Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Paris, 25 March 2008

N° 587 /SGDN/DCSSI/SDR
Reference : NOTE/12.1

APPLICATION NOTE

TARGET OF EVALUATION'S SECURITY POLICIES FORMAL MODELLING

Application : From publication

Circulation : Public

Courtesy Translation

SÉCURITÉ CERTIFICATION

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

Modifications

Version	Date	Modifications
1.0	25/03/08	Initial version

TABLE OF CONTENT

1. PURPOSE OF THE APPLICATION NOTE 4

2. REFERENCES 4

3. ISSUE 4

3.1. Clarifications Regarding Terminology 4
3.2. Technical objectives of the SPM assurance component 5
3.3. Task Subjectivity 5

4. METHODOLOGY 6

4.1. Specific Evidence to be Supplied 6
4.2. Evaluation work 7

5. CONCLUSION 13

APPENDIX A SUMMARIES 14

TABLE OF ILLUSTRATIONS

Figure 1 Summary of the process 14
Figure 2 Elements supplied by the developer 15
Figure 3 Evaluations tasks according to [CC v2.3] 15

1. Purpose of the application note

The purpose of this note is to specify the role of the Security Policy Modelling task (SPM), included in the Common Criteria (CC), for a product in the framework of an evaluation.

This note applies to all current versions of the CC ([CC v2.3] and [CC v3.1]). In order to avoid any ambiguity, this task shall be referred to as SPM throughout this document, regardless of the CC version concerned (i.e. the term SPM shall refer to SPM.3 in [CC v2.3] and SPM.1 in [CCv3.1]).

2. References

- [CC v2.3]: Common Criteria Parts 1-2-3 and CEM; version 2.3; August 2005; ref.: CCMB-2005-08-001 to 004
- [CC v3.1]: Common Criteria Parts 1-2-3 and CEM; version 3.1; June 2006; ref.: CCMB-2006-06-001 to 004
- [AIS 34]: Evaluation Methodology for CC Assurance Classes for EAL5+; version 1.0; June 2004

3. Issue

This chapter firstly clarifies the various concepts relating to the SPM task introduced by the CC. The objectives of this task are then described, providing an overview of what it requires both of the developer and of the Information Technology Security Evaluation Facility (ITSEF), and of the value it can add to the development of a product.

3.1. Clarifications Regarding Terminology

The [CC v2.3] and the [AIS 34] describe a model in terms of two aspects, each offering two levels of representation:

- "*characteristics*" and "*rules*" (or "*principles*"),
- "*features*" and "*properties*".

As these concepts can sometimes cause confusion, their meaning in the context of the French scheme is clarified below:

- "*Features*" and "*properties*" correspond to the formal representation of a subset of "*characteristics*" and "*rules*" respectively.
- More specifically:
    - The "*characteristics*" of the TOE[1] refer to the TSF[2] (which implement the TOE's security policies as defined in the CC). The level of representation is that of the security target and they correspond to a subset of the SFR[3] of the security target in question. They therefore correspond to the behaviour of the TOE.
    - The "*features*" correspond to the formal representation of the "*characteristics*" that are modeled. They therefore correspond to part of the TOE's behaviour (i.e. the behaviour of the TOE which is effectively modeled).
    - The "*rules*" of the TOE represent the properties guaranteeing the TOE. At the level of the security target, they are described as the security objectives for the TOE.
    - The "*properties*" correspond to the formal representation of the subset of "*rules*" that are modeled. (NB: in [CC v3.1] they correspond to the preservation of a secure state. An

[1] Target Of Evaluation

[2] TOE Security Functions in [CC v2.3], TOE Security Functionality in [CC v3.1]

[3] Security Functional Requirement

unsecure state is therefore considered as derogating from the modeled security objectives for the TOE).

The [CC V3.1] no longer use all of these concepts. However, they shall be used throughout this document regardless of the CC version concerned in order to distinguish between the various levels of representation.

In addition, “formal model” shall mean all characteristics and formal properties (i.e. “*features*” + “*properties*”).

