Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, 5 mai 2015

N° 1817/ANSSI/SDE/PSS/CCN

Référence: ANSSI-CC-NOTE-17/1.0.EN

APPLICATION NOTE

ALC ASSURANCE CLASS RE-USE

Application : From date of publication.

Circulation : Public.

COURTESY TRANSLATION

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

Version history

Version	Date	Modifications
1.0	05/05/2015	Creation

Pursuant to amended decree No. 2002-535 of 18th April 2002, this application note has been submitted to the certification management committee, which gave a favourable opinion.

This application note is available at the ANSSI's institutional website (www.ssi.gouv.fr).

TABLE OF CONTENTS

1. Introduction

1.1. Subject of the note

This note outlines the process for re-using the evaluation results for components for the ALC assurance class of Common Criteria applied by the French scheme. In fact, independent elements of a TOE[1] but which are identical for a product category[2] and associated with a site visit may be re-used.

This note describes a mandatory methodology to be able to re-use generic results produced in the context of a product certification, a site certification or the optional mutualisation approach defined below.

This note is a complement to the Common Criteria and Note 02 quoted in the reference.

1.2. References

[CC] Common Criteria for Information Technology Security Evaluation, version 3.1, revision 4, September 2012. Part 2: Functional security components.

Common Criteria for Information Technology Security Evaluation, version 3.1, revision 4, September 2012. Part 3: Assurance security components.

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012.

[SITE_CER] Supporting Document, Site Certification, version 1.0, revision 1, October 2007, reference CCDB-2007-11-001, CCRA.

[AIS.38] Application Notes and Interpretation of the Scheme, AIS 38, version 2, 28 September 2007, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

[Note 02] Application note, Development environment visit, version 2.4, 5 January 2015, ANSSI.

1.3. Definitions

Generic evaluation — A generic evaluation denotes the analysis of the ALC class components identified by the term "Generic" in appendix A applied to a specific product category. This evaluation corresponds to a documentary analysis (analysis of the documentation common to all the sites in question and to a specific product category, called "generic documentation") and to the verification of the application of the generic documentation in the context of site visits (called "generic audits").

[1] TOE: *Target Of Evaluation*.

[2] For example: SIM cards, health cards, bank cards, each potentially with its own life cycle.

Specific evaluation	A specific evaluation denotes the analysis of the ALC class components identified by the term "Specific" in appendix A applied to a specific product. This evaluation corresponds to a documentary analysis only: analysis of documents showing the application of the generic documentation evaluated, work associated with the "Specific/Confirmation" tasks in appendix A; and analysis of the other tasks specific to the products evaluated, work associated with the "Specific/Documentary" tasks in appendix A.
Mutualisation	The term mutualisation refers to the multiple use of generic evaluation results for a type of technology considered independently of any product or site evaluation.

1.4. Scope

The ALC assurance class components cover different aspects of the inspection and the protection of the TOE from its creation to its delivery.

A given site may constitute the same development or production environment for different products to be certified of the same type. Therefore, the evaluation of the ALC assurance class components, when carried out independently for each product and by different ITSEFs may lead to redundancies. To enable developers to avoid carrying out unnecessary evaluation tasks, an approach to re-use ALC assurance class components evaluation results is defined here. It applies when the procedures, methods and tools are common to several products of the same category and described in the same documentation.

This ALC assurance class components re-use approach comprises two steps:

- A results production step: this applies to a set of products, corresponding to a specific product category, called generic evaluation;
- A results re-use step: this applies to a specific product to check that the generic documentation has been applied correctly when the product was manufactured, called specific evaluation.

In its first section, this note describes the conditions for producing a generic evaluation and the reports expected in order to re-use the results.

In its second section, the note presents the rules for re-using the results of the generic evaluation in the context of the evaluation of a specific TOE by an ITSEF which is not involved in the generic evaluation phase.

The categorisation of the ALC class evaluation tasks is provided in appendix A.

An example of the mutualisation principle is provided in appendix B.

The re-use report template is provided in appendix C.

This note may apply to all types of product, but it considers more specifically the hardware type products (microcontrollers and smart cards).

