



➔ **A more efficient method for performing evaluations**

11th ICCC, Antalya, 21-23 September 2010

Thales ITSEF: A more efficient method for performing evaluations

- ▶ Purpose
- ▶ Origins
- ▶ Presentation of the method
- ▶ Examples of usage
- ▶ Conclusion



Thales ITSEF:

- ➔ HW & embedded SW ITSEF
- ➔ Under ANSSI agreement

- ▶ Speaker: **Sophie LABORDE** (Sophie.Laborde@thalesgroup.com)
 - Evaluator for 8 years
 - Member of the ISCI-WG1 working group
 - Risk manager ISO/IEC 27005:2008 (certified by LSTI)

Purpose of Thales ITSEF efficient method



- ▶ Maintain the resistance/assurance level on complex products
- ▶ Perform an “efficient” assurance evaluation
 - “resistance oriented” assurance evaluation.
- ▶ Take into account “time to market” issue
 - Without impacting evaluation level.
- ▶ Take into account developer practices
 - (Fit the method with the practice) if the CC requirements can be covered



- EAP_VAN5 feedback
- JIL Collection of Developer Evidence v1.1
- ITSEF experience

Evaluation method



▶ EAP_VAN5 feedback from the ISCI-WG1



- ▶ Gemalto (F. Guérin) has proposed a new assurance package, defining new assurance components for ADV. Two of the main ideas were:
 - Training on TOE usage to obtain early in the evaluation a functional knowledge of the product (ADV_TRA)
 - Components derived from ADV_TDS and ADV_ARC: ADV_TDK and ADV_ARK introducing the notion of information
- ▶ Principles were considered interesting, but it would be more interesting working directly on EAL:
 - Keeping existing assurance components and improving the evaluation method
 - Training on the product, interviews can also be part of the evaluation method
- ▶ Indeed, a new assurance package could have a limited acceptance:
 - Mutual recognition by CC community
 - Interest for customers: what is the difference with classical EAL?



▶ JIL Collection of Developer Evidence v1.1

- ▶ Discussing the EAP_VAN5 package with the ISCI-WG1 working group permitted to conclude that the JIL document could be a basis for an evaluation optimization method (and keep the EAL level packages).
- ▶ The JIL document proposes to improve flexibility for obtaining evaluation evidence.
- ▶ The JIL document permits to "remain" within the existing EAL level packages.



▶ ITSEF experience

- ▶ Discussion with developer improves knowledge of the TOE with efficiency
- ▶ Evaluations are often impacted by documentation problems (delays, additional workload, ...)



Main evaluation issue → Documentation related iterations

(information incomplete in documentation, that is to say, the contents required by the assurance component can be finally verified even if they are not initially documented)

moreover,

- CC documentation does not always represent the “reality”.**
- CC documentation does not always help for evaluator’s product understanding.**

Consequences:

- Delays
- Additional evaluation Workload
- Additional project management Workload
- Additional developer Workload



Objective → Avoid most of documentation iterations

→ Product training after ASE (knowledge and confidence)

→ Interviews to compensate lacks in the documentation - by using the JIL collection of developer evidence

→ Formalized in questionnaires filled by the evaluator that will be recorded as complementary evaluation evidence.

→ There are therefore two possibilities for “evidence” presentation:

→ Documentation (classical)

→ Information (existing documentation + complementary filled questionnaire)



▶ **Three major assumptions are defined in the JIL document to guarantee evaluator independency, the ITSEF methodology verifies them:**

- ▶ Evaluator contributions are fully endorsed by the developer → the questionnaire is accepted by the developer and integrated in the documentation CM of the TOE
- ▶ Approval is given in advance by the CB → the CB is informed at the evaluation registration or during kick-off meeting.
- ▶ The evaluator contributions are independently reviewed by other members of the evaluation team, and their review is documented in the ETR → Evaluation reports are already systematically reviewed, a focus is done on the collection/creation of evidence verification



- ▶ **Some assurance components are not concerned by this method:**
 - ▶ ASE / APE
 - Basis for evaluation understanding/public document
 - ▶ AGD
 - Part of the TOE deliveries, deficiencies are not acceptable
 - ▶ Work units of components that involve semi formal/formal method
 - Cannot be applicable for formal model (but can be used for the understanding of the model)

The ITSEF considers that the other assurance components can be evaluated with the help of this methodology



- ▶ **A Design documentation has been delivered to the ITSEF**
 - ▶ The level of description was sufficient for TDS (modules and subsystem description), but the traceability was missing
 - ▶ A mapping was asked during a first iteration. The mapping delivered was not useful for the evaluator (“security mechanisms” vs SFRs)
- ▶ **A visit was the occasion to complete TDS evaluation thanks to a questionnaire**
 - ▶ The purpose of the questionnaire was to make the traceability, not to obtain additional design information



SFR	SFR description	TDS subsystem	TDS module
Cryptographic key management (FCS_CKM)	<i>FCS_CKM.3.1. The TSF shall perform a read of cryptographic key in accordance with a specified cryptographic key access method, a temporary copy key in RAM that meets the following: none.</i>	SS1, SS2	Function1() calls function2()
	<i>FCS_CKM.4.1. The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method, erasure of a temporary copy key present in RAM, that meets the following: none.</i>	SS3	Function3()

- **First step:** the evaluator listed the SFRs and their associated definition (he is able to “translate/interpret” them to the developer during the interview if necessary)
- **Second step:** during the interview the developer indicated to the evaluator which module(s) and subsystems are implementing each SFR
- **Third step:** the evaluator was able to refer to TDS documentation and to give an overall verdict
- **Fourth step:** internal review by another evaluator, integration of the document to the TOE CM.



