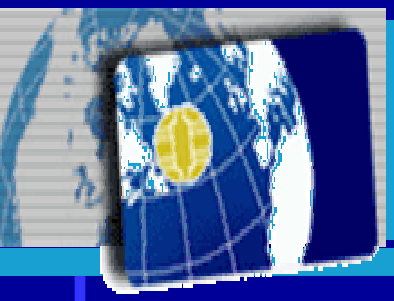
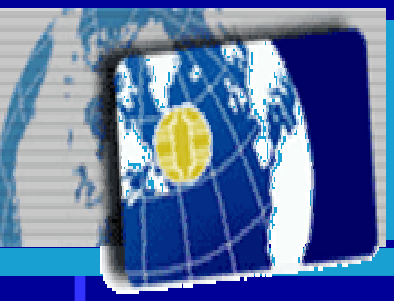


CC V3.0

How it affects Smart Card evaluation

6th ICCC TOKYO – 28-29 September 2005

Hans-Gerd Albertsen/ Philips Semiconductors
Françoise Forge/ Gemplus
Catherine Gibert/ ST Microelectronics
Tyrone Stodart/ Renesas

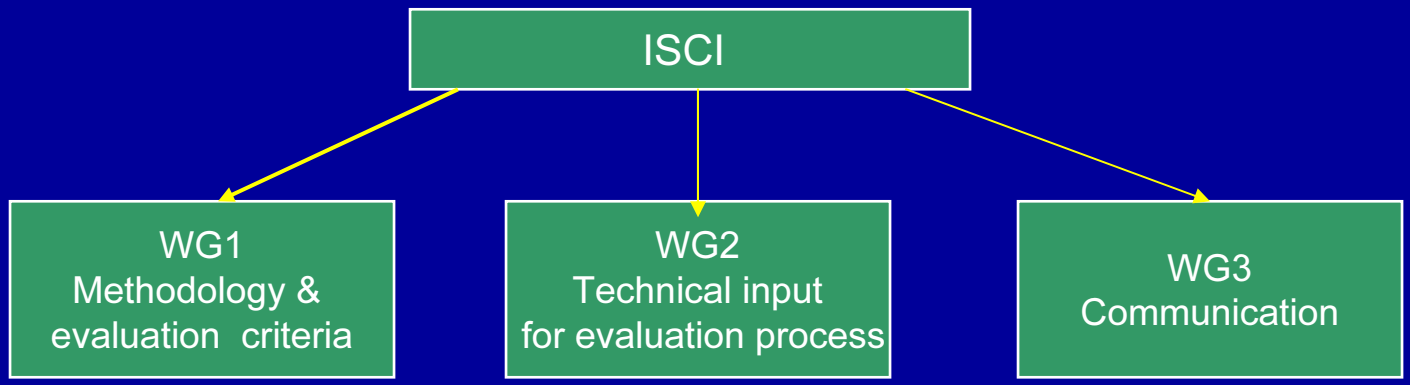


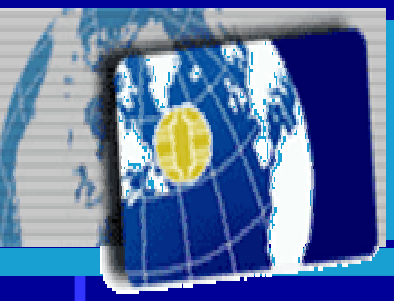
Presentation overview

- Who is ISCI?
- Smart Card evaluation overview
- How CC 3.0 will affect Smart Card evaluation
- Conclusion

Who is ISCI?

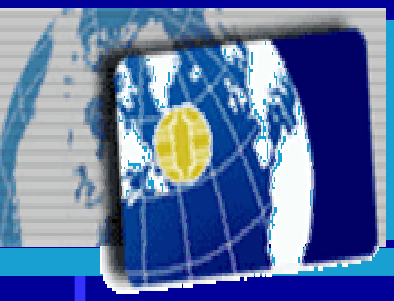
- International organization supported by Eurosmart
- Major participation from the Smart Card industry
  - Aspects, Axalto, Cartes Bancaires, Gemplus, G&D, Infineon, Master Card, NTT Data, OCS, Orga, Philips, Renesas, SFPMEI, STM,
  - CEA/ Leti, Serma, SiVenture, SRC, Thales, TNO, T-System, TÜViT
  - BSI, CCN/CNI, CESG, DCSSI