2. Generic evaluation

A generic evaluation is constructed in the context of the following processes:

- Site certification;
- Product certification;
- Mutualisation approach.

Paragraph 2.1 describes the principle for re-using generic results established via a site or product certification and paragraph 2.2 describes an alternative generic evaluation approach.

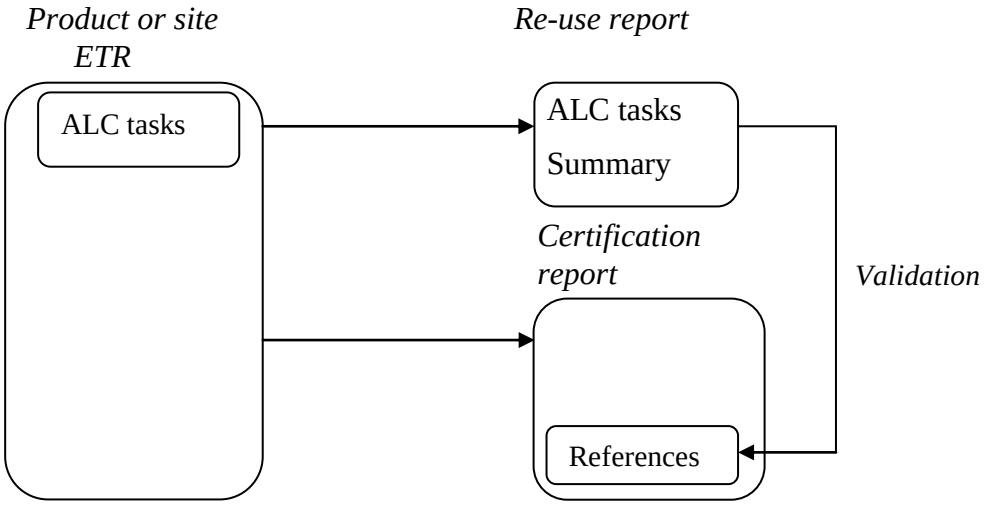
Information is transferred between ITSEFs via a re-use report, whose content is described in 2.3 and for which a template is available in appendix C.

2.1. Product or site evaluation

Following a site certification, in accordance with [SITE_CER], or a product certification, in accordance with [CC], the generic evaluation results may be re-used in the context of a product evaluation once a re-use report is available.

Before it is used, this report must have been validated by the certification body in charge of the site certification or product certification in question. To indicate this validation, the certification body may identify this re-use report in the site or product certification report in question.

The following diagram indicates the re-use of results in the context of a product or site evaluation.



2.2. Mutualisation process

This paragraph describes the optional mutualisation process.

Unlike the site or product evaluation:

- The mutualisation process enables the generic evaluation results to be re-used without being produced in the context of a certification process; the associated results must therefore be validated by the certification body independently of a certification project;
- Several ITSEFs may be involved in the production of generic evaluation results: an ITSEF may carry out the generic documentary evaluation and one or more other ITSEFs may carry out the associated generic site audits.

The diagram in appendix B illustrates this process.

2.2.1. Developer conditions related to mutualisation process

The developer must provide the following information:

- The description of a life cycle model[3] applied to the product category targeted by the developer to be re-used; this life cycle model may be refined by breaking down the technology type development and production phases into processes;
- The level of ALC assurance class components targeted by the developer;
- The generic documentation required by these class assurance components.

This information must be provided to all the ITSEFs involved in the generic evaluation work below.

2.2.2. Generic evaluation work related to mutualisation process

The ITSEF in charge of the generic documentary evaluation analyses the generic documentation provided by the developer in relation to the evaluation tasks identified by "Generic/Documentary" in appendix A. This analysis must cover all the options for the procedures considered by the developer or mention clearly, in the introduction to the report, the options which will not have been taken into account (for example, the case of procedures which identify several tools/approaches).

The results of this analysis are entered into a generic documentary report and a summary generic documentary report. This second report must correspond to extracts from the generic documentary report which are sufficient to carry out the specific evaluation.

