



## Monitoring Common Criteria for Smart Cards and Similar Devices


11th ICCC

Antalya, 21-23 September 2010

ISCI-WG1

Speaker name : Alain Boudou

## History- ISCI is a Eurosmart initiative

- Eurosmart,
  - International non-profit association founded in 1995 in Brussels
  - 27 companies of the Smart Security industry (smart card manufacturers, semiconductors, terminals, issuers)
  - Promotion and standardization of smart secure devices and smart secure systems
  - Harmonization of security evaluation schemes
- ISCI created by Eurosmart
  - To define, support and promote a universal framework for security evaluation and certification methods, tools and procedures, based on internationally accepted standards.
    - Fair, high quality, comparable, standardised evaluations.
  - To involve all actors within the evaluation process, with the goal to improve smart card evaluation time & cost
  - To provide supporting documents to guide smart card evaluations
- Two working groups
  - WG1 for methodology  This presentation
  - WG2 for technical issues - known as JHAS

## History: WG1 Previous contribution to CC

- Monitoring CC V3
- Composite Product evaluation for smart cards and similar devices  
CCDB-2007-09-01 (Mandatory)
- ETR template for composition CCDB-2007-09-02 (Mandatory)
- Application of CC to IC CCDB-2009-03-002 3-0 (Mandatory)
- Supporting Site Certification process definition developed by BSI,  
reviewing and commenting final supporting document (CCDB-2007-  
