



ISCI

International Security Certification Initiative

Stepping into CC v3.1 – Supporting efficiently the ADV_ARC in the Smart Card industry

10th ICCC

Tromsø, 22–24 September 2009

ISCI-WG1

speaker :

22 September 2009

10th ICCC Tromsø

Feedback on the ARC template

Contents

- ISCI-WG1 approach and vision about ADV_ARC
- Security Architecture Requirements (ADV_ARC) for Smart Cards and similar devices
 - Interpretation guideline
 - Template (HW & SW)
- Feedback from Smart Card industry various experiences
 - HW & SW developer (and related evaluation & certification bodies)
- Conclusion

ISCI WG1 – Approach & Vision (1/2)

- Migrating from CC v2.3 to CC 3.1
- Many points were unclear with the new ADV_ARC class family:
 - Importance of such deliverable for the security assessment
 - Integration in the set of ADV and links with ASE, ATE
 - Evaluation & Certification expectations
- Other concerns from developers:
 - Efficiency to perform this task
 - Reduce as much as possible the evaluation and certification time process
 - Anticipate blocking point due to CC interpretations



ISCI WG1 – Approach & Vision (2/2)

- Taking experience from all stakeholders gathered in this working group:
 - Analysis of the ARC requirements
 - Preliminary agreement on ARC expectations between all evaluation stakeholders (HW developers, SW developers, evaluators & certifications bodies, final customers)
 - Decision to formalize this interpretation in a guideline documentation
 - Decision to support the completion of the ARC activity with guidance in two parts for smartcards developers:
 - One for HW developers
 - One for SW developers


Interpretation Guideline

- Based on CC requirements, the guideline refines the expected answer (“the essence of Security Architecture”):
 - TSF “always invoked” – Non bypassability
 - Definition of TSFI, Port, TOE physical boundaries
 - Protection of the TSF– Secure Initialization and self protection
 - Security domain (focusing on what is not described in ADV)
 - Example with Java Cards and applet execution on well defined resources
 - Level of description in ADV_ARC
 - Shall be the level used for the description of SFR_Enforcing in ADV_TDS: subsystems or modules

Template

- For better efficiency in application all contributors have enhanced the interpretation guidelines with a template for smartcard developers
- Specificity:
 - mapping the self-protection and non-bypassability analysis to the list of attacks defined in “Application of attack potential to smart cards”
 - Referring to Eurosmart PP/0035
- Ensuring consistency with ASE, ADV_FSP, ADV_TDS and ATE documentation
- Point whenever possible or applicable to other ADV documentation to avoid description redundancy
- Keep self-sufficiency of ARC documentation

Developer experience

- Pilot certifications in September 2008 (HW chips) and July 2009 (SW products) under French scheme and different labs
 - Until then, several other products have succeeded in CC v3.1 evaluations:
 - HW Chips, EAL5+
 - ePassport, EAL4+
 - Banking card, EAL4+
 - Javacard platforms, EAL5+
- } ISCI Experience 
- References
 - Common Criteria v3.1
 - “Application of Attack Potential to Smart Cards”, version 2.5 (april ‘08) and 2.7 (march ‘09)
 - ADV_ARC Security Architecture Description ISCI WG#1, version 2.0, January ‘08

General feedback on ARC writing and evaluation

- The ARC analysis is useful even outside the CC context
 - Welcomed by all developer teams
 - Allow to improve global security view
- The template re-used from ISCI WG#1 allows to limit the internal workload for the ARC writing
- Cost and time reduced compared with VLA
- Existence of template saved up time for the document validation by evaluation & certification bodies
- CB & labs found ISCI approach and ARC documentation consistent with CC

Remark:

Template targets smartcard EALs 4+/5+ (with AVA_VAN.5)
Different templates could be developed for lower or higher lever

