Open Smart Card Infrastructure for Europe

V2

Volume 8: **Security and Protection Profiles**

Part 3-3: **ETR-lite for composition: Annex B Guidance for composite evaluations of multi-application smart cards on open platforms**

Authors: **eESC TB3 Protection Profiles, Security Certification**

NOTICE

This eESC Common Specification document supersedes all previous versions.

Neither eEurope Smart Cards nor any of its participants accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this document.

Latest version of OSCIE and any additions are available via www.eeurope-smartcards.org and www.eurosmart.com. For more information contact info@eeurope-smartcards.org.

Preamble

In continuation to the work done in a two layers smart card architecture which edited the document “ETR-Lite for composition” – **Annex A: Composite Smart Card evaluation: Recommended best practice, IC and ES composition, Version 1.2 – March 2002** endorsed as JIL document, this document presents the evaluation methodology and recommendations for a three layers smart card architecture.

Audience

This document is dedicated to Smart Card issuers, IC manufacturers, Smart Card Operating System & applications developers that are already familiar with smart card architecture and Common Criteria, in particular with the C.C. assurance requirements (Part3).

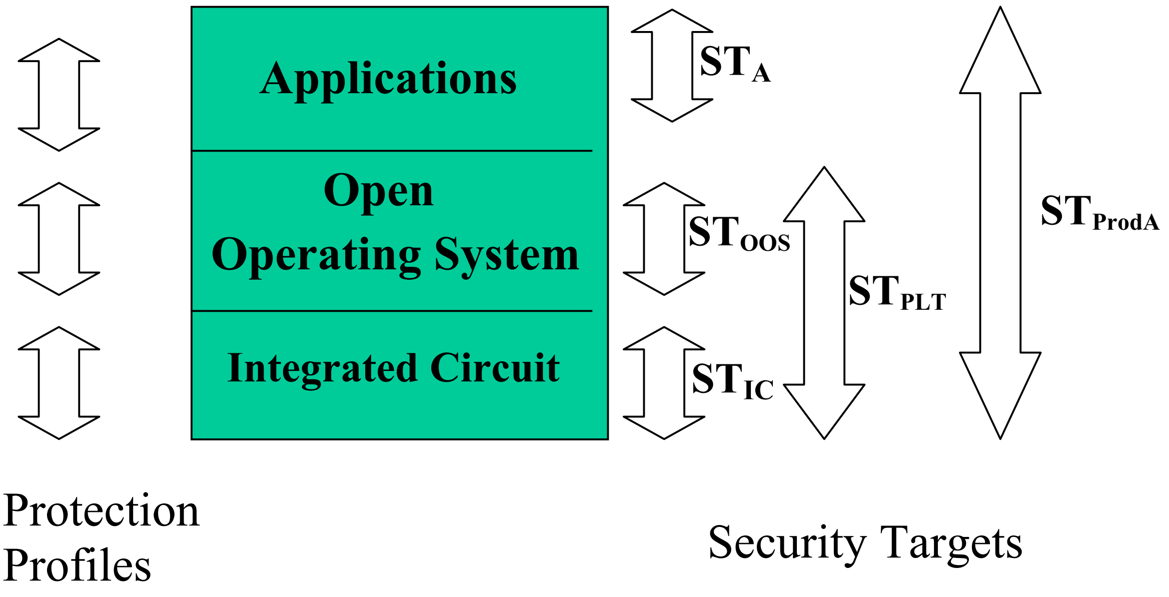
Table of Contents

1 Composite Evaluations for three layer Smartcard Products

The goal of eEurope Smart Card Trail Blazer 3 SubGroup1 is to make recommendations on how to go to a product evaluation using a modular approach that allows the most re-usability in composite evaluations.
The hypothesis of work is the smartcard product requires a High level of security, resistant to a high attack potential that is being evaluated and certified in a Common Criteria security evaluation scheme.

1.0 Introduction

The evolution of smartcard technology towards Open Operating Systems, lead to the consideration of a modular approach that takes into account a three layer product architecture: the IC, the Open Operating System (OOS) and the Applications.