These documentary reports are sent to the certification body and the developer before any audits and according to [NOTE 02] at least one month before the associated generic audits are carried out.

The ITSEFs in charge of the generic audits check:

- That the generic documentary report is relevant for carrying out the generic audit;
- And that the procedures evaluated under the generic documentary evaluation are actually applied in the context of site visits.

This work corresponds to the evaluation tasks identified by "Generic/Audit" in appendix A. To do so, these ITSEFs must at least have the summary generic documentary report.

After the site audits, the ITSEFs produce audit reports according to [NOTE 02]. Summary audit reports intended to be sent to other ITSEFs may also be produced. These second reports must

[3] The life cycle model is the description of the steps involved in an object's life cycle, their connections, their sequencing and their high level characteristics.

correspond to extracts from the generic documentary reports which are sufficient to carry out the specific evaluation.

All of the reports produced in the context of this process are circulated for validation to the certification body and to the developer at the same time.

2.3. Re-use report

The result re-use report provides all the elements from the generic evaluations necessary for carrying out a specific evaluation. It is intended to be shared with an ITSEF which is not involved in the generic evaluation process, but which is in charge of a specific evaluation for a product which falls into the same category as the product studied by the generic evaluation.

This document is made up of two sections:

- A documentary section corresponding at least to the summary results of the generic evaluation; this section specifies the list of evidence elements expected under the specific evaluation so that the developer can show that the generic document has been applied effectively;
- An audit section corresponding at least to the summary audit reports.

The report template is provided in appendix C.

The developer is tasked with providing the re-use report to the ITSEFs in charge of the specific product evaluation.

In the context of a report established under a product or site evaluation, the certification report may identify the re-use report. This identification counts as validation of the re-use report by the certification body.

In general, if the re-use report's validity is not identified in a public document, the certification body in charge of the specific evaluation checks its validity with the certification body involved in the generic evaluation.

The circulation list for the results re-use reports issued by an ITSEF is managed and updated by the developer with information to the report owner (the ITSEF) and the certification body associated with the generic evaluation.

<u>Specific feature of the re-use report produced in the context of the mutualisation process</u>

The audit section of the re-use report established under mutualisation process may develop over time and so be enhanced with new results following the different audits carried out by the ITSEFs.

The assembly of the re-use report for the evaluation of a specific product (this product's life cycle does not necessarily contain all of the audited sites, a sufficient sub-set may therefore be constituted) is fully managed by the developer.

The re-use report established under mutualisation process provides a status, if it is available, on the validation of the report by the certification body and clearly indicates which sections have been validated (documentary section, site audits, etc.).

3. Specific evaluation

The re-use of the results of a generic evaluation is only authorised if a re-use report is provided to the laboratory in charge of the specific evaluation.

The ITSEF responsible for the specific evaluation considers whether it has the necessary and sufficient elements for this specific evaluation for its analysis; if not, it immediately alerts its certification body.

The certification body may refuse the re-use at any time if it considers that the re-use proposed is not relevant (for example, because the specific evaluation drifts too much in relation to the generic evaluation).

3.1. Re-use rules

3.1.1. Developer conditions

The developer must provide the CESTI in charge of the specific evaluation with the following information:

- The identification of all the differences in relation to the generic life cycle model, which indicates all the changes for the product in question in the operations, the procedures or the generic documentation tools;
- All of the documentation specific to the product and necessary to process the specific evaluation's ALC tasks. In particular, it describes the product's actual life cycle and, where applicable, when several configurations have been considered in the generic document, specifies which ones are relevant for the product in question;
- All of the evidence elements which certify that the product has been developed/manufactured according to the generic procedures which were previously evaluated;
- The documentation evaluated in the context of the generic evaluation re-used;
- The re-use report.