▶ Advantages:

- ▶ Two methods have been tried on the same task evaluation
 - Classical iteration was unsuccessful
 - Interview permitted to conclude for TDS task
- ▶ Evaluation of evidence obtained “on the field” completed successfully the documentation.
- ▶ The time used for collecting evidence on site was shorter than the time usually used for analyzing this kind of mapping.
- ▶ Workload saved for the developer

▶ Constraints:

- ▶ An additional specific work has been done by the evaluator to elaborate the collection of evidence report
- ▶ Nevertheless, we considered that global workload for traceability analysis was less important than a classical approach. Moreover, this workload permitted to conclude the TDS task without any iteration. Approach depending on the initial contents of developer documentation



- ▶ **The usage of the collection of evidence method was decided at the beginning of the evaluation to minimize the risk of any evaluation delay.**
- ▶ **ATE task was concerned.**
- ▶ **Incomplete ATE documentation was delivered before the collection of evidence (2/3 of final documentation):**
 - ▶ No “obvious” CC mapping from the evaluator point of view
 - ▶ The documentation finalization was still on-going when ATE evaluation was beginning
- ▶ **The visit was the occasion initiate the evaluator analysis as much as possible:**
 - ▶ Understanding the documentation articulation
 - ▶ Understanding the whole testing process
 - ▶ Obtaining the CC traceability thanks to interview



- **First step: the evaluator prepared some questionnaires (see next slides for details)**
- **Second step: during the visit the developer give some answers such as:**
 - **Complete and detailed answers permitting to conclude**
 - **References to delivered documents permitting to avoid the evaluator some difficult search in the amount of delivered information**
 - **Demonstrations of real testing**
- **Third step: the evaluator was able to complete the analysis after the visit and to give an overall verdict**
- **Fourth step: internal review by another evaluator, emission of the report, acceptation of the report by the developer and integration of the document to the TOE CM.**



ATE_COV.2: TSFI testing

TSFI	Question to the developer : can you identify the tests permitting to verify the following TSFI functionality	Answer
TDES enciphering	TDES enciphering Associated countermeasure(s) functioning	See document xxx chapter y.z (document delivered)
TSFIxx	Functionality 1 Functionality 2	Documentation seen on site, not delivered yet => OK (reference ZZZ)
TFSlyy	Functionality	The developer explains the following: The evaluator audited that explanations corresponds to actual practises (not completely described in documentation)



ATE_DPT.3: subsystem interactions

Subsystem	Question to the developer : can you identify the tests permitting to prove the correct interaction between subsystem for the following interactions	Answer
SS1	With SS2: service xx provided by SS2 to SS1	Test of error code xx at TSFI aa Emulator: test zz Etc.
SS1	With SS5: error detected/managed by SS5 when SS1 functionality processing	Characterisation xx
SS2	With SS3	...



ATE_DPT.3: Modules testing

Module	Question to the developer : can you identify the tests permitting to verify that the modules interfaces have been tested	Answer
Module1	See document ZZZ already delivered	
Module2	Informal description to complete document yyyy:	
Module3	The developed showed the associated document during the visit, the evaluator concluded that it is done thanks to	



▶ Advantages:

- ▶ The evaluator obtained a global understanding of the testing approach very efficiently compared with documentation analysis only=>aid for FUN, COV, DPT work units evaluation
- ▶ Confidence in developer practice: the evaluator is able to determine on site the knowledge of the testing processes by the developer. For example, a developer being able to answer quickly by referring to documentation permits to be confident that documentation is not “CC-only” documentation
- ▶ Independent thinking of the evaluator before analyzing developer document: it avoid the evaluator to fit automatically developer approach
- ▶ Obtaining any documentation corresponding to the information collected will not have been possible in the evaluation schedule
- ▶ Workload saved for the developer and for the developer

▶ Constraints:

- ▶ An additional specific work has been done by the evaluator to elaborate the collection of evidence report and to complete it after the visit (the visit was not sufficient by itself).
- ▶ It was difficult to explain to the developer that the visit does not permit to give immediately a verdict for the task as additional workload was necessary after the visit (different from an environment audit):
 - Finishing the analysis
 - Review from another evaluator
- ▶ The workload saved for this evaluation is difficult to evaluate precisely, however we think that we saved some (and/or the workload permitted to obtain a deeper understanding)
- ▶ This new experience confirms that this approach is quite specific, depending of each evaluation need.



- ▶ This new approach still guarantees the evaluator independency
 - ▶ The evaluator verdict is still depending on the contents of information obtained
 - ▶ The questionnaire is reviewed and validated by another ITSEF member (evidence collection)
 - ▶ Evaluator contributions are fully endorsed by the developer who shall approve the questionnaire (it becomes a “classical delivery”)
 - ▶ Once the questionnaire becomes a delivery, it is integrated in the TOE configuration.
- ▶ This new approach does not replace the classical approach
 - ▶ It is proposed as an option in case documentation would be written only for CC needs
 - ▶ In case the evaluator would not be able to give any verdict because interviewed people do not cooperate enough, additional documentation could be required



Any questions?

Thank you for your attention...