11-001)
- Security Architecture (ADV\_ARC) –for smart cards and similar devices  
Released as JIL trial supporting document

# ISCI International Security Certification Initiative

## ISCI WG1 2010 Contributors

### IC manufacturers



### Smart card manufacturers and issuers

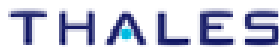


Giesecke & Devrient



Gouvernement des Comores - République "ICSI"

### Evaluation laboratories



### Certification Authorities



Bundesamt für  
Sicherheit in der  
Informationstechnik



Algemene Inlichtingen- en  
Veiligheidsdienst  
Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties

## ISCI WG1 Motivation

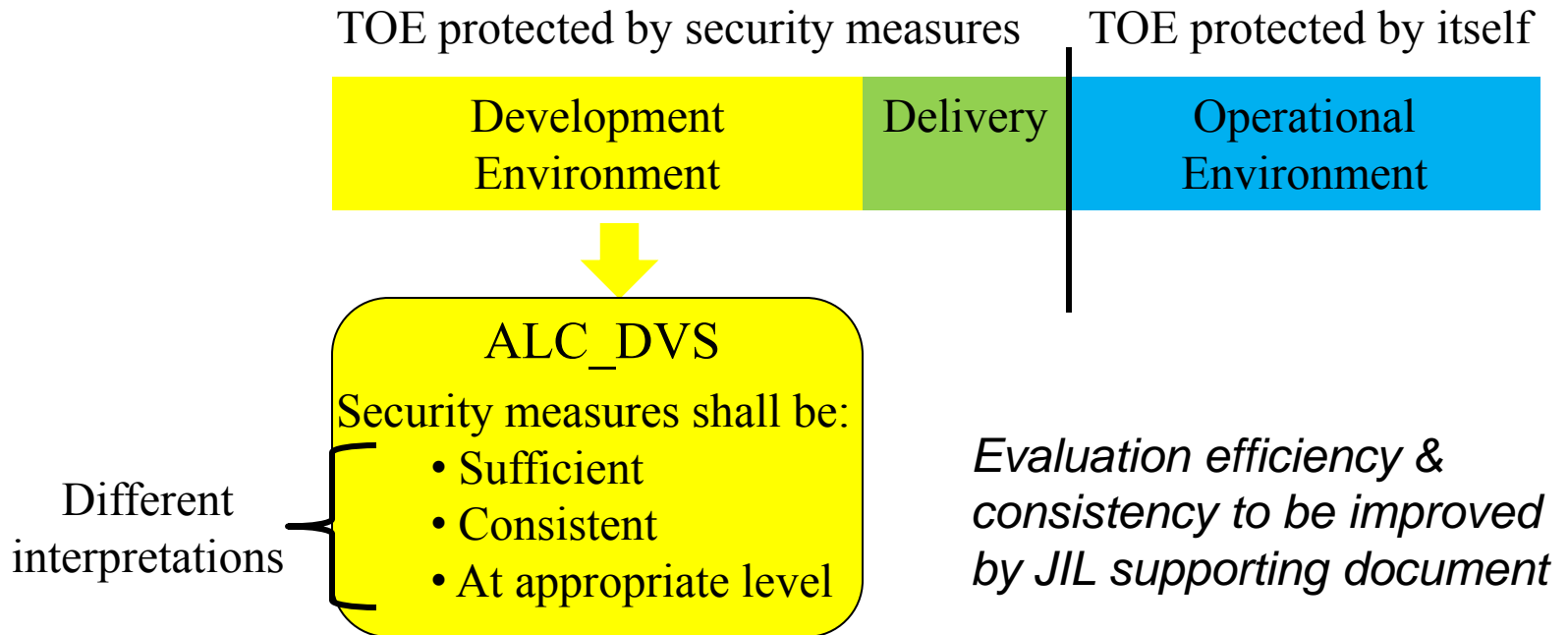
- CC is a moving target
  - Existing guidance and mandatory documents need to be updated to reflect changes in the CC.
- Smartcard & similar device is a moving target
  - Open architecture and layered structure
  - Multiple actors designing a product
  - Convergence of business cases
- CC provides higher assurance but does have a high overhead
  - that is increasing with product complexity
- There is a strong benefit working together to provide generic solutions to shared issues ...even between competitors.
  - developers, evaluators, certification bodies and other stakeholders
- Fair, high quality, comparable, standardised evaluations is not the only goal. **Efficiency is also desirable**
  - **Efficiency is the driving force of the current work program**