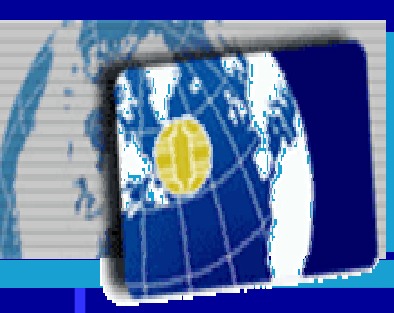
ISCI Working Group 1 activities

- ISCI-WG1 Objectives
  - Promote CC evaluation for Smart Card
  - Provide supporting documents to guide Smart Card evaluation tasks
- Activities
  - Supporting French banking to establish the Vulnerability Analysis Grid (ETR-for-Issuer)
  - Commenting and monitoring the CC V3.0 drafts from the Smart Card point of view
- Next tasks
  - Provide Smart Card industry Comment on public CC 3.0
  - Provide examples for Smart Card to complete Part 3 and CEM
  - Support JIL in the updating of Smart Card supporting documents



Smart Card evaluation overview (1)

- Smart Card industry strongly committed to CC
  - CC evaluation used since 1999
  - Smart Card and IC represents 30% of all common criteria evaluation (source CC Portal July 2005)
  - Application of CC evaluation to commercial products
  - Effort to reuse evaluation results to optimize cost & duration
- Some Smart Card Protection profiles issued
  - Hardware IC (PP9806, BSI-PP-0002)
  - Smart Card product (PP9911, PP9810, PP0010, SCSUG, JCSPPc)



Smart Card evaluation overview (2)

- Supporting documents issued by the JIL
  - Application of Attack Potential to Smart Card
  - Application of CC to Integrated Circuit
  - Guidance for Smart Card Evaluation
  - ETR-Lite for composition + annex A , ST-Lite
    - not dedicated to Smart Card but widely used for Smart Card composite evaluations

How CC 3.0 will affect Smart Card evaluation

- ISCI-WG1 : review and monitoring of CC V3.0
  - Part 2 : completely rewritten
  - Part 3 :
    - ASE & APE : conformance, package claim
    - ADV : new or reviewed families ; ARC & TDS,
    - ATE : aligned with new TDS ; no major changes
    - AGD: Operational & preparative used guidance
    - ALC : merge of ACM/ALC/ADO
    - AVA : Developer analysis removed & quotation changed

CC V3.0 Part 2

- Main changes
  - Completely rewritten!
  - Reduction to a minimum of classes : FDP, FIA, FCO, FAU, FPT, FMI
  - Classes merged or removed (in particular FCS Cryptography),
- Consequences
  - Rewrite Smart Card product Protection Profiles and other protection profiles used for smart Cards (Electronic signature, Electronic purse , banking applications …..)
    - First candidate for rewrite is the BSI-PP-0002 (Eurosmart)
  - Need to adapt to Smart Card security definition , may require additional components definition

CC V3.0 Part 3 : ASE & APE

- Main changes
  - Conformance to a PP: exact, strict, demonstrable
  - Package claim: defining set of reusable security requirements
  - Objectives for the TOE environment: clarification between development environment and operational environment
  - TOE summary specification : overview, no rational to SFRs
  - Defines low assurance PP/ST
- Consequences
  - Simplification and clarification of PP/ST structure
  - More flexibility in ST conformance claim
  - More flexibility and ease in ST building , using and combining multiple PP

CC V3.0 Part 3: Assurance classes & EAL

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	4
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

- Smart Card evaluation level with CC2.2 is EAL4 or EAL5 augmented

→ Analyze and interpret CC V3.0 changes to keep same level of assurance

CC V3.0 Part 3: ADV (1)

- 6 families defined
  - 4 families to demonstrate that security works as specified
    - ADV_FSP
    - ADV_TDS
    - ADV_IMP
    - ADV_SPM
  - 2 families to demonstrate that TOE cannot be used to corrupt its own security
    - ADV_ARC
    - ADV_INT

CC V3.0 Part 3: ADV (2)

- ADV_FSP: functional specification
  - FSP.4 requires explicitly precise description of TSFI
  - FSP.5 semi-formal , almost identical to CCV2.2 FSP.3
  - SFR coverage rational not required to developers, evaluators job
  - Consequence
    - None , as for Smart Card all parts are security enforcing or supporting

CC V3.0 Part 3: ADV (3)

- ADV_TDS : TOE design
  - Merge of HLD & LLD , corresponds to design reality
  - ADV_TDS.3 Basic Modular Design at EAL4,
    - Requires explicitly identification and description of interaction
    - Requires algorithmic description
  - ADV_TDS.4 semiformal modular design at EAL5
    - Allows identification of SFR-enforcing, SFR-supporting, SFR-non interfering to reduce amount of description,
    - No semiformal style description is provided
  - Consequence
    - Need to interpret and define with examples what is Data ,return values and ‘algorithmic description’ for Hardware IC part.