These terms shall be used as follows throughout this English version of the document:

Informal représentation	**Formal représentation**	**French Interpretation**
characteristics	*features*	*Formal or informal characteristics*
rules (principles)	*properties*	*Formal or informal properties*

Despite the correspondence between the terms described above, it should be noted that the level of granularity in the representation of each of these concepts can be very heterogeneous.

3.2. Technical objectives of the SPM assurance component

The “characteristics” part of the formal model represents the security functions described in the security target, with their security features as they will be implemented (level ADV_FSP: functional specifications, see chapter 4).

The aim here is to verify that the security objectives described in the security target (as formal properties) are covered by these security functions.

In other words, it must be formally demonstrated that the features satisfy the formal properties. The informal interpretation of this formal proof is that the security functions meet the security objectives.

3.3. Task Subjectivity

Certain criteria concerning SPM are subjective. For example:

> In the [CC v2.3] (§370), the modelling must *at the very least* represent the flow control and access control policies *if the state of the art so permits.*
>
> In [CC v3.1], no evaluation criteria enables the ITSEF to criticise the perimeter of what has been modelled (the ADV_SPM.1.1D assurance requirement has an open field enabling the developer to define the security policies he/she wishes to model, but no criteria enables the evaluator to criticise these parameters). The French scheme requires the ITSEF to carry out this analysis according to the same process as in [CC v2.3].

In order to address any potential issues resulting from this subjectivity, the certification body shall act as arbitrator between the ITSEF and the developer. The roles of the various actors in the evaluations are as follows:

- The ITSEF verifies the pertinence of the proposed model only with regard to the state of the art (from a “in the best of formal worlds” point of view).
- The certification body may relax the ITSEF’s verdict and conclude that a minimum acceptable level has been achieved. To do this, it may refer to previous models deemed acceptable in the framework of the French scheme. It can also take into account economic considerations (return on investment

generated by SPM and investment linked to the development of the product) if such considerations are combined with a commitment on the part of the developer to reinforce the process in future evaluations.

This aspect requires that the certification body be informed of any disagreement between the ITSEF and the developer at the earliest opportunity and that the corresponding report describing the ITSEF's view of the formal model supplied be delivered as soon as possible as it is likely to incur several changes[4].

4. Méthodology

This chapter specifies what the certification body expects with respect to this SPM evaluation task for the different current versions of the CC ([CC v2.3] and [CC v3.1]). It complements the [AIS34] and constitutes an extension of this methodology for the [CC v3.1].

Paragraph 4.1 sets forth all the evidence expected from the developer. The evaluation tasks are described in 4.2.. Figure 1 of Appendix A offers a summary of this process.

4.1. Specific Evidence to be Supplied

This paragraph sets forth the evidence specific to SPM (Figure 2 of Appendix A offers a summary of this evidence). The developer can organise the documents as he/she wishes.

The evidence expected for these tasks consists of:

- The source code of the formal model [SRC] (formal characteristics and properties) et the proof of this model [PROOF] (traces of the proof tool and/or all the proof carried out "by hand" by the developer);
- An explanatory document [ARG] for the model, explaining the formal model used by the developer, including:
  - Justification of the level of confidence associated with the method and tools used to carry out this task [ARG_TOOL];
  - Explanatory text [ARG] explaining the model used and the link between the different concepts applied in this model [ARG_SPM];
  - An argument [ARG_CDS] defending the link between the model and the security target (links between the features and characteristics as well as between the properties and rules). For [CC v3.1] evaluations, this argument must also specify the content of the ADV_SPM.1.1D requirement applied by the developer;
  - Presentation and justification (ARG_PROOF] of the "hypotheses"[5] (elements used in the proofs but which are not themselves proven), which may have been introduced into the model. This justification can be based on the security target (e.g. in the case of hypotheses concerning the security target or requirements of the TOE environment). This document must also show consistency between all the "hypotheses" used. In addition, [ARG_PROOF] must complement [ARG_SPM] by showing the implicit hypotheses resulting from the modelling choices applied;
  - The correspondence [ARG_FSP] between the model and the TOE specifications (the level of formality in which this connection is expressed is imposed by the evaluation criteria

[4] A preparatory meeting on the SPM analysis may be organised at the request of the evaluation sponsor in order to resolve these issues as soon as possible. Regardless of the CC version selected, the discussion is based on the security objectives of the TOE (rules) and the ITSEF and developer supply in advance a list of these objectives, which must be formally proven (i.e. identification of the properties; the features, which depend on the properties selected, are examined with the formal reports).

