Porting ST and PP to CC 3.0: problems and some answers

Axel Boness
Axel.Boness@cea.fr
CESTI LETI

Context

- CESTI-LETI is an ITSEF of French Certification Scheme

- Main field of expertise of CESTI-LETI is
  - IC and IC + ES evaluation
  - against high attack potential

- Theorytical study of porting to 3.0
  - Neither PP nor ST were written or evaluated yet against CC3

- Here, we are dealing with CC 3.0 revision 2, july 05

Plan

- Assess rewriting is mandatory
- Identify known problems for CC 2.2
  - Usability of PP
  - Easiness of reuse
- Identify new tools in CC 3.0
  - ACO class
  - Conformity claims
- Propose some hints
  - Divide et Imperia

Is rewriting really mandatory ?

- It's a technical question

- About SFR
  - There is not a direct one to one transformation for the SFR of CC2.i to CC3.0
  - SFR were moved, or deleted, …

- About SAR
  - Commonly used via a package (EAL)
  - Stated explicitly as augmentation in PP or ST
  - SAR & EAL are roughly consistent from v2 to v3

Is rewriting really mandatory ? (continued)

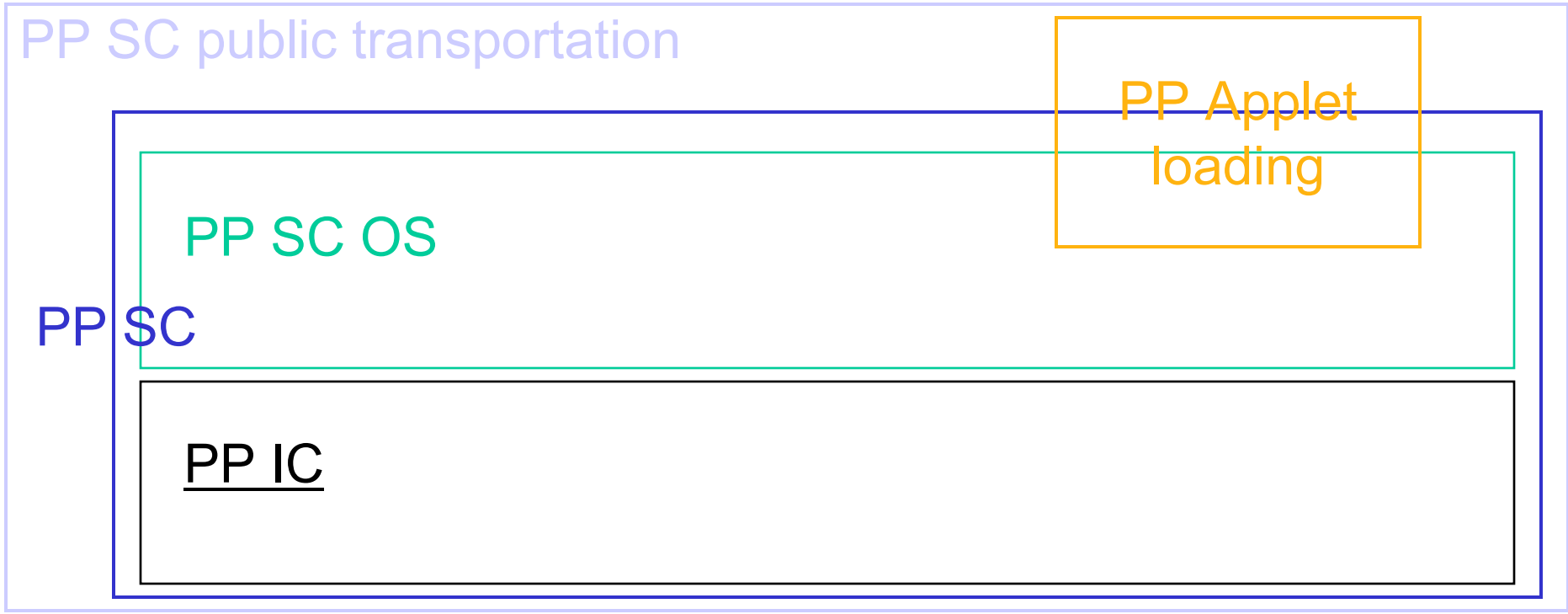
- The conformance claim
  - v2 PP can be considered as calling for demonstrable conformance