3.1.2. Evaluator rules

The ITSEF in charge of the specific evaluation checks the following points:

- The product evaluated corresponds to the product category which was subject to generic evaluation an the necessary re-use reports have been provided to them;
- The availability of all of the necessary elements sufficient for the specific evaluation;
- The levels of the components processed during the generic evaluation are greater than or equal to the specific evaluation's levels;
- The generic evaluation results are valid (remember that this validity period is established in [NOTE 02] for the French scheme) and relevant;
- The results of the specific evaluation tasks have been entered:
    - The evidence elements certifying that the product has been developed/manufactured according to generic procedures which were evaluated previously are analysed under the evaluation tasks identified by "Specific/Confirmation" in appendix A; this analysis is carried out for each site involved in the application of the generic procedure in question;

- The specific documentation is analysed under the evaluation tasks identified by "Specific/Documentary" in appendix A.

In addition to the points above, the ITSEF references in its ALC report the re-use reports and the generic documentation used.

The ITSEF in charge of the specific evaluation is also charged with evaluating the difference between the life cycle of the product in question and the generic life cycle model:

- if these differences are ponctual, the ITSEF confirms the impact on the specific evaluation's components and, if necessary, re-evaluates these components from the evidence elements which were communicated to them;
- otherwise, the ITSEF alerts the certification body which will decide on the action to be taken.

As the specific evaluation is carried out in the context of a product evaluation, all of these results are entered into the ALC task report and in the ETR[4], according to [CC].

[4] Evaluation Technical Report

Annexe A Categories

The "Generic" category characterises the tasks which may be re-used between products of the same type and which must be carried out under a generic evaluation.

The "Specific" category characterises the tasks which must be carried out under the evaluation of a specific product of the same type as those analysed under the generic evaluation (see chapter 3).

This categorisation is compliant with the results established by the BSI in [AIS.38] and is provided here from evaluation level EAL3.

The ALC_FLR task may be processed generically; it is often associated with site audits (see [NOTE 02]).

The "comments" column specifies the nature of the work: "documentary" for the documentary analysis, "audit" for the site audits and "confirmation" when the ITSEF in charge of the specific evaluation needs to confirm the results of the generic documentary evaluation or site audits.

Component	Requirements	Evaluation task	Category	Comment
ALC_CMC.3				
	ALC_CMC.3.1C	ALC_CMC.3-1	SPECIFIC	Documentary
	ALC_CMC.3.1C	ALC_CMC.3-2	SPECIFIC	Documentary
	ALC_CMC.3.2C	ALC_CMC.3-3	GENERIC	Documentary
	ALC_CMC.3.3C	ALC_CMC.3-4	SPECIFIC	Documentary
	ALC_CMC.3.4C	ALC_CMC.3-5	GENERIC	Documentary
	ALC_CMC.3.5C	ALC_CMC.3-6	GENERIC	Documentary
	ALC_CMC.3.6C	ALC_CMC.3-7	GENERIC	Documentary
	ALC_CMC.3.7C	ALC_CMC.3-8	GENERIC	Documentary
	ALC_CMC.3.8C	ALC_CMC.3-9	GENERIC	Documentary
			SPECIFIC	Confirmation
	ALC_CMC.3.8C	ALC_CMC.3-10	GENERIC	Audit
			SPECIFIC	Confirmation
ALC_CMC.4				
	ALC_CMC.4.1C	ALC_CMC.4-1	SPECIFIC	Documentary
	ALC_CMC.4.1C	ALC_CMC.4-2	SPECIFIC	Documentary
	ALC_CMC.4.2C	ALC_CMC.4-3	GENERIC	Documentary
	ALC_CMC.4.3C	ALC_CMC.4-4	SPECIFIC	Documentary
	ALC_CMC.4.4C	ALC_CMC.4-5	GENERIC	Documentary
	ALC_CMC.4.5C	ALC_CMC.4-6	GENERIC	Documentary
	ALC_CMC.4.5C	ALC_CMC.4-7	GENERIC	Documentary
	ALC_CMC.4.6C	ALC_CMC.4-8	GENERIC	Documentary
	ALC_CMC.4.7C	ALC_CMC.4-9	GENERIC	Documentary
	ALC_CMC.4.8C	ALC_CMC.4-10	GENERIC	Documentary
	ALC_CMC.4.9C	ALC_CMC.4-11	GENERIC	Documentary
	ALC_CMC.4.10C	ALC_CMC.4-12	GENERIC	Documentary
			SPECIFIC	Confirmation