Template structure & main paradigm

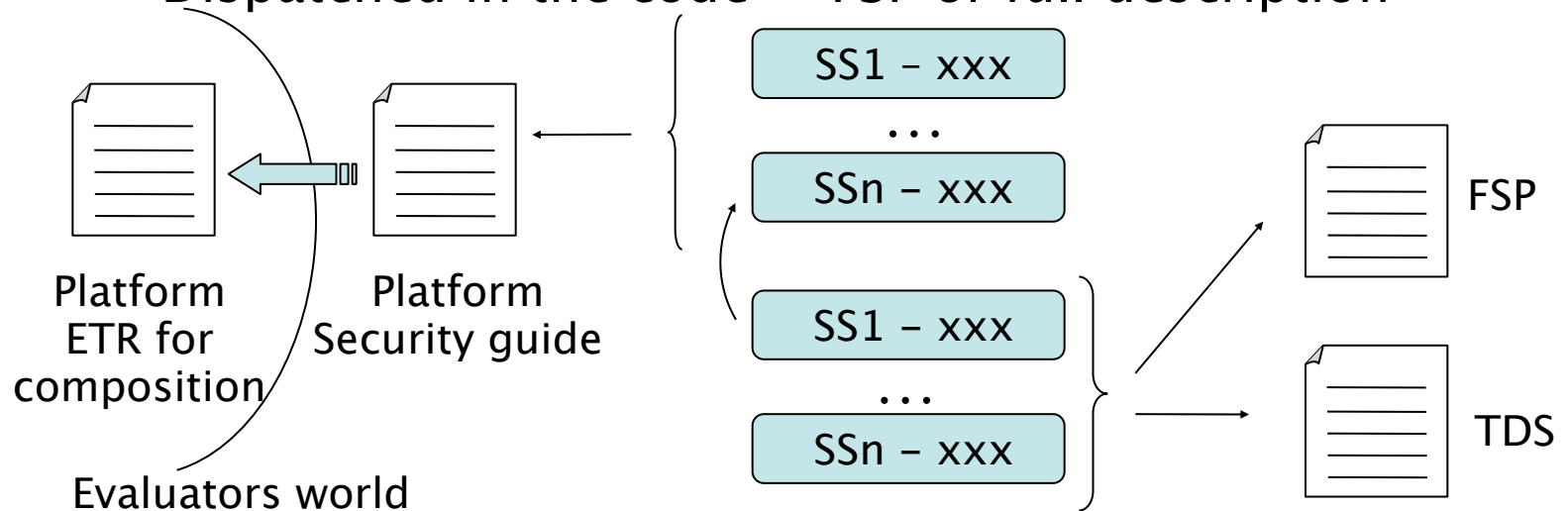
- – Global security architecture ↔ ADV_ARC.1.1
- Initialisation/Start-up ↔ ADV_ARC.1.3
- Cooperation of security mechanisms ↔ ADV_ARC.
- Security domain separation ↔ 1.4/5
- ↔ ADV_ARC.1.2

The ISCI ARC template:

- Relies on FSP & TDS description but self-sufficient
 - avoid documentation redundancy
 - take advantage of our FSP/TDS description
- Highlights on global security especially cooperation
 - focus on added-value of ARC documentation
 - Provide a structured approach