- It's unlikely that a v3 ST or PP can be conformant to a v2 PP (or a consequent rationale is provided)

- As a consequence :
  - Rewriting (or designing) new PP is mandatory
  - Therefore ST rewrite is also mandatory

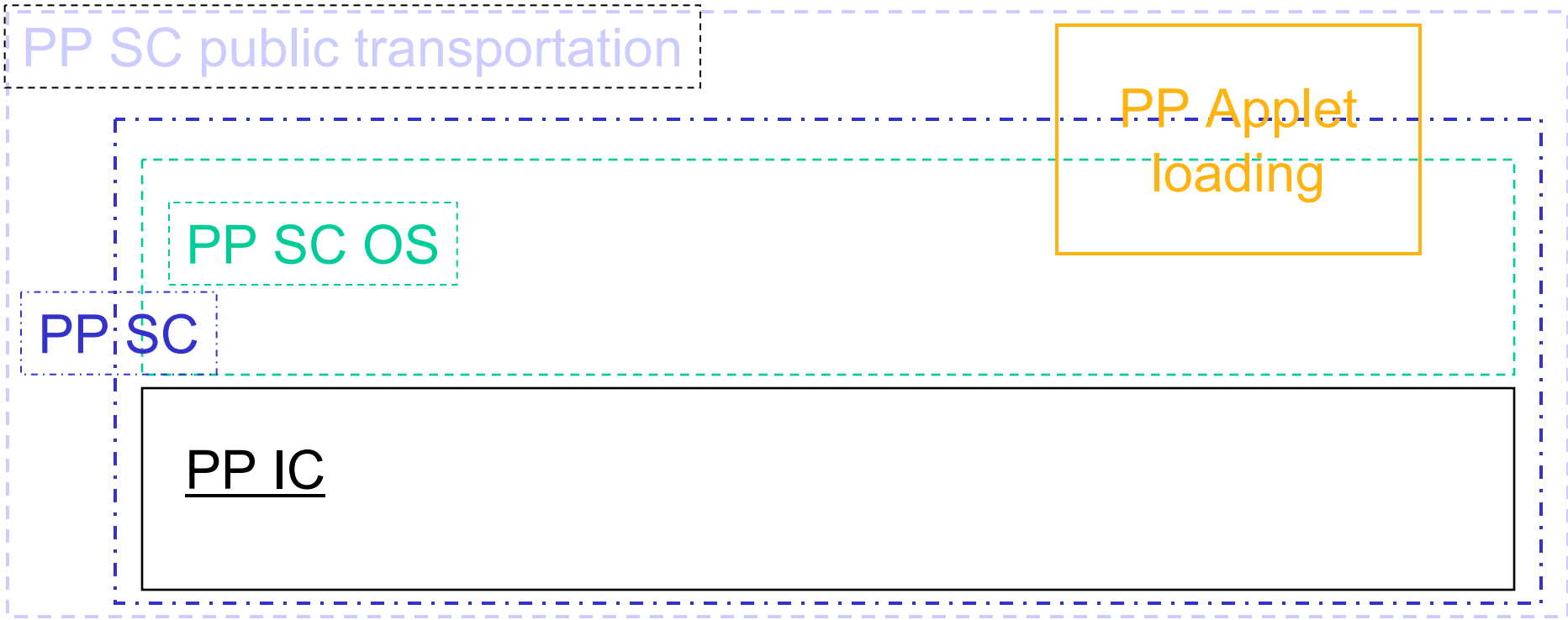
Example from CC part 1 § 8.4

For instance, one could take a PP for an Integrated Circuit and a PP for a Smart Card OS, and use these to construct a Smart Card PP (IC and OS). One could then combine this with a PP on Applet Loading and use this to write a PP on Smart Cards for Public Transport.