[5] This term does not refer to any formal method in particular and also includes any axioms (e.g. axiom of the excluded middle).

applied). For [CC v3.1] evaluations, this argument must also show the correspondence between the modeled interfaces and those identified in the functional specifications.

The developer must also make the tools used in the framework of SPM available[6] to the ITSEF if the latter does not have them at its disposal.

4.2. Evaluation work

The table below shows the work units associated with this assurance component for the [CC v2.3] and [CC v3.1](Figure 3 of Appendix A offers a summary of this work for the [CC v2.3]).

The evaluation criteria are presented in the grey boxes, as well as the work units which are either taken directly from the [AIS 34] for the [CC v2.3], or inspired by the [AIS 34] and adapted to the [CC v3.1]. The white boxes, which are sometimes shared by two CC versions, offer explanations with regard to these work units. Regardless of the CC version concerned, this table should be read in the light of the [AIS 34] (the correspondence between the concepts used in the various CC versions is provided in paragraph 3.1.).

<table>
<tr><th>CC v2.3 (AIS34)</th><th>CC v3.1</th></tr>
<tr><td>ADV_SPM.3.1E</td><td>ADV_SPM.1.1E</td></tr>
<tr><td colspan="2">The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.</td></tr>
<tr><td>ADV_SPM.3.1C The TSP model shall be formal.</td><td rowspan="2">ADV_SPM.1.1C The model shall be in a formal style, supported by explanatory text as required, and identify the security policies of the TSF that are modeled.</td></tr>
<tr><td>ADV_SPM.3.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.</td></tr>
<tr><td>ADV_SPM.3-1 The evaluator shall examine the TOE security policy model to determine that it is written in a formal style.</td><td>ADV_SPM.1-1 The evaluator shall examine the TOE security policies model to determine that it is written in a formal style.</td></tr>
<tr><td colspan="2">This work unit consists in verifying the theoretical bases of the method in order to ensure that they are well-founded.
The evaluator must identify the formal method and tools used by the developer, with the aim of gathering all the relevant scientific documentation in the context of the evaluation (on the basis of [ARG_TOOL] and additional references).
The documentary research on these methods and tools should facilitate the identification of “pitfalls” in the method or tool[7]: gathering of elements relating to the method and tool that could, for example, allow for the introduction of paradoxes.</td></tr>
<tr><td>ADV_SPM.3-2 The evaluator shall examine the TOE security policy model to determine that it contains all necessary informal explanatory text.</td><td>ADV_SPM.1-2 The evaluator shall examine the TOE security policies model description to determine that it contains all necessary explanatory text.</td></tr>
</table>

[6] Making the tools available should be understood in a broad sense: it could mean the lending of a licence, granting on-site access to the tools under terms compliant with the requirements of the evaluation, etc.

[7] See, for e.g., the DCSSI note on “pitfalls” in formal methods and tools: “Observations concerning the use of (deductive) formal methods in information systems security”.

<table>
<tr><th>CC v2.3 (AIS34)</th><th>CC v3.1</th></tr>
<tr><td colspan="2">This work unit consists in verifying the pertinence and adequacy of the explanatory document for the model [ARG_SPM].

Comments included directly in the source code of the model [SRC] can also help to understand the model, but they do not exclude provision of the document itself [ARG_SPM].</td></tr>
<tr><td>ADV_SPM.3-3 The evaluator shall check the TOE security policy model to determine that all security policies that are explicitly included in the ST are modeled.