CC V3.0 Part 3: ADV (4)

- ADV_ IMP : implementation
  - ADV_IMP.1 identical to CC V2.2 ADV_IMP.2
  - More flexibility for mapping with TDS
  - Developer shall ‘make available’ the implementation representation of the entire TSF
  - Consequence
    - none
- SPM : Security policy model
  - One single component allowing formal and semi-formal model
  - Moved to EAL6 & EAL7
  - Consequence
    - less work for EAL4 & EAL5

CC V3.0 Part 3: ADV (5)

- ADV _ARC :Architectural design
  - Description & demonstration of TOE self protection, domain separation & non-bypassability of the TSP
  - Consequence
    - Need to define what represents ARC for Smart Card
- ADV_INT : TSF internal design
  - ADV_INT.1 partial modular design defined but not related to EAL can be used for critical security parts design
  - ADV_INT.2 full modular design starting EAL5
  - Consequence
    - Need to analyze how full modular design applies to Smart Cards

CC V3.0 Part 3: ATE - ACO

- ATE : Test
  - Realigned with FSP & TDS new definition ,
  - Consequence
    - no major changes
- ACO : composition
  - Addresses interconnection of different evaluated TOEs
  - Scope is different from Smart Card composite evaluation: integration of Software masked /loaded on hardware
  - Consequences
    - JIL document for Smart Card composite evaluation still relevant
    - Need to check what is required for a composition between a smart card and a terminal for example

CC V3.0 Part 3: AGD- ALC

- AGD guidance documents
  - AGD_OPErational & AGD_PREparation
  - Consider the 'User' with different roles
  - AVA_MSU moved to AGD_OPE & AGD_PRE
  - Reorganization of AGD_ADM & AGD_USR that fits real product life
- ALC Life Cycle support
  - Merge and reorganization of ALC/ACM/ADO
  - Remove redundancy both for developer description and evaluator task.
- Consequence
  - Makes compliance easier, although need to review internal document organization

CC V3.0 Part 3 : AVA (1)

- Main changes
  - Developer Vulnerability analysis no longer required
  - SOF removed
  - AVA_CCA now covered by AVA_VAN but not clearly defined
  - Developer provides only ‘suitable TOE’ for Evaluator penetration testing
  - Quotation of attack potential
    - Notion of IDENTIFICATION and EXPLOITATION removed
    - Do not match with the quotation established for smart cards (Attack Potential JIL document)

CC V3.0 Part 3 : AVA (2)

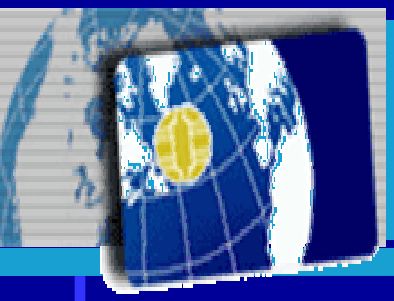
CC V2.2/JIL and VAN comparison

Attack example	JIL quotation for Smart Cards	CC 3.0 VAN quotation
Simple DPA	17= VLA.2 Low	8= Extended-Basic
DEMA	27 = VLA3 moderate	14 = moderate
DFA	15 = No rating	8 = Extended-Basic
Laser direct perturbation	24 = VLA3 low	10 = moderate
Laser direct perturbation Algo reduction	29 = VLA3 moderate	30 = Beyond high
CEM V3.0 example	16 = VLA.2 low	27 = Beyond high

➡ Need to keep Smart Card quotation table to ensure the current security level

Smart Card evaluation with CC V3.0

- Advantages of CC V3.0
  - Clarification of language and definition
  - Merge of HLD/LLD in TDS
  - SPM only needed for EAL6 & EAL7
  - AGD/ALC/ACM/ADO reorganized
  - Simplification of developers work : less documents, closer to real life
  - Simplification for evaluators : enforced level of knowledge of TOE details and more consistency in evaluation task
- Disadvantages of CC V3.0
  - Difficult to reuse CC V2.2 results also for composition
  - Difficult to compare VLA and VAN levels (does not fit to current practice)
  - Must rewrite Protection Profiles
  - Must review supporting documents
  - Additional documents are to be provided (ARC)
  - Existing documents need to be adapted (ADV; ALC, ACM, ADO, AGD, AVA)



Conclusion

- What we expected from CC V3.0 is time and cost saving for the same security assurance
- Current experience on CC V3.0 is insufficient to state whether this goal is attainable.
- ISCI-WG1 will provide comments and is looking forward to CC V3.1