Consequences

If PP SC OS becomes obsolete, at least 2 other PPs become obsolete



Inter-PP claims

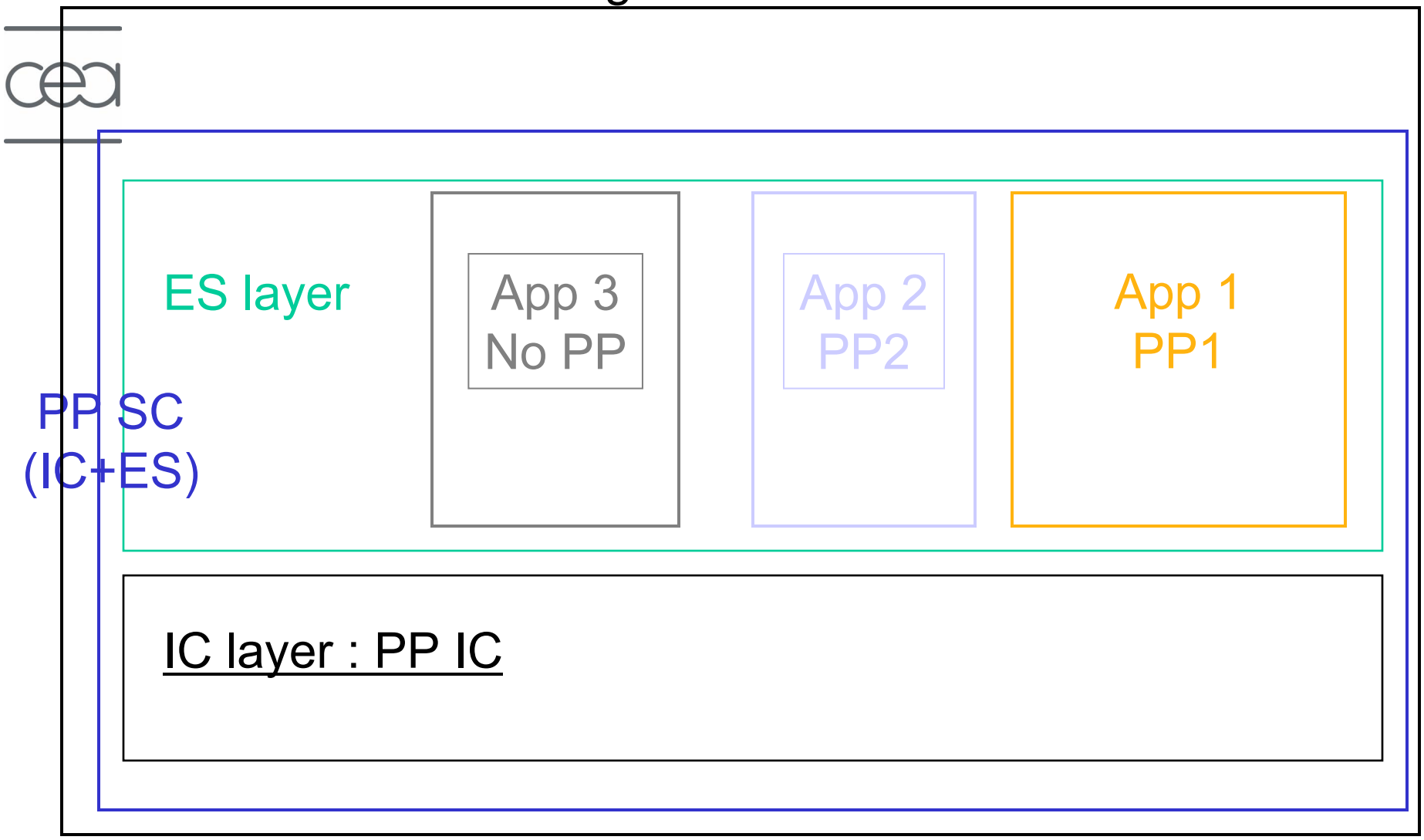
- Creates inter-dependency relationships
- Implies : SFR of ST = O(Σ(SFR of each PP))
- The french PP0101 indirectly asks for a conformity to PP9809 which was later superseded by PP9911
- PP9911 is tied to PP9806, some would like to use instead of it BSI-PP-0002 (SSVG PP). How ?
- What if a base PP becomes unusable because of a radical change in the underlying technology ?
- Conclusion: avoid inter-PP relationships

Other facts

- Using huge ST for huge projects is hazardous:
  - Assets are multiple and not always shared among the whole product
  - TSFI becomes very hard to define
  - Is security problem consistently described ?
  - At some point security and functionnality become intermixed and the « problem » becomes messy
  - ST are unreadable but for the writer and the evaluator

- Conclusion: avoid large ST whenever possible

Multi-application smarcard



Divide et Imperia = DaC

- Conformances
  - The SC has to be conformant to PP SC
  - APP1 to PP1
  - APP2 to PP2
  - APP3 to the ST

- Writing only one ST would not be a good idea

- What is usually done:
  - 3 ST: 1 per application each conformant to PP SC !!!