ADV_SPM.3-4 The evaluator shall examine the TOE security policy model to determine that all security policies represented by the security functional requirements claimed in the ST are modeled.</td><td>ADV_SPM.1-3 The evaluator shall examine the TOE security policies model to determine that all security policies listed in the ADV_SPM SAR in the ST are modeled.</td></tr>
<tr><td>Subjectivity is introduced in the case where the minimal modelling required by he CC is not clearly established.

The certification body can arbitrate between the ideal modelling (such as established by the evaluator, taking into account the state of the art of the techniques implemented) and the model supplied by the developer, according to the state of the art of evaluations under the French scheme, as well as that of other schemes.</td><td>The notion of critical examination by the evaluator of the modelling parameters used by the developer is no longer included in this version of the evaluation criteria.

This concept is nonetheless maintained in the framework of the French scheme so that the evaluator can provide his/her opinion.

The same rule as that described opposite is therefore applied. The evaluator thus judges the evaluation parameters used by the developer in respect of ADV_SPM.1.1D.

In addition, if the certification body finds that the model provided does not correspond to the state of the art of evaluations already completed, it will fails this work unit.</td></tr>
<tr><td colspan="2">This work unit consists in analysing the pertinence of the [ARG_CDS] justification supplied by the developer with regard to the modelling parameters used.

To these ends, and although this does not seem to be required by the wording of the work unit, the evaluator provides the ideal list of properties to be modeled, which he/she then compares to those which have been effectively modeled. The developer must then justify the formal parameter used so that the certification body may reach a decision.

The same work must be carried out for the characteristics, which must of course be linked to formal properties (the evaluator will refer to his/her “ideal” list).</td></tr>
<tr><td>ADV_SPM.3-5 The evaluator shall examine the rules and characteristics of the security policies to determine that the modeled security behaviour of the TOE is clearly articulated.</td><td>ADV_SPM.1-4 The evaluator shall examine the rules and characteristics of the security policies to determine that the modeled security behaviour of the TOE is clearly articulated.</td></tr>
</table>

<table>
<tr><th>CC v2.3 (AIS34)</th><th>CC v3.1</th></tr>
<tr><td colspan="2">The explanatory document for the model must establish the correspondence between the formal and informal concepts ([ARG_CDS]).
As the levels of detail in the formal and informal concepts are by nature very different, the evaluator’s critical examination of this correspondence is also required here. In effect, an informal characteristic can be described from a much more macroscopic point of view than its formal counterparts, which must be represented at a sufficiently pertinent level to enable the identification of the security mechanisms which will be effectively implemented and demonstrate their ability to cover the security need.
The subjectivity of this work unit may again require the intervention of the certification body in order to establish the final verdict.
The explanatory document for the model ([ARG_CDS]) must also describe and justify the scope of the model (justification of all “hypotheses” implemented by the model; e.g. it is acceptable to introduce “hypotheses” which correspond to security objectives concerning the environment).</td></tr>
<tr><td>ADV_SPM.3.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.</td><td>ADV_SPM.1.2C For all policies that are modeled, the model shall define security for the TOE and provide a formal proof that the TOE cannot reach a state that is not secure</td></tr>
<tr><td>ADV_SPM.3-6 The evaluator shall examine the TOE security policy model <s>rationale</s> to determine that it formally proves the correspondence between the security properties and the security features.</td><td>ADV_SPM.1-5 The evaluator shall examine the TOE security policies model to determine that it formally proves that the behaviour modeled cannot reach a state that is not secure</td></tr>
<tr><td>Formal proof that the features correspond to the properties.</td><td>Formal proof that an unsecure state has not been reached.
(Reminder: An unsecure state is a state which does not fulfil the security objectives).</td></tr>
<tr><td colspan="2">This work unit consists in verifying the pertinence of the elements identified in [ARG_PROOF] as well as the completeness of this document, then in verifying the proof [PROOF] derived from the model source code [SRC].
The evaluator must manually test the proof developed using the tools supplied by the developer, by checking all the paper proofs provided.
The evaluator must examine these proofs with regard to the information he/she previously gathered in respect of ADV_SPM.3-1 in [CC v2.3] or ADV_SPM.1-1 in [CC v3.1] concerning the method and tool used, as well as concerning the model (verification that the proof is complete, verification of the pertinence of the “hypotheses” introduced by the developer, etc.).</td></tr>
<tr><td>ADV_SPM.3-7 The evaluator shall examine the TOE security policy model rationale to determine that it proves the internal consistency of the TOE security policy model.</td><td>ADV_SPM.1-6 The evaluator shall examine the TOE security policies model rationale to determine that it proves the internal consistency of the TOE security policies model.</td></tr>
<tr><td colspan="2">The evaluator verifies the consistency between the model’s “hypotheses” based on the justification provided by the developer in [ARG_PROOF].</td></tr>
</table>