	ALC_CMC.4.10C	ALC_CMC.4-13	GENERIC	Audit
			SPECIFIC	Confirmation
ALC_CMC.5				
	ALC_CMC.5.1C	ALC_CMC.5-1	SPECIFIC	Documentary
	ALC_CMC.5.1C	ALC_CMC.5-2	SPECIFIC	Documentary
	ALC_CMC.5.2C	ALC_CMC.5-3	GENERIC	Documentary
	ALC_CMC.5.3C	ALC_CMC.5-4	GENERIC	Documentary
	ALC_CMC.5.4C	ALC_CMC.5-5	SPECIFIC	Documentary
	ALC_CMC.5.5C	ALC_CMC.5-6	GENERIC	Documentary
	ALC_CMC.5.6C	ALC_CMC.5-7	GENERIC	Documentary
	ALC_CMC.5.6C	ALC_CMC.5-8	GENERIC	Documentary
	ALC_CMC.5.7C	ALC_CMC.5-9	GENERIC	Documentary
			SPECIFIC	Confirmation
	ALC_CMC.5.8C	ALC_CMC.5-10	GENERIC	Documentary
	ALC_CMC.5.9C	ALC_CMC.5-11	GENERIC	Documentary
	ALC_CMC.5.10C	ALC_CMC.5-12	GENERIC	Documentary
	ALC_CMC.5.11C	ALC_CMC.5-13	GENERIC	Documentary
	ALC_CMC.5.12C	ALC_CMC.5-14	GENERIC	Documentary
	ALC_CMC.5.13C	ALC_CMC.5-15	GENERIC	Documentary
	ALC_CMC.5.14C	ALC_CMC.5-16	GENERIC	Documentary
	ALC_CMC.5.15C	ALC_CMC.5-17	GENERIC	Documentary
	ALC_CMC.5.16C	ALC_CMC.5-18	GENERIC	Documentary
			SPECIFIC	Confirmation
	ALC_CMC.5.16C	ALC_CMC.5-19	GENERIC	Audit
			SPECIFIC	Confirmation
	ALC_CMC.5.2E	ALC_CMC.5-20	GENERIC -	Audit
			SPECIFIC	Confirmation
ALC_CMS.4				
	ALC_CMS.4.1C	ALC_CMS.4-1	SPECIFIC	Documentary
	ALC_CMS.4.2C	ALC_CMS.4-2	SPECIFIC	Documentary
	ALC_CMS.4.3C	ALC_CMS.4.3	SPECIFIC	Documentary
ALC_CMS.5				
	ALC_CMS.5.1C	ALC_CMS.5-1	SPECIFIC	Documentary
	ALC_CMS.5.2C	ALC_CMS.5-2	SPECIFIC	Documentary
	ALC_CMS.5.3C	ALC_CMS.5-3	SPECIFIC	Documentary
ALC_DEL.1				
	ALC_DEL.1.1C	ALC_DEL.1-1	GENERIC	Documentary
			SPECIFIC	Documentary
	ALC_DEL.1.2D	ALC_DEL.1-2	GENERIC	Audit
ALC_DVS.1				
	ALC_DVS.1.1C	ALC_DVS.1-1	GENERIC	Documentary
	ALC_DVS.1.2C	ALC_DVS.1-2	GENERIC	Documentary
	ALC_DVS.1.2E	ALC_DVS.1-3	GENERIC	Audit
			SPECIFIC	Confirmation

