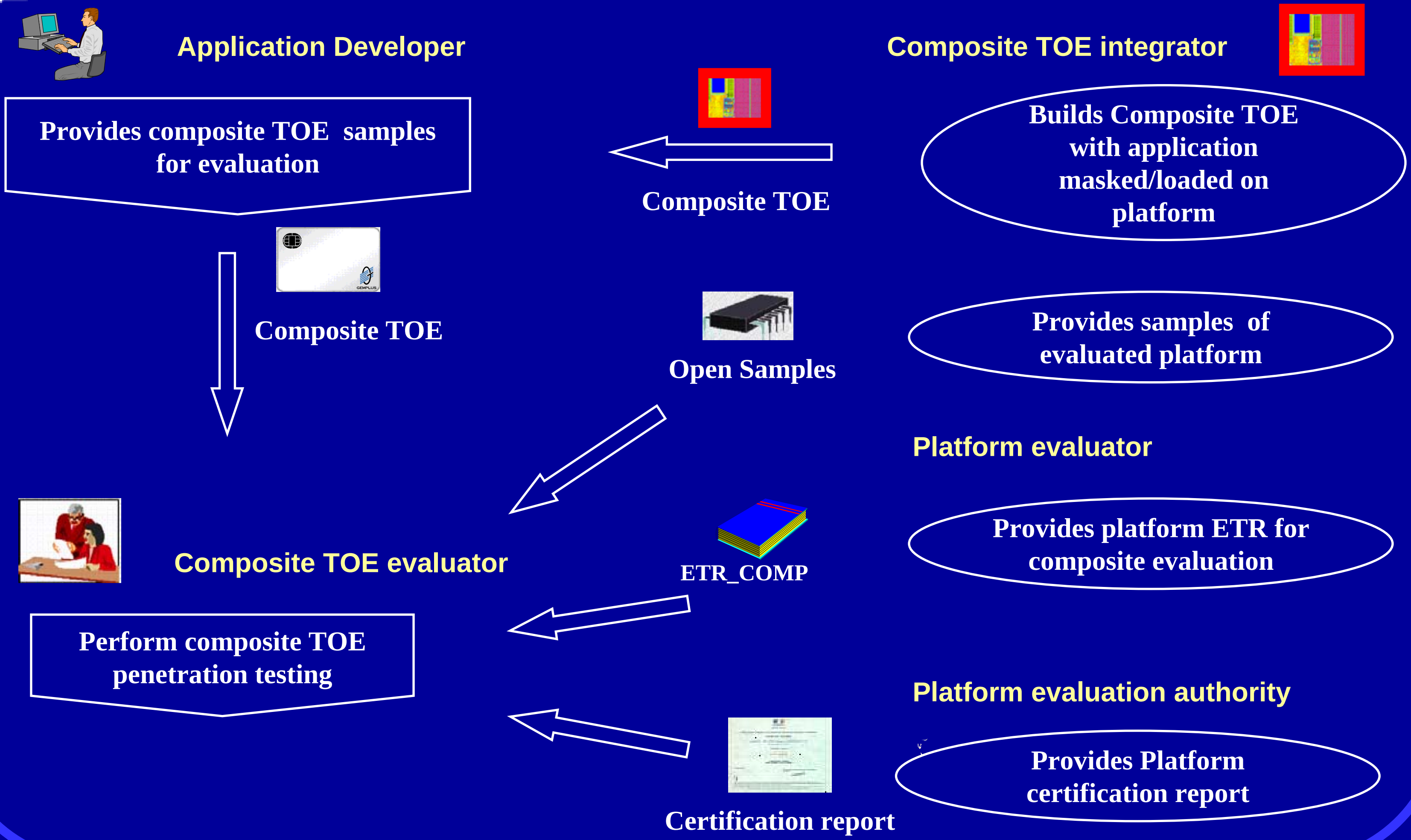
Mask file & pre-personalization instruction

Application Data

Integration of Application data in Platform configuration management system

Composite TOE Evaluator checks consistency of procedures & configuration management

Composite evaluation steps(2)