CC v2.3 (AIS34)	**CC v3.1**
ADV_SPM.3-8 The evaluator shall examine the TOE security policy model rationale to determine that the behaviour modeled is consistent with respect to policies described by the security policies (as articulated by the functional requirements in the ST).	*ADV_SPM.1-7 The evaluator shall examine the TOE security policies model to determine that the behaviour modeled (e.g. the features) is consistent with respect to policies described by the security policies (as articulated by the functional requirements in the ST).*
This work unit consists in analysing the model's consistency with all security policies of the TOE described in the security target, including those not modeled. As the model does not represent the entire security target, this task will return the verdict "Failure" if the evaluator identifies SFR not modeled which are inconsistent with the modeled behaviour.	
ADV_SPM.3-9 The evaluator shall examine the TOE security policy model rationale to determine that the behaviour modeled is complete with respect to the policies described by the security policies (i.e. as articulated by the functional requirements in the ST).	*ADV_SPM.1-8 The evaluator shall examine the TOE security policies model rationale to determine that the behaviour modeled (e.g. the features) is complete with respect to the policies described by the security policies (i.e. as articulated by the functional requirements in the ST).*
The evaluator verifies that the model corresponds to the SFR representing the SFP using [ARG_CDS]. Failure if the evaluator identifies SFR which should have been modeled but which are not.	
ADV_SPM.3.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.	**ADV_SPM.1.4C** The correspondence shall show that the functional specification is consistent and complete with respect to the model.
ADV_SPM.3-10 The evaluator shall examine the functional specification correspondence demonstration of the TOE security policy model to determine that it identifies all security functions described in the functional specification that implement a portion of the policy.	*ADV_SPM.1-10 The evaluator shall examine the functional specification correspondence demonstration of the TOE security policies model to determine that it is complete*
The evaluator verifies the correspondence between features and FSP using [ARG_FSP] and [SRC]. This work unit notably consists in verifying that [ARG–FSP] identifies all the security functions fully or partially corresponding to features.	
ADV_SPM.3-11 The evaluator shall examine the functional specification correspondence demonstration of the TOE security policy model to determine that the descriptions of the functions identified as implementing the TSP model are consistent with the descriptions in the functional specification.	*ADV_SPM.1-11 The evaluator shall examine the functional specification correspondence demonstration of the TOE security policies model to determine that the descriptions of the functions identified as implementing the TSP model are consistent with the descriptions in the functional specification*