7 types of evaluations are identified as follows:

- Type 1: Evaluation of Open Operating System **on** IC_1 (Scope of ST_{OOS}).
- Type 2: Evaluation of the platform PLT_1: OOS **with** IC_1 (scope of ST_{PLT1}).
- Type 3: Re-evaluation of the platform PLT_2: OOS **with** IC_2 (scope of ST_{PLT2}).
- Type 4: Evaluation of the Application **alone** (Scope of ST_A)
- Type 5: Evaluation of the Application **on** a platform PLT_1 (Scope of ST_A).
- Type 6: Evaluation of an Application **with** platform PLT_1 (scope of ST_{ProdA1})
- Type 7: Re-evaluation of an Application **with** platform PLT_2 (scope of ST_{ProdA2})

Note 1: a further type, the combination (OOS + Application) with IC, is not covered here because it appears to be the same case as IC with embedded S/W (see ETR-lite –Annex A). This type would contradict the modularity that brings the OOS.

Note 2: S/W alone for an OOS is irrelevant due to the tight integration between H/W and S/W on a smart card product. Alone meaning here without any reference to any hardware that the S/W is supposed to run on.

S/W alone can make a sense in case of, for instance, an applet for a smartcard; this is discussed in Type 4.

In the reminder of this document, the details of these different evaluations will be discussed in terms of the Scope of the Evaluation, Developers' activities, Evaluation activities and Recommendations on Use; showing the best re-usability for the complete product evaluation.

In summary, the **recommended Composite evaluation strategy is a Type 2 evaluation followed by a Type 6 evaluation.** This strategy represents the optimum of evaluation re-usability and trust in product robustness; Type 2 and Type 6 include both evaluation activities of the upper layer, re-usability of the lower layer and evaluation activities related to the composition of these two layers.

For the complete product the corresponding evaluation will encompass the three layers with re-usability of the OOS and its IC: Type 6 and 7.

Summary of recommendation:

Type N°	Recommendation for use	Index of Developer & evaluation efforts	Index of confidence towards the product
Type 1	First step for correctness of OOS, but does not give a complete view on Platform robustness. Composite evaluation is needed towards final product evaluation and certification. Moreover, significant effort is needed for this type of evaluation, implying significant costs, compared to a type 2	**Significant**	**70**
Type 2	**Most efficient** step for the platform and towards final product evaluation and certification. Re-usability of this certificate is a key issue within this respect.	**Significant & Complete**	**90**
Type 3	Efficient and cost-effective for maximum costs and timesavings in case the platform' IC is changed.	**Medium**	**90**
Type 4	Can be used when the developer does not know on which platform the applet is being loaded to get confidence on the Application development process Difficulty to focus on the security of the transactional application layer without the platform; today most of the application PPs include OOS security features.	**Minimum**	**5**
Type 5	First step for correctness of Application, but little indications on final product robustness. Composite evaluation is needed towards final product evaluation and certification.	**Light**	**15**
Type 6	**Most efficient** approach **to final product** evaluation and certification. Re-usability of certificate is a key issue within this respect.	**Light**	**100**
Type 7	Efficient and cost-effective for maximum cost and time savings in case the IC is changed for the same Platform.	**Very light**	**100**

Index of developers/evaluator effort: rough estimated amount of work for the developers to provide the appropriate assurance documentations and for the evaluator to verify the conformance related to security features described in a Security Target (Scale from very light to complete)

Index of confidence towards the product: rough estimated confidence gained towards the final product security related to security features described in a Security Target. (Scale from 0 to 100 %)
It is important to state that the confidence given through a security certificate to a product is valid when the certificate is emitted; only the maintenance of a product certificate will guarantee confidence during time.

Glossary:

- **Integrated Circuit (IC):** Electronic component(s) designed to perform processing and/or memory functions. (i.e. the hardware component containing the micro-controller and IC dedicated software).

- **Platform:** a usual denomination for a smart card component which may undergo an evaluation process, as a complete Target of Evaluation (TOE) in itself but is not an end-user product (i.e., for instance, a smart card component without any Application Software loaded).

- **Product:** a product corresponds to a fully operational smart card, composed of both IC and complete ES, including an application software, if appropriate.

- **TOE**: Target of Evaluation is a Common Criteria terminology addressing the object of the evaluation.

1.1 Evaluation type 1: Evaluation of an Open Operating System on IC_1

1.1.1 Scope of the evaluation: ST_{OOS}

The scope of evaluation is the OOS **on** an identified IC1.
Hypothesis:
- The OOS has dependencies on the IC_1 security features but the IC_1 may not be certified. In this case the IC_1 is seen as a black box.