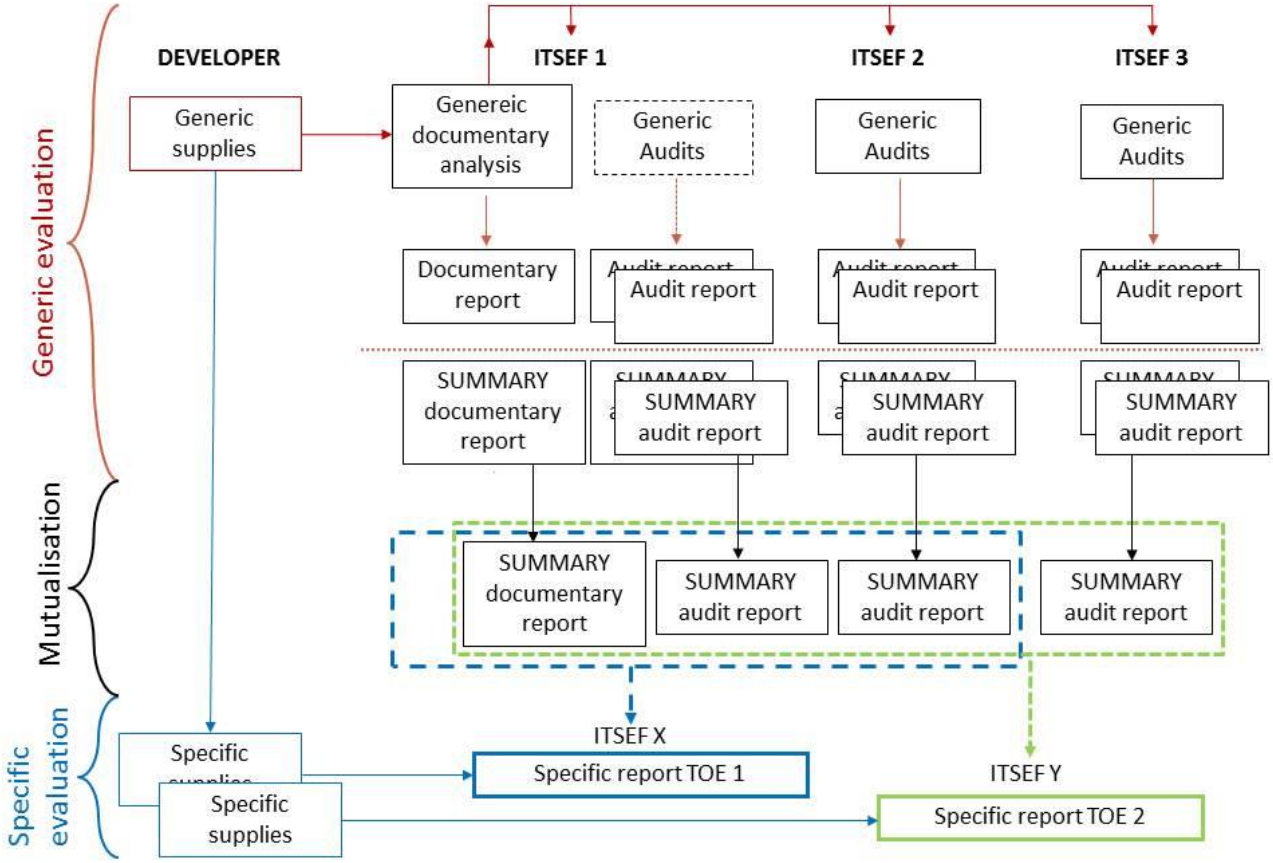
ALC_DVS.2				
	ALC_DVS.2.1C	ALC_DVS.2-1	GENERIC	Documentary
	ALC_DVS.2.2C	ALC_DVS.2-2	GENERIC	Documentary
	ALC_DVS.2.2C	ALC_DVS.2-3	GENERIC	Documentary
	ALC_DVS.2.2E	ALC_DVS.2-4	GENERIC -	Audit
			SPECIFIC	Confirmation
ALC_LCD.1				
	ALC_LCD.1.1C	ALC_LCD.1-1	GENERIC	Documentary
	ALC_LCD.1.2C	ALC_LCD.1-2	GENERIC	Documentary
ALC_LCD.2				
	ALC_LCD.2.1C	ALC_LCD.2-1	GENERIC	Documentary
			SPECIFIC	Confirmation
	ALC_LCD.2.2C	ALC_LCD.2-2	GENERIC	Confirmation
	ALC_LCD.2.3C	ALC_LCD.2-3	SPECIFIC	Confirmation
ALC_TAT.1				
	ALC_TAT.1.1C	ALC_TAT.1-1	GENERIC	Documentary
			SPECIFIC	Confirmation
	ALC_TAT.1.2C	ALC_TAT.1-2	GENERIC	Documentary
	ALC_TAT.1.3C	ALC_TAT.1-3	GENERIC	Documentary
ALC_TAT.2				
	ALC_TAT.2.1C	ALC_TAT.2-1	GENERIC	Documentary
			SPECIFIC	Confirmation
	ALC_TAT.2.2C	ALC_TAT.2-2	GENERIC	Documentary
	ALC_TAT.2.3C	ALC_TAT.2-3	GENERIC	Documentary
	ALC_TAT.2.2E	ALC_TAT.2-4	GENERIC	Audit
ALC_TAT.3				
	ALC_TAT.3.1C	ALC_TAT.3-1	GENERIC	Documentary
			SPECIFIC	Confirmation
	ALC_TAT.3.2C	ALC_TAT.3-2	GENERIC	Documentary
	ALC_TAT.3.3C	ALC_TAT.3-3	GENERIC	Documentary
	ALC_TAT.3.2E	ALC_TAT.3-4	GENERIC	Audit