<table>
<tr><th>CC v2.3 (AIS34)</th><th>CC v3.1</th></tr>
<tr><td colspan="2">This work unit consists in verifying that the description of the security functions listed in ADV_SPM.3.10 in [CC v2.3] or ADV_SPM.1.10 in [CC v3.1] is consistent with the description of these same functions in the functional specifications; notably, verification that all restrictions stated in the representation of the features are also described in the FSP documentation.</td></tr>
<tr><td>ADV_SPM.3.5C Where the functional specification is semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal.</td><td rowspan="2">ADV_SPM.1.3C The correspondence between the model and the functional specification shall be at the correct level of formality.</td></tr>
<tr><td>ADV_SPM.3.6C Where the functional specification is formal, the proof of correspondence between the TSP model and the functional specification shall be formal.</td></tr>
<tr><td>ADV_SPM.3-12 The evaluator shall examine the functional specification correspondence demonstration of the TOE security policy model to determine that it is presented in a semiformal style.</td><td rowspan="2">ADV_SPM.1-9 The evaluator shall examine the functional specification correspondence demonstration of the TOE security policies model to determine that it is presented be at the correct level of formality, and that it is correct</td></tr>
<tr><td>ADV_SPM.3-13 The evaluator shall examine the functional specification correspondence demonstration of the TOE security policy model to determine that it is in a formal style.</td></tr>
<tr><td>If FSP.4 is applied, this correspondence must be formal.
If FSP.3 is applied, this correspondence must be semiformal.</td><td>If FSP.6 is applied, this correspondence must be formal for the formal parts of FSP, and semiformal for the semiformal parts of FSP.
If FSP.5 is applied, this correspondence must be semiformal.
Otherwise, there is no restriction with regard to formality.</td></tr>
<tr><td colspan="2">If the specifications are supplied in a formal style, the proofs supplied by the developer must be tested by the evaluator by implementing the elements gathered in ADV_SPM.3-1 in [CC v2.3] or ADV_SPM.1-1 in [CC v3.1].
If the specifications are not formal, systematic verification of the elements of proof is required.</td></tr>
<tr><td></td><td>ADV_SPM.1.5C The demonstration of correspondence shall show that the interfaces in the functional specification are consistent and complete with respect to the policies in the ADV_SPM.1.1D assignment.</td></tr>
</table>

CC v2.3 (AIS34)	**CC v3.1**
	ADV_SPM.1-12 The evaluator shall examine the functional specification correspondence demonstration of the TOE security policies model to determine that the interfaces described in the functional specification are consistent with the behaviour modeled (e.g. the features)
	The evaluator verifies that there is no inconsistency between the external interfaces of the features and those of the functional specifications (notably that the model not include any external interface not described in the functional specifications). The evaluator also verifies that the external interfaces of the functional specifications are sufficiently detailed with respect to the features.

5. Conclusion

This assurance component and associated procedure provides formal verification that security functions specified by the SFR are sufficient to cover the security needs expressed in the security target, plus the detection of any inconsistencies. We therefore conduct a formal proof for a part of the security target deemed pertinent and show, from a mathematical point of view, that the modeled part of the TSF can indeed assure the modeled security properties stated in the security target.

This assurance component also offers:

- a modelling of the security principles underlying the construction of the security target and chosen security functionalities;
- a more precise description of the process applied to construct the security of the product;
- establishment of a mathematical model and an interpretation consistent with the TSF, thereby contributing to a better understanding of the latter.

Hence, this task makes it possible to reinforce confidence in the fact that the product effectively meets certain of its security objectives and does not contain any inconsistencies.

Appendix A Summaries

The following diagrams offer a summary view of the content of this note.

The first diagram below presents the transitions between the various stages identified in this note. The level of formality between these various stages is symbolised by the thickness of the arrows: transitions represented by double arrows represent formal work, while single and broken arrows represent informal work.