1.1.2 Developer activities

The **Security Target** author will have to define the security interfaces with the IC_1 and specify IC1 IT security objectives for the TOE environment.
It is recommended to refine these IC_1 IT security objectives for the TOE environment into IT security requirements stated in the form of "SFRs " to ensure easier traceability to existing IC_1 security features.
The ST will also have to refer to the detailed reference of the IC_1, and the IC_1 guidance manuals references.

The developer needs the IC_1 users' guidance manuals.
The developer has to implement IC security guidance if any or justifies any equivalent method.
All the other evaluation deliverables should be compliant to CEM.

1.1.3 Evaluation activities

The evaluator requires the IC_1 users' guidance manuals but not the ETR-Lite (it may not exist).

The evaluator has to check if the IC_1 recommendations have been taken in account by the S/W developer.
The evaluator will perform "penetration tests" on the OOS as required by the evaluation scope and will also perform 'blind' penetration test on the platform (including environmental modification such as DPA, EMA, DFA....) to challenge the overall platform (IC+OOS) security.
No invasive penetration tests are performed on the IC_1 (i.e. no physical modification on IC)

1.1.4 Recommendations on use

This type of evaluation is recommended for an initial experience of security evaluation or when the IC is not certified yet, in order to qualify the security of the Platform. This type of evaluation is a significant step for enforcing OOS correctness but will not give a complete view on on platform robustness.

As far as developers' and evaluators' activities are concerned, they represent around **80% of the workload** for compared to a composite evaluation of the OOS with the IC_1.

In order to progress towards a complete platform evaluation, composite evaluation tasks with the IC_1 will be required.

1.2 Evaluation type 2: Evaluation of the platform composed of an OOS with an IC_1

1.2.1 Scope of the evaluation: ST_{PLT1}

The scope of the evaluation is the composite platform PLT_1 of the OOS **with** the IC_1

Hypothesis:

- IC_1 has been certified and is being maintained.
- This is the first evaluation of OOS with an IC.

Subsequent evaluations of OOS with a different IC are addressed in next chapter.

1.2.2 Developer activities

The ST author needs to know about the IC_1 certificate reference, the IC_1 detailed reference, the IC_1 guidance manuals references and the IC_1 ST-lite.
Moreover, the developer needs to know about the IC_1 Security User Manual.

The Composite Platform Security Target will include at least the IC ST-lite contents and the OOS PP with all operations completed.
The number of threats for the composite product may be greater than the sum of the threats of the IC and the OOS, due to the possibilities of combinations of threats that are not adequately countered by either the IC or the OOS security functions alone.

The ST author has to ensure consistency and coherence at the composite Platform level.

1.2.3 Evaluation activities

The Composite platform evaluation methodology is the same as described in the "ETR-Lite –Annex A.: - Composite Smart Card Evaluation".
As for any composite evaluation activities are shared into OOS dedicated activities and composite activities.

The evaluator needs to know about the IC_1 certificate reference, the IC_1 detailed reference, the IC_1 guidance manuals references (IC_1 data sheet, the IC_1 Security User Manual), the IC_1 ST-lite and the ETR-lite from the IC_1 evaluation results.

Through the ETR-lite (including the list of the IC_1 mechanisms), the evaluator gets information on the IC vulnerability analysis and the IC_1 penetration tests that were performed during the IC_1 evaluation usually performed by another laboratory (ITSEF).
The evaluator has the complete information on OOS with IC_1 vulnerabilities and shall perform additional penetration tests, including invasive test on IC_1.
The global vulnerability analysis shall demonstrate an attack path could not defeat the Software security, through the deactivation or corruption of a hardware mechanism.

1.2.4 Recommendation on use

This type of evaluation is recommended because it is the most efficient intermediate step towards the final product evaluation.

1.3 Evaluation type 3: Re-evaluation of the platform PLT_2: OOS with IC_2

1.3.1 Scope of the evaluation: ST_{PLT2}

The scope of the evaluation is the **composite** platform PLT_2 of the OOS **with** the IC_2
This scope corresponds to the case of a card manufacturer who requires a second source product relative to the IC.

Hypothesis:

- A previous platform PLT_1 (OOS with IC_1) was certified and is being maintained.
- The OOS is adapted to IC_2.
- The IC_2 has been certified previously and is being maintained
- The IC_2 provides about the same security functions as IC_1.
- All OOS evaluations and maintenance are performed in the same laboratory for optimum re-use.