- What could be done DaC (Divide and Conquer)
  - 4 ST:
    - 1 per application
    - 1 for the whole SC

More ST and PP : why ?

- To focus on specific problems at a specific level

- ie: Application problems are commonly a superset of the ES problems
  - Confidentiality of stored data is already assessed at the PP IC+ES level

- To « factorise » problems :
  - Global assets should be studied once

Distinguish composition and composition

- ICCC BERLIN 2004

« Suggestion for a Framework for Composite Evaluations »
Helmut Kurth & Paul A. Karger

- Defines several types of composition:
  - Layering composition (HW / SW)
  - Network composition (connected TOEs)
  - Component composition (TOE reused in larger system)

Distinguish specialisation and composition

- Composition:
  - using multiple independently evaluated TOE composed together to obtain a bigger TOE

- Specialisation:
  - specialising requirements or adding requirements to a predefined set
    - Defining assets for an ES in an application
    - Giving specific values for SFR

ACO: composition class

- ACO_COR
  - Demonstration of appropriateness of base TOE for composition
- ACO_DEV
  - Information on base TOE
- ACO_REL
  - Description of expectations of dependent TOE
- ACO_TBT
  - Testing of base TOE in the composition context

ACO and IC+ES

- ACO is not defined for classical IC+ES evaluation levels
  - AVA_VAN.5 (AVA_VLA.4), it stops at extended basic

- ACO seems suited for cooperative TOEs rather than for « hosted » TOEs

- IC + ES is a symbiotic environnement
  - IC demands support from ES (only ES knows when security is needed)
  - ES uses IC mainly to protect it from physical attacks

- ES is not evaluated alone (IC+ES=SC)
  - It's done in the IC context
  - Same ES on different IC implies specific work

Nowadays DaC

- In the SC world for multi-application in closed systems
  - 1 evaluation of several TOEs at a time
  - Usually one ST per application

- Different from ACO composition

- Proposition:
  - Add an SC specific ST
  - 1 more ST that will lighten applications ST

Tomorow's DaC

- Multiply independent ST by writing independent PP

- Benefits:
  - Simple PPs and simple STs
  - Independency implying versatility
  - Readibility
  - Easiness of design

- Problem:
  - Everybody
    - Believe security is complexity
  - Therefore this approach might be too simple
    - We are the ennemy

DaC, ACO and porting to 3.0

- Avoid combining PP :
  - Use DaC when possible
  - When there is specialisation or partition
- SC PP deal with phase 1 to 7:
  - Why not specifying security behaviour by phases ?!
  - IE application data/ specific assets in phase 4 or 5 doesn't exist as such but the ST commonly identifies it's handling…
- ACO and smartcards :
  - IC+ES composition : seem left to the national schemes (at least in France)

Conclusion

- ACO gives a 3.0 formalisation of the composition paradigm nevertheless specific problems (smartcards) are not yet dealt with

- ACO and DaC are to be studied against non-SC composition

- Multiple ST on a product is not an issue, it's often a solution. Light ST are reusable !

- DaC is not a 3.0 necessity, but 3.0 implies rewriting
  - so why not DaCing to enhance maintenability and simplify each solved problem

References

- ICCC 2004 in Berlin proposed several presentations on the theme of composition:
  - « Composite Evaluation: Necessary as never before »
    Dr. Igor Furgel & Volker Schenk
    also using « Divide & Impera » from a methodology point of view
  - « Suggestion for a Framework for Composite Evaluations »
    Helmut Kurth & Paul A. Karger
    for the taxonomy of composition
- Also see « Summary of Changes »
Informal document on CC V3.0 update

Any questions

Axel Boness
Axel.Boness@cea.fr