## ISCI WG1 this year: 4 axes

- ❑ Assurance related to the construction of the product
  - **Minimum Site Security Requirement**
  
- ❑ Specificities of Smart Secure Devices
  - **Security Architecture**
  
- ❑ Best practices
  - **Collection of evidences**
  
- ❑ Optimization
  - **Reuse of previous evaluation results**

## Minimum Site Security Requirements (1)

- Edited by Netherlands National Communication Security Agency



- Define the requirements the developer shall meet & the evaluator shall verify
- specifically for EAL4/5 + (high attack potential)
  - based on today's standard practices

## Minimum Site Security Requirements (2)

### Table of content

- Generic requirements
- Physical security
- Admission & escort of visitors
- Granting & revoking access rights
- Transfer of protected material
- Continued application of security measures and detection of security breaches
- Personnel
- IT security

### Structure

- Mandatory
  - Security objectives
- Informative
  - What could be done (Examples)
  - What is not acceptable

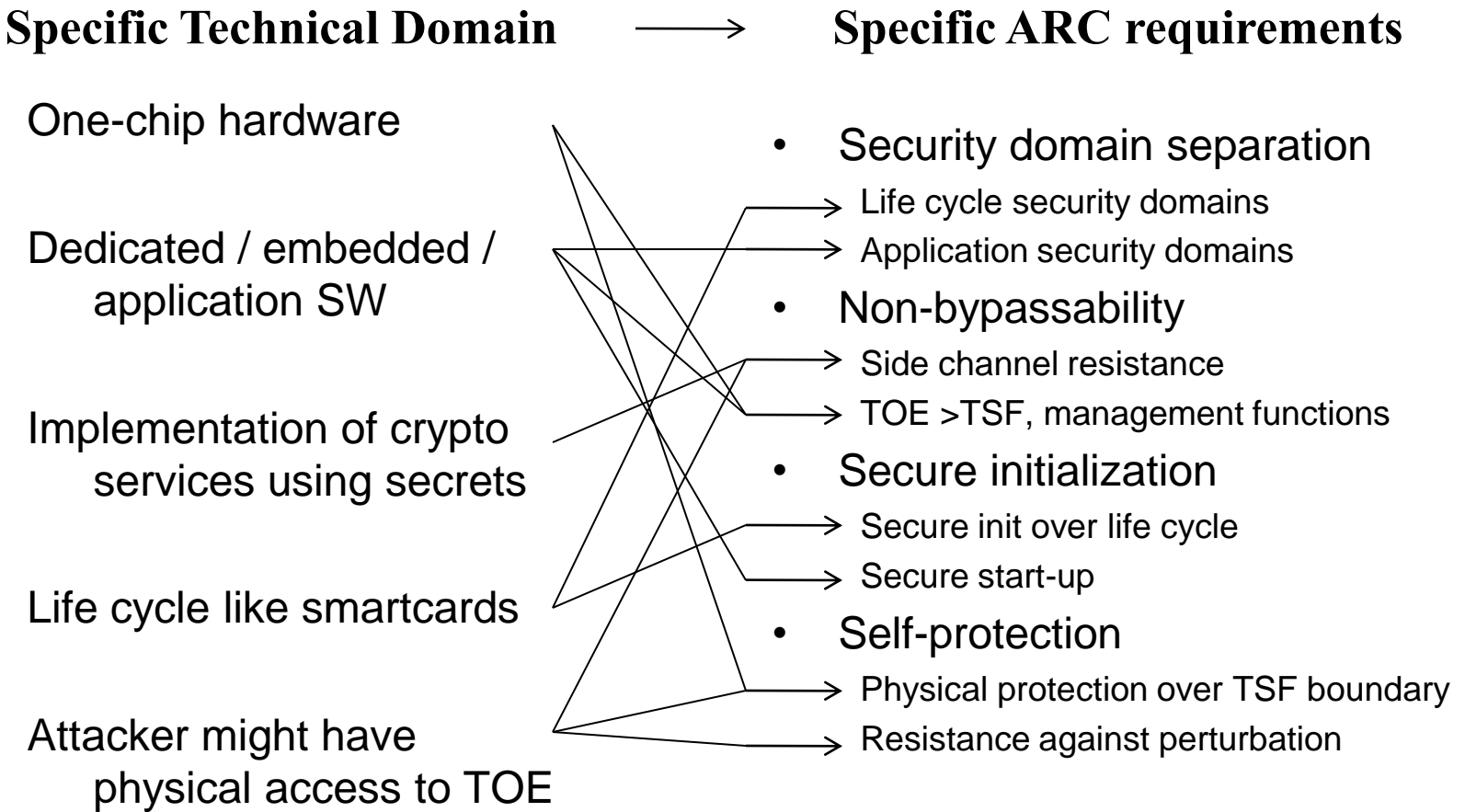
***Draft version  
Final release end 2010***