The new platform has to be **evaluated and certified.**

1.3.2 Developer activities

The ST author needs to know about the IC_2 certificate reference, the IC_2 detailed reference, the IC_2 guidance manuals references and the IC_2 ST-lite.
Moreover, the developer needs to know about the IC_2 Security User Manual.

Most deliverables from the previous PLT_1 evaluation can be re-used; see details below:

Assurance Requirements	**Developer's deliveries**
ASE: Security Target	Updating of the composite platform Security Target: The work on the ST will vary according to the differences between the content of the IC_2 ST-lite and IC_1. No formal claim to an IC PP is mandatory.
ACM: Configuration management	New configuration list.
ADO: Delivery and operation	May need a new document if the process is different with this manufacturer.
ADV: Development	Partial re-use: At least the ADV lower levels (i.e. HLD, LLD, IMP, RCR). Full Re-use: FSP, SPM.
AGD: Guidance doc	Full re-use.
ALC: Life cycle support	Full re-use.
ATE: Tests	ATE.FUN, IND,.DPT: Test plan partial re-use according on HLD changes; New prototypes and Tests results. Full re-use: ATE.COV,.
AVA: Vulnerability assessment	AVA.MSU, AVA.SOF: Full re-use. AVA.VLA: New update on IC dependencies.

1.3.3 Evaluation activities

The evaluator needs to know about the IC_2 certificate reference, the IC_2 detailed reference, the IC_2 guidance manuals references (IC_2 data sheet, the IC_2 Security User Manual), the IC_2 ST-lite and the ETR-lite from the IC_2 evaluation results.

As for any composite evaluation activities are shared into OOS dedicated activities and composite activities:

Assurance Requirements	**Evaluation Activities**	
	OOS Dedicated Activities	**Composition Activities (Completely redone)**
ASE: Security Target	Re-evaluation: the evaluator has to verify the claimed IC_2 Security Functions of the composed ST_{PLT2} are part of the IC_2 ST-lite.	
ACM: Configuration management	Only Configuration list checking.	Integration of the OOS software in the IC2 manufacturer configuration management system.
ADO: Delivery and operation	None.	Consistency check for delivery and pre-personalization procedures.
ADV: Development	Important work on the HLD, LLD, IMP, RCR.	Compliance with the IC_2 Security User Manual in light with IC_2 ETR-lite.
AGD: Guidance documents	None.	None
ALC: Life cycle support	None.	None
ATE: Tests	ATE.IND, DPT, FUN: New check on tests results on low layers. ATE.COV: no change.	Composite product functional testing.
AVA: Vulnerability assessment	Partly redone for IC_2 dependencies	Composite product vulnerability analysis.

1.3.4 Recommendations on use

This type of evaluation is recommended for evaluation results re-use in the case the IC changes.

1.4 Evaluation type 4: Evaluation of an application A alone.

1.4.1 Scope of the evaluation: STA

The TOE scope is the application only dedicated to a generic smart card platform but with no specific platform reference.
It can be for instance, an applet compliant to a referenced Javacard specification.
The TOE is obviously a mono application.

1.4.2 Developer activities

The Security target author will have to take care to address for the TOE only the security transactional security features related to the application; the others security objectives relative to a platform where the application may be loaded, may be introduced as part of the TOE IT environment.
Warning: Current applications PPs do not fit the scope of this type of evaluation because most PPs include platform security features.

All the other assurance deliveries should be compliant with CEM.
No smart card needs to be supplied; the software is supplied on an appropriate media.

1.4.3 Evaluation activities

The evaluation of an Application alone is a pure software evaluation.
No evaluation tasks cover the TOE IT environment.

1.4.4 Recommendation on use

It can be recommended for a first experience when the developer is not the platform developer otherwise the type 5 is recommended.
This type of evaluation is a significant step for enforcing Application development process but will give little indications on product robustness.
Once the application is evaluated alone and a platform is evaluated on another side, the results of those evaluations do not guarantee anything about the combination of both.
To progress towards a complete product evaluation, composite evaluation tasks with a platform will be required. As a consequence, the effort needed for this type of evaluation will not be entirely saved in the next step (i.e. final product evaluation and certification).