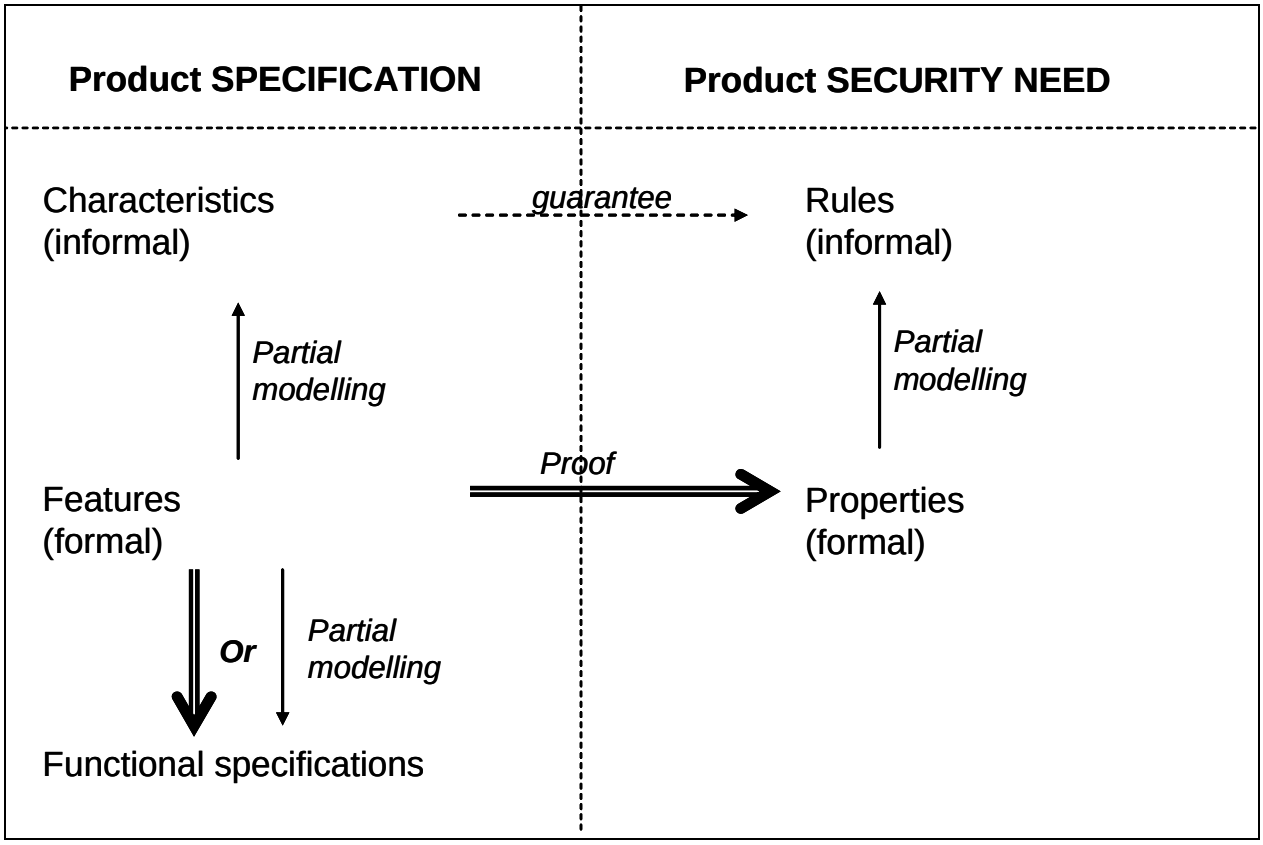

Figure 1 Summary of the process

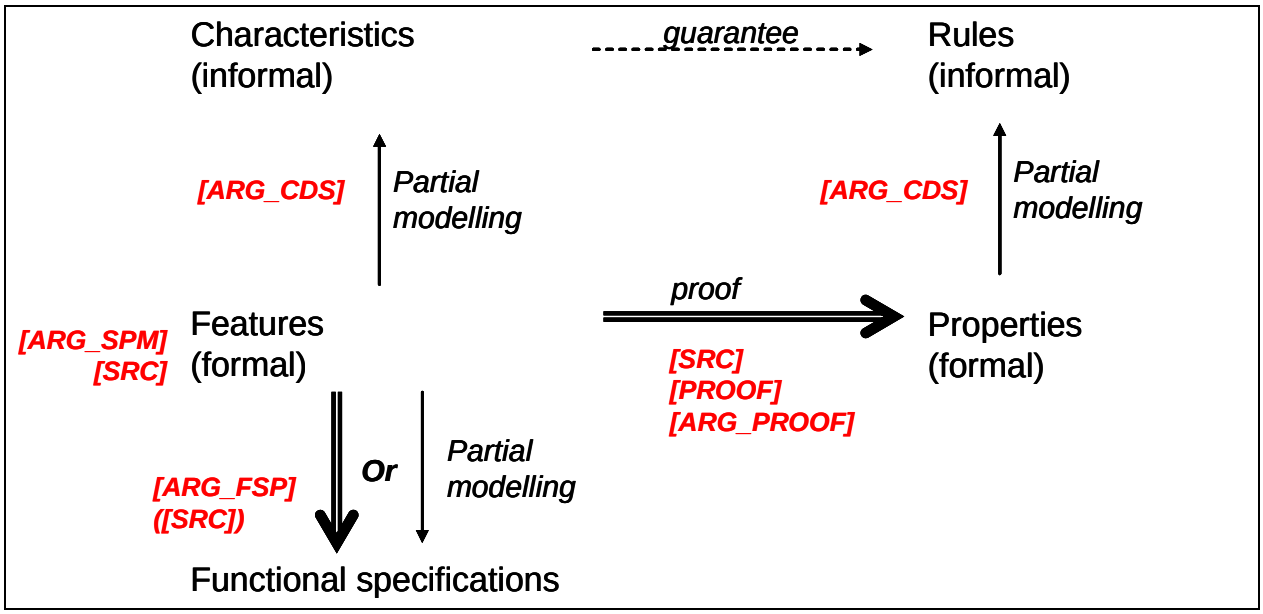