## ARC Guidance for Technical Domain « Smart cards & similar devices » (1)

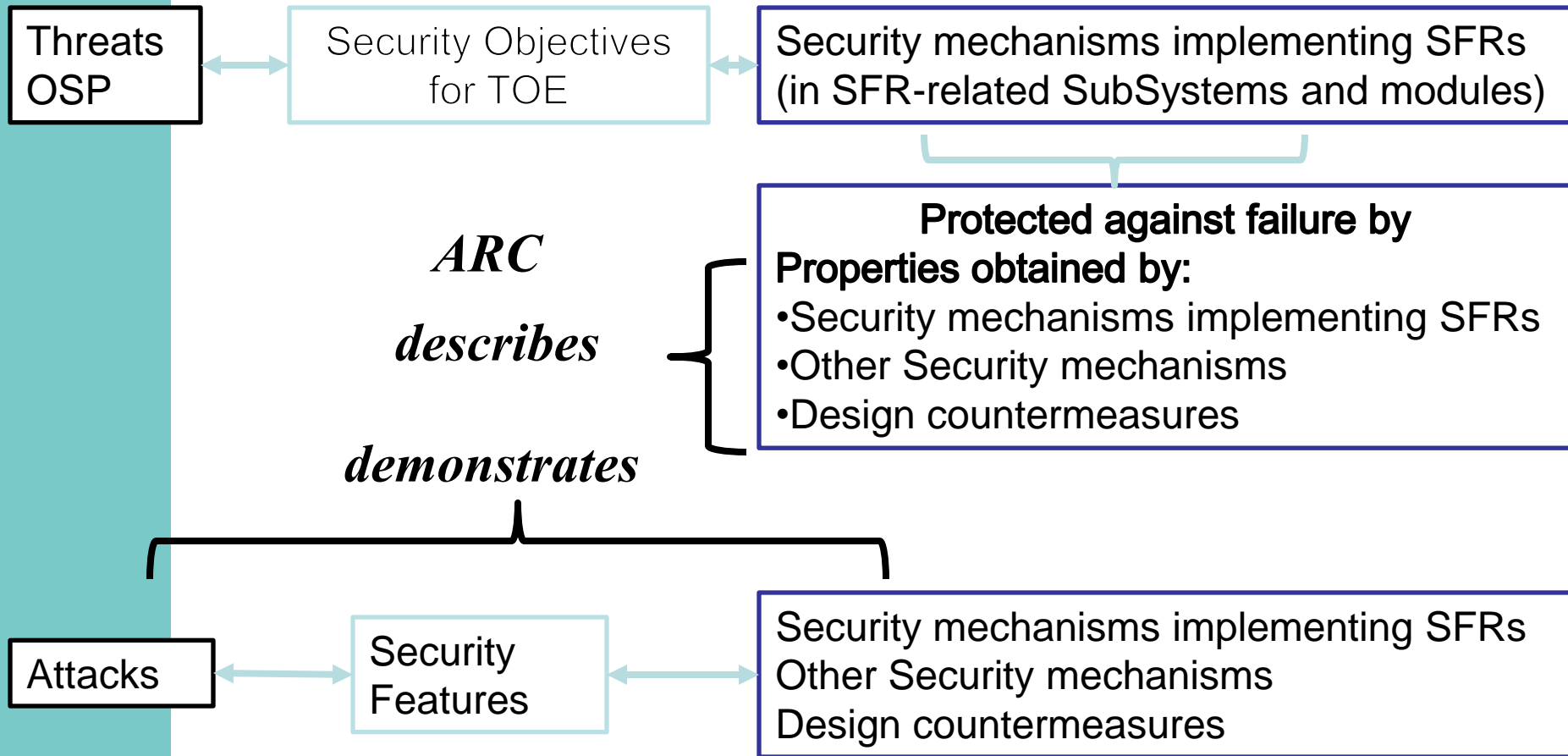
- Why do we need ARC guidance for a specific TD?
  - Supporting documents define how the criteria and evaluation methods are applied when certifying specific technologies
  - Supporting documents of a Technical domain are pre-requisites for SOGIS mutual recognition of certificates with assurance > EAL4
- What is specific with TD “Smart Cards & similar devices”?
  - TOE characterized by
    - One-chip hardware including dedicated, embedded or application SW
    - Implementation of cryptographic services using secrets
  - Environment characterized by
    - Life cycle like smartcards
    - Attacker might have physical access to TOE
  - *Examples of TOE within the TD SC&SD*

*Security Integrated Circuit , Smartcard (closed/open architecture) (composite TOE) (different form factor), Trusted platform module (TPM), One-chip cryptomodules*

## ARC Guidance for TD « SC & SD » (2)



## ARC Guidance for TD « SC & SD » (3)



## ARC Guidance for TD « SC & SD » (4)

- Security Architecture (ADV\_ARC) for smart cards and similar devices supporting document
  - Released as JIL trial supporting document (2008)
  - Feedback from experience with CC V3.1 evaluation of IC, closed and open platforms, applications (2009 / 2010)
  - Adapted to IC evaluation but needs to be revisited for IC+SW evaluation (2010 / 2011)
  - Draft content:
    - Mandatory part: ADV\_ARC requirements for the developer
    - Informative part:
      - Guidelines for application of the Security Architecture concept to Technical Domain « Smartcards & similar devices »
      - Examples
      - ADV\_ARC Template