1.5 Evaluation type 5: Evaluation of an application <u>on</u> the Platform PLT_1

1.5.1 Scope of the evaluation: ST_A

The TOE scope is the application A on a specific platform $PLT_{1.}$
Hypothesis:

- The TOE environment consists of the platform PLT_1 and any coexisting application
- The platform PLT_1 and any coexisting application may not be certified yet.

In the environment of the application A, others applications (ie Application B) may co-exist with their appropriate relationship with Application A. This relationship is under the scope of the evaluation**.**
In this case, the application B may be require the same type of evaluation, then Application A is to be taken in its environment.

1.5.2 Developers' activities

The **Security Target** author will have to define the security interfaces with the PLT_1 and eventually with any other co-existing application; they have to be specified as IT security objectives for the TOE environment.
It is recommended to refine these IT security objectives for the TOE environment into IT security requirements stated in the form of "SFRs " to ensure easier traceability to existing PLT_1 security features.
The ST will have to refer to the detailed PLT_1 reference and the PLT_1 guidance manuals references.
Warning: Current applications PPs do not fit the scope of this type of evaluation because most PPs include platform security features.
The Application developer needs the PLT_1 users' guidance manuals; he has to implement PLT_1 security guidance if any or justifies any equivalent method.
All the other deliverables should be compliant to CEM.

1.5.3 Evaluation activities

The evaluator needs the PLT_1 users' guidance manuals ; ETR-lite may not exist and is not required.
The evaluator checks if the PLT_1 recommendations are taken in account by the Application developer.

The evaluator will perform penetration test on the Application as required by the evaluation scope and will also perform 'blind' penetration test with the Platform PLT_1 to challenge the overall combination. The TOE environment is seen as a black box.
All the other evaluation tasks should be compliant to CEM.

1.5.4 Recommendation of use

It can be recommended for a first experience of security evaluation in order to qualify the security of the Application development process. This type of evaluation is a significant step for enforcing Application correctness but will give little indications on product robustness.
Warning: Current applications PPs do not fit the scope of this type of evaluation because most PPs include platform security features.
To progress towards a complete product evaluation, composite evaluation tasks with a platform will be required. As a consequence, the effort needed for this type of evaluation will not be entirely saved in the next step (i.e. final product evaluation and certification).

This type of evaluation is mainly of interest when the application developer is not the platform developer.

1.6 Evaluation type 6: Evaluation of an application with the Platform PLT_1

1.6.1 Scope of the evaluation: ST_{ProdA1}

The TOE encompasses the **product ProdA1**: Application A WITH the platform PLT_1 (OOS with IC_1). It is a **composite evaluation** of the Application A and the platform PLT_1.

Hypothesis:

- The platform has been already certified and is being maintained.
- The application A has not been certified (such as Type 4 or 5).

In the environment of the application A, others applications (ie Application B) may co-exist with their appropriate relationship with Application A. This relationship is under the scope of the ProdA1 evaluation**.**
In this case, the product ProdB1 may be require the same type of evaluation, then ProdB1 have to take into account Application A in its environment.

1.6.2 Developers activities

In the Security Target of product $ProdA_1$ most of the non- transactional security objectives will be addressed by the platform PLT_1; the ST_{ProdA1} author will map the product IT security objectives on the application level only and/or the platform PLT_1; mapping with ST-Lite of the platform PLT_1 is mandatory.

The ST_{ProdA1} has to refer to the Platform certificate reference, the detailed reference of the Platform and the Platform guidance manuals reference (the Platform administration and user guidance, Platform Security Users' Guidance).

The Application developer has to implement the recommendations of the Platform Security Users' Guidance or justify equivalence of another method.
The knowledge of the PLT_1 Security Users' Guidance may lead to a deeper composite vulnerability analysis.

The other deliverables will require almost the same workload as for the application on a platform.

1.6.3 Evaluation activities

The evaluator needs to get the Platform PLT_1 certificate reference, the PLT1 detailed reference, the PLT_1 guidance manuals reference (the Platform administration and user guidance, Platform Security Users' Guidance) and the ETR-lite of the PLT_1 evaluation.