Annexe B Mutualisation principle diagram

The figure below shows the mutualisation approach with three ITSEFs involved, one in charge of the generic documentation evaluation and potentially generic site audits and two which carry out one or more site audits.

During the specific evaluation, the developer chooses to re-use certain generic results thanks to the re-use report they provide to the ITSEFs in charge of the specific evaluation.

Mutualisation involves constituting the sufficient and necessary re-use report for the ITSEF in charge of the specific evaluation.



Annexe C Re-use report template

As indicated in paragraph 5.4, the re-use report contains two sections:

- The documentary section: this corresponds to the summary evaluation results for the generic documentary evaluation, whose template is provided below. These results must be sufficient for the generic site audits and the specific evaluations;
- The audit section, which corresponds to the necessary and sufficient summary audit reports for the ITSEF in charge of the evaluation of a specific product, the template for which is provided below.

Re-use report: documentary section must contain the following information at least:

1. Introduction
   a) Re-use report identification
   b) ITSEF name
   c) Certification body name
   d) Report date
   e) Reference to the CC and the methodology used
   f) Reference of the full report (generic report)
   g) Information about the previous analyses (if any exist). In particular the status of the remarks opened during the last analysis
   h) Status of the validation by the certification body if available
2. Description of the evaluation
   a) Description of the activities analysed and their environments
   b) List of the ALC assurance class work-units evaluated during the documentary analysis
   c) References of the generic documentation (policies and procedures) and list of tools (in particular, the configuration management system)
   d) List of evidence elements needed to confirm the evaluation results for a specific product
3. Results
   a) Results of the evaluation for each "Generic/Documentary" work-unit
   b) List of remarks (summary of the remark and non-conformity sheets) and their status

Re-use report: audit section must contain the following information at least:

1. Introduction
   a) Re-use report identification
   b) ITSEF name
   c) Certification body name
   d) Composition of the audit team (evaluators and certifiers)
   e) Name and address of the sites audited
   f) Dates of the site audits
   g) Identification of the people met during the site audits
   h) Reference to the CC and the methodology used

   i) Reference of the full report (generic report) in the case of the mutualisation process
   j) Information about the previous audits (if any exist) with the reference to their audit report, in particular the status of the remarks opened during the last audit
2) Description of the evaluation
   a) Description of the audited activities
   b) List of the ALC assurance class work-units evaluated during the site audit
   c) Reference to the re-use report (first documentary section which does not deal with the site audit results i.e. the summary generic documentary report)
   d) Reference to all of the developer's documentation (policies and procedures) and list of tools (in particular, the configuration management system)
3) Results
   a) Results of the evaluation for each "Generic/Audit" work-unit
   b) List of remarks and their status (comprising the status of the remarks from the last audit which were closed during this audit)