## Applying Collection of Developer evidence (1)

- From experience it often happens that
  - Developer documentation are reformatted to fit clearly the CC requirement for evidence
  - CC breakdown of evidence is not the straight way for product understanding
  - Iterations are needed to complete the documentation
  - Work item check from the documentation is a long process due to the complexity of the product

⇒ Delays, developer and evaluator additional workload
- JIL paper “Collection of developer evidence” V1.1 brings an alternative allowing to
  - Take into account the developer practices
  - Perform a more efficient evaluation
  - Maintain the exhaustive approach needed by high attack potential

## Applying Collection of Developer evidence (2)

### What the JIL paper says?

- The developer must provide specified evidence but the format is not mandated.
- Collecting evidence from a number of separate sources and formats is legitimate evaluator work.
- The evaluator work must be limited to the objective *collection* of developer supplied material (e.g. by the means of open-ended questions or presentation of particular aspects of the TOE security)
- It is provided that:
  - Evaluator contributions are fully endorsed by the developer (the collection of evidence report is integrated in the TOE configuration management)
  - Approval is given in advance by the CB
  - The evaluator contributions are independently reviewed by other team member
  - Security Target and Guidance documentation are outside the scope

## Applying Collection of Developer evidence (3)

- Feedback from ITSEFs
  - Only one at the moment by Thales (see the presentation at this conference)
- Questionnaire to build the traceability to complete ADV\_TDS and ATE\_FUN, \_DPT, COV
- Interview for a rapid understanding of the developer documentation structure
- **Time for collection < Time for doc completion**
- **Product grasping easier**
- **Complete and consistent in one step**
- **Additional workload to elaborate the report**
- Other experiences are ongoing

**Positive feedback**  
**Reduced delays**  
**Reduced workload**

## Reuse of evaluation results (1)

- New usage cases appear in particular in the mobile card field
  - Convergence between business cases (Telecom, Payment, E-Signature, Transport, ...)
  - Same Application is running on different underlying platforms (e.g. Javacard)
  - Applications needs to be evaluated by different ITSEFs and possibly different CBs at EAL4+ level
  - Roles are reallocated to a number of actors: application developer, platform developer, product integrator, card issuer, application issuer ...
  - CC re-evaluations are costly and not always compatible with time to market
- CCRA-2002-09-009 “Reuse evaluation results and evidence” supporting document could be at the root of optimizing such multiple evaluations.
- CCDB-2007-09-001 “Composite product evaluation for smart cards and similar devices” authorizes a partial evaluation regarding the results obtained from previous application evaluation

## Reuse of evaluation results (2)

- **What the CCRA document says?**
  - Previous evaluation results and evidence of a TOE can be used, to the extent they are available
  - The evidence for the evaluation can include evaluation results and evidence produced by an evaluation facility as the result of a previous evaluation
  - The sponsor needs to provide the necessary information upon which future evaluation activities can be built, and this is directly related to the contractual agreement for the previous evaluation
  - The evaluation facility would be required to perform a delta analysis between the new security target and the original security target to determine the impact of changes on the analysis and evidence from the original evaluation
  - This delta analysis will determine the extent to which the results of previous evaluation(s) can be re-used in the current evaluation
  - Minimum items required are
    - Original ST, ETR, CR and Certificate
    - Original Evaluation Work Packages (if available)
    - New ST
    - Product and supporting documentation (including the evaluation evidence)

## Reuse of evaluation results (3)

- Some questions under study
  - Is the SecurityTarget delta analysis sufficient?
    - Platform delta analysis is required to extend the reuse to composite evaluation activities
  - How to determine the impact of differences on the re-use of results in a standardized way ?
  - To which extent the differences between applications and between platforms are possible for using this method?
  - Which form is acceptable by all parties in order to transfer evaluation results and evidence?
  - What is the real gain of such a method?
    - Feedback from experience is needed
- This ongoing work is done in collaboration with the Global Platform Security WorkGroup (see the presentation at this conference)

# Monitoring Common Criteria for Smart Cards and Similar Devices

**Thank you !**

**Questions?**