As for any composite evaluation activities are shared into Application dedicated activities and composite activities with the Platform PLT_1:

Assurance Requirements	**Evaluation Activities**	
	Application Dedicated Activities	**Composition Activities**
ASE: Security Target	Evaluator has to verify the claimed Platform Security Functions of the composed ST_{ProdA1} are part of the Platform PLT_1 ST-lite.	
ACM: Configuration management	CEM compliant.	None
ADO: Delivery and operation	CEM compliant.	Consistency check for delivery and pre-personalization procedures. If application is loaded, a means to identify unambiguously the application is to be checked at the application-loading site.
ADV: Development	CEM compliant.	Compliance with the Platform PLT_1 user and administrator guidance's, PLT_1 Security Users' Manual.
AGD: Guidance documents	CEM compliant.	None
ALC: Life cycle support	CEM compliant.	None
ATE: Tests	CEM compliant.	Composite product functional testing.
AVA: Vulnerability assessment	CEM compliant.	Composite product vulnerability analysis with knowledge of ETR-lite of PLT1.

1.6.4 Recommendation on use

The evaluation type reaches the ultimate goal for a <u>product certification</u> and to gain the highest security confidence in the product.

If the Application has been evaluated, then the Application dedicated evaluation activities are not to be performed again.

In case of multi application, the product ProdB1 may be require the same type of composite evaluation. The certificates of ProdA1 and ProdB1 will encompass the complete product and does not require any additional evaluation tasks. It is the evaluation strategy to adopt in such a case for a better re-usability where one application may evolve separately from the others.

1.7 Evaluation type 7: Re-evaluation of the Application A with Platform PLT_2

1.7.1 Scope of the evaluation: ST_{ProdA2}

The TOE encompasses the **global product**: Application **with** the platform (OOS with IC_2); it is a **composite evaluation** of the Application A with the platform PLT_2.
This is the case that corresponds to a second source product relative to the IC.

Hypothesis:
The product $ProdA_1$ has been already certified and is being maintained.
The platform PLT_2 has been already certified and is being maintained.
The same laboratory that evaluated the ProdA1 for a better internal re-use, performs this new evaluation.

1.7.2 Developers activities

The main documents that will indicate the level of changes from the previous evaluation deliveries, are: Platform PLT_2 user's guidance, PLT2 ST-lite and PLT_2 Security User's Guidance.

Most of the deliveries are unchanged or required very little updates.

Assurance Requirements	**Developer's deliveries**
ASE: Security Target	Updating of the composite platform Security Target: The work on the ST will vary according to the differences between the content of the PLT_2 ST-lite and PLT_1 ST-lite. .
ACM: Configuration management	New configuration list.
ADO: Delivery and operation	May need a new document if the process is different with this manufacturer. TBC
ADV: Development	Partial re-use: At least updates of the ADV lower levels (i.e., HLD, LLD, IMP, RCR). Full Re-use: FSP, SPM.
AGD: Guidance doc	Full re-use.
ALC: Life cycle support	Full re-use.
ATE: Tests	ATE.FUN, IND, DPT: Test plan partial re-use according on HLD changes; New prototypes and Tests results. Full re-use: ATE.COV.
AVA: Vulnerability assessment	Full re-use: AVA.MSU, AVA.SOF. AVA.VLA: New update on IC dependencies.

1.7.3 Evaluation activities

The evaluator needs the ETR-lite of the platform PLT_2 and product $ProdA_1$ evaluations. The evaluator needs the following documents: Platform PLT_2 user's guidance, PLT2 ST-lite and PLT_2 Security User's Guidance.

Assurance Requirements	**Composite Smart card Evaluation Activities**	
	Application Dedicated Activities	**Composition Activities**
ASE: Security Target	Re-evaluation. Evaluator has to verify the claimed platform Security Functions of the composed ST_{ProdA2} are part of the PLT_2 platform ST-lite.	
ACM: Configuration management	Configuration list checking.	Integration of the OOS software in the IC manufacturer configuration management system.
ADO: Delivery and operation	None	Consistency check for delivery and pre-personalization procedures.
ADV: Development	Some work on the HLD, LLD, IMP, RCR analysis.	Compliance with the PLT_2 user guidance.
AGD: Guidance documents	None.	None
ALC: Life cycle support	None.	None
ATE: Tests	ATE.IND, DPT, FUN: New check on tests results on low layers. ATE.COV: no change.	Composite product functional testing.
AVA: Vulnerability assessment	Partly redone for IC dependencies	Composite product vulnerability analysis.

END OF THE DOCUMENT