Application Developer

Provides composite TOE samples for evaluation

Composite TOE

Composite TOE evaluator

Perform composite TOE penetration testing

Composite TOE integrator

Builds Composite TOE with application masked/loaded on platform

Composite TOE

Open Samples

Provides samples of evaluated platform

Platform evaluator

ETR_COMP

Provides platform ETR for composite evaluation

Platform evaluation authority

Certification report

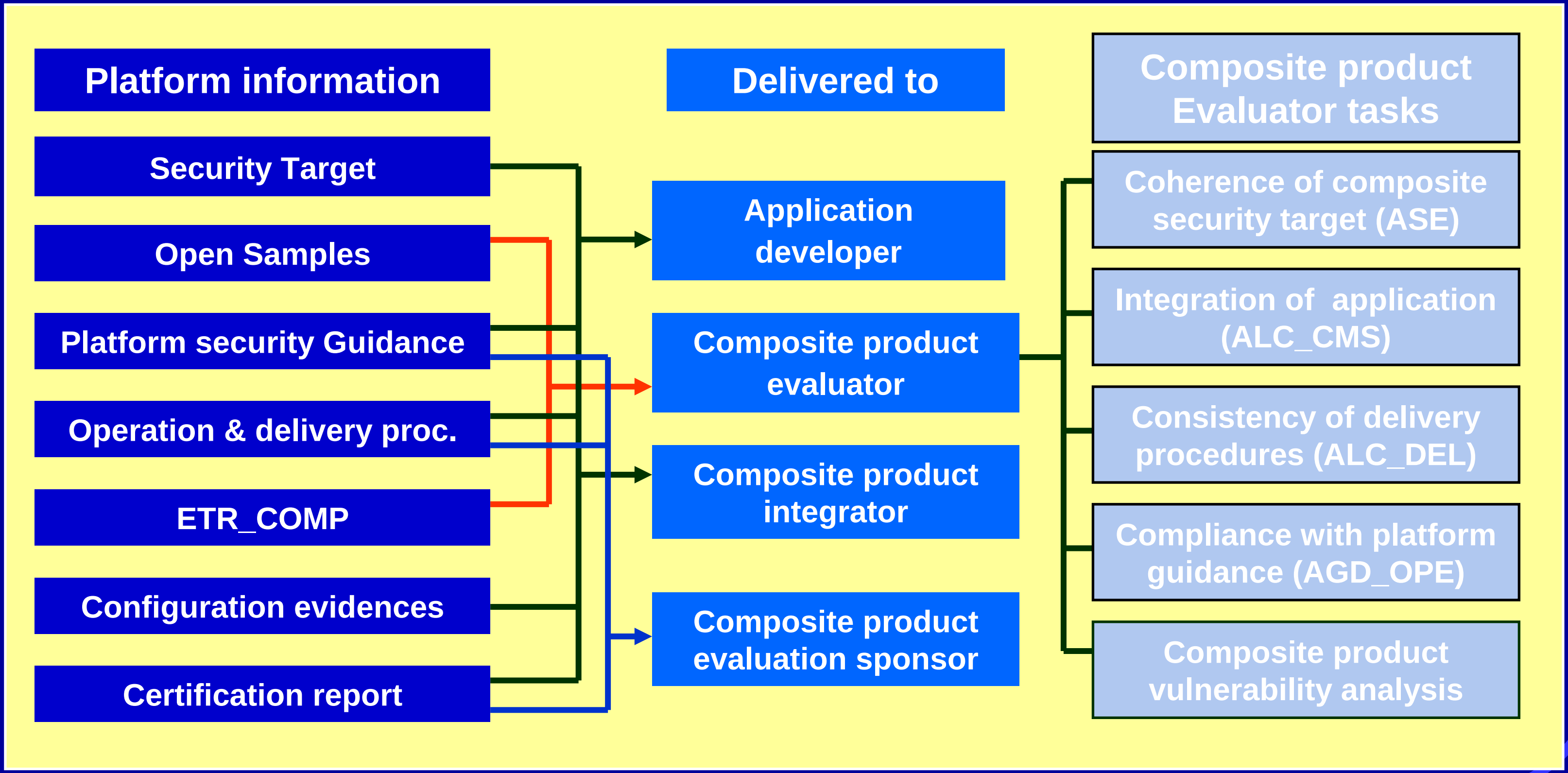
Provides Platform certification report

Composite product evaluation documents (1)

- Document objectives
  - Provide well defined methodology for smart card and similar products
  - Define precisely actors, roles and tasks for the different parties involved in the composite product evaluation
  - No definition of additional CC assurance class, but additional evaluation work units.
  - Address ‘smart cards and similar devices’ as other security IC technologies where an independently evaluated product is part of a final composite product to be evaluated.
- Document structure
  - Guidance defining the composite evaluation concept
  - Work units definition in CC Evaluation methodology language
  - Template of ETR for composite evaluation (ETR_COMP)

Composite product evaluation documents (2)

- Guidance defines actors and roles, information exchange, evaluators tasks



Platform information

- Security Target
- Open Samples
- Platform security Guidance
- Operation & delivery proc.
- ETR_COMP
- Configuration evidences
- Certification report

Delivered to

- Application developer
- Composite product evaluator
- Composite product integrator
- Composite product evaluation sponsor

Composite product Evaluator tasks

- Coherence of composite security target (ASE)
- Integration of application (ALC_CMS)
- Consistency of delivery procedures (ALC_DEL)
- Compliance with platform guidance (AGD_OPE)
- Composite product vulnerability analysis

Composite product evaluation document (4)

- Work units define precisely task of composite product developers and evaluators
  - ASE_COMP.1: Coherence of security target
    - Developer action elements
      - ASE_COMP.1.1D ;ASE_COMP.1.1.C
    - Evaluator action elements:
      - ASE_COMP.1.1E ;ASE_COMP.1.2.E :
  - ALC_COMP.1: Integration of application software into the Platform CM
  - DEL_COMP.1: Consistency check of delivery procedures
  - ADV_COMP.1: Composite design compliance (user guidance, recommendations)
  - AVA_COMP.1: Composite product vulnerability assessment

Composite product evaluation: ETR_COMP

- Defined template to ensure that same type of information is available from one evaluation to another
- Contains the necessary information from the Platform evaluation for composite evaluation work units
  - Platform certification summary
  - Design general information
  - Evaluated configurations (evaluation limits, configuration, installation..)
  - Delivery procedures and data exchange
  - Vulnerability assessment and penetration testing
    - list of attack path, description, rating of the attack, result
  - Observations and recommendation to users.

Conclusion

- Composite evaluation document improved
- Compatible to CC V2.3 and CC V3.1
- Includes composite Evaluation Technical Report template
- Mandatory for all smart cards and similar products
- Well defined work units based on 10 years of experience and shared best practice between schemes
- Ready to perform composite evaluation for Smart cards consistent with CC V3
- Need stable CC version !