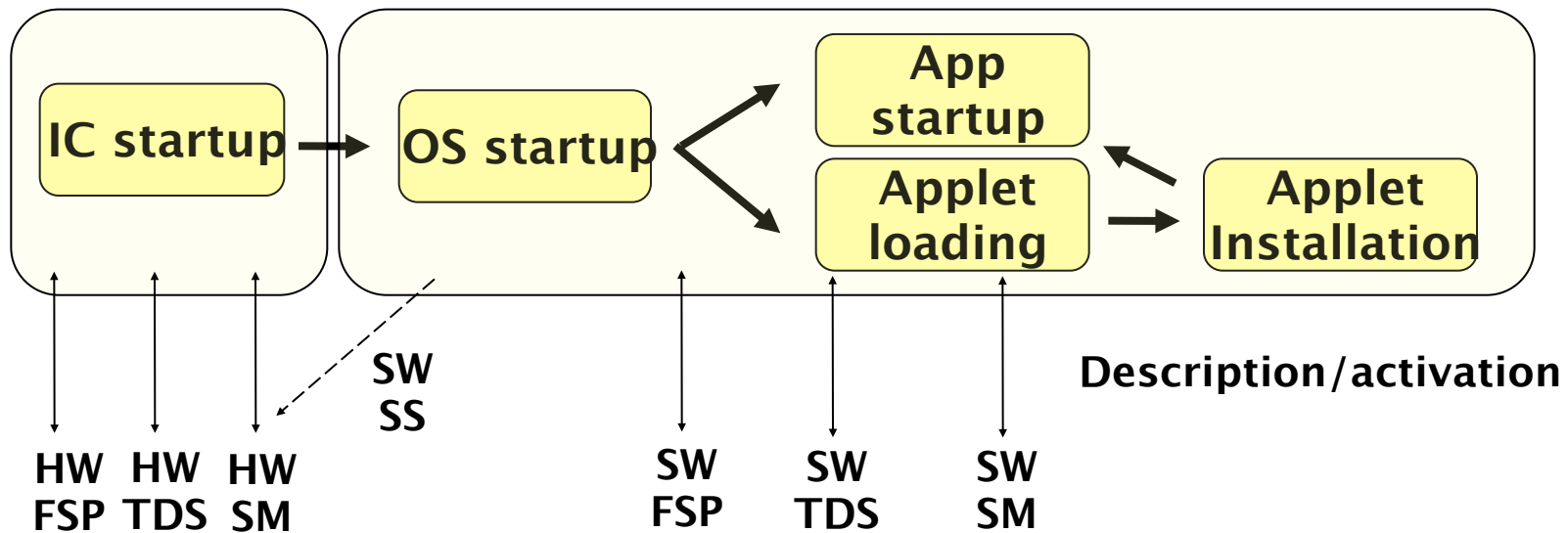
Global security architecture

- Security services (SS), support TOE security
 - secure block provided by underlying platform (HW crypto...)
- Security mechanisms (SM), enforce TOE security
 - Defined block (or function) – TDS reuse
 - Dispatched in the code – FSP or full description



Secure initialisation/start-up

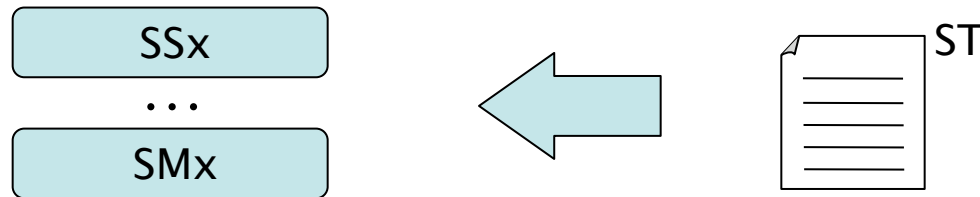
- For the whole initialisation IC+OS+Application (select, installation...)



justification of architecture choices with the appropriate security substantiations

Cooperation of security mechanisms

- Mapping SM/TSS highlights how security features are enforced



Self protection and non-bypassing

- Analysis of each attack (see [CCDB-2009-03-001])
- Attack path description when relevant
- Rationale and list of which SM/SF contribute to enforce self-protection or non-bypassability for each specified attack
 - Nota: Re-use of AVA_VLA work for these sections was very poor

Conclusion

- Building ARC templates and shared interpretation
 - Saved time for writers and certification phase
 - Detailed template, may add work for some developers and should be simplified
 - Early discovery of potential vulnerabilities
 - Avoid misinterpretation between developers, evaluators and certification authorities
- Following feedback from field guidance usage
 - The ISCI WG#1 will go on the fine-tuning of this template
 - The template will be proposed to CCDB as CC supporting document