Figure 2 Elements supplied by the developer

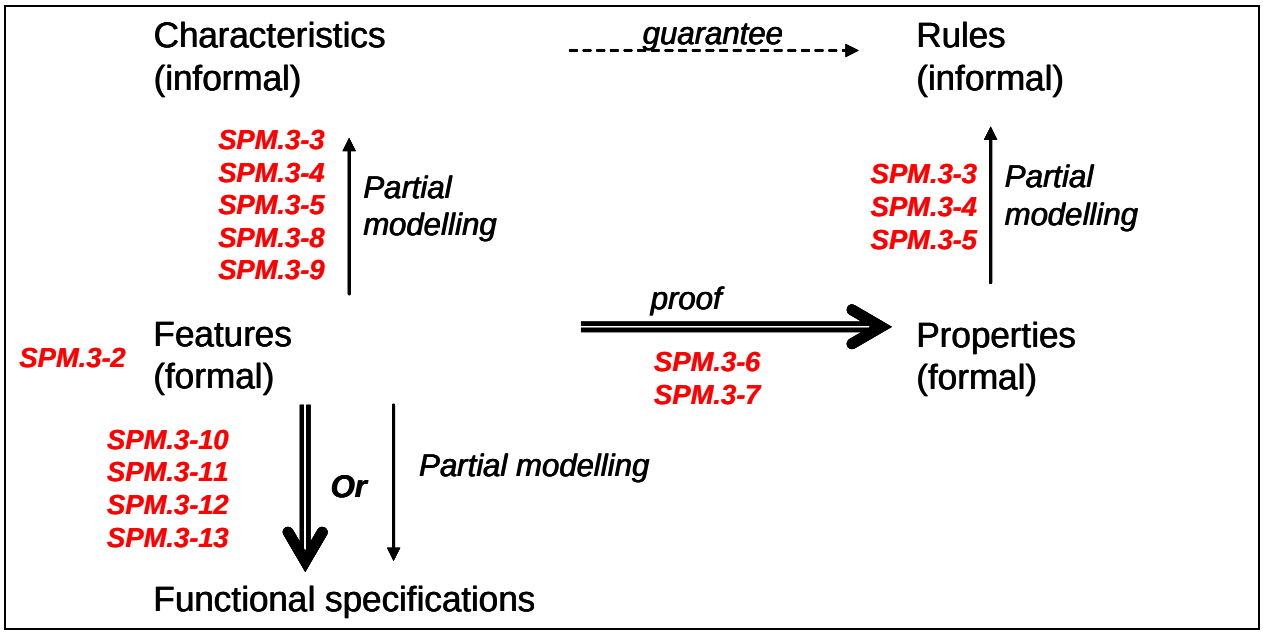

Figure 3 Evaluations tasks according to [CC v2.3]