Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Paris, le 25 mars 2008,

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

NOTE D'APPLICATION

MODELISATION FORMELLE DES POLITIQUES DE SECURITE D'UNE CIBLE D'EVALUATION

Application : A compter de la publication

Diffusion : Publique

Vérifiée par	Validée par le sous-directeur de la régulation	Approuvée par le directeur central de la sécurité des systèmes d'information
Le responsable qualité [ORIGINAL SIGNE] *Le chef du centre de certification* [ORIGINAL SIGNE]	[ORIGINAL SIGNE]	[ORIGINAL SIGNE]

Suivi des modifications

Révision	Date	Modifications
1.0	25/03/08	Version initiale

TABLE DES MATIERES

TABLE DES ILLUSTRATIONS

1. Objet de la note

L'objet de la présente note est de préciser le rôle de la tâche, prévue par les critères communs (CC), de modélisation formelle des politiques de sécurité (SPM[1]) d'un produit dans le cadre d'une évaluation.

Cette note s'applique à toutes les versions courantes des CC ([CC v2.3] et [CC v3.1]). Pour éviter toute ambiguïté, cette tâche sera désignée par SPM dans le reste du document quelle que soit la version des CC considérée (i.e. le terme SPM désignera SPM.3 en [CC v2.3] et SPM.1 en [CC v3.1]).

2. Références

- [CC v2.3] : Critères Communs Parties 1-2-3 et CEM ; version 2.3 ; août 2005 ; réf. : CCMB-2005-08-001 à 004
- [CC v3.1] : Critères Communs Parties 1-2-3 et CEM ; version 3.1 ; juin 2006 ; réf. : CCMB-2006-06-001 à 004
- [AIS 34] : Evaluation Methodology for CC Assurance Classes for EAL5+ ; version 1.0 ; juin 2004

3. Problématique

Ce chapitre précise tout d'abord les diverses notions relatives à la tâche SPM introduites par les CC. Ensuite, les objectifs de cette tâche sont décrits pour offrir une vue globale sur les attendus de cette tâche tant de la part du développeur que du Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI), et sur la plus-value qu'elle peut apporter au développement d'un produit.

3.1. Précisions sur la terminologie

Les [CC v2.3] et l'[AIS 34] décrivent un modèle en distinguant deux aspects, chacun d'eux étant décliné à deux niveaux de représentation :

- les « *characteristics* » et les « *rules* » (ou « *principles* »),
- les « *features* » et les « *properties* ».

Ces notions étant parfois obscures, leur interprétation dans le cadre du schéma français est précisée ici :

- Les « *features* » et « *properties* » correspondent respectivement à la représentation formelle d'un sous-ensemble des « *characteristics* » et des « *rules* ».
- Plus précisément :
    - Les « *characteristics* » de la TOE[2] désignent la TSF[3] (qui réalise les politiques de sécurité de la TOE d'après la définition CC). Leur niveau de représentation est celui de la cible de sécurité, elles correspondent à un sous-ensemble des SFR[4] de la cible de sécurité étudiée. Elles correspondent donc au comportement de la TOE.
    - Les « *features* » correspondent à la représentation formelle des « *characteristics* » qui sont modélisés. Elles correspondent donc à une partie du comportement de la TOE (i.e. le comportement de la TOE qui est effectivement modélisé).
    - Les « *rules* » de la TOE représentent les propriétés que doit permettre de garantir la TOE. Elles sont décrites, au niveau de la cible de sécurité, par les objectifs de sécurité de la TOE.

[1] Security Policy Modelling

[2] Target Of Evaluation

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

[4] Security Functional Requirement

- Les « *properties* » correspondent à la représentation formelle du sous-ensemble des « *rules* » qui sont modélisées. (NB : [CC v3.1], elles correspondent à la préservation d'un état sûr, un état non sûr étant alors considéré comme dérogeant aux objectifs de sécurité modélisés de la TOE).

Les [CC v3.1] n'utilisent plus toutes ces notions, mais celles-ci ayant été ici clarifiées, elles sont toujours employées dans le reste du document quelle que soit la version des CC considérée pour permettre la distinction entre les différents niveaux de représentation.

Par ailleurs, on désigne par « modèle formel » l'ensemble des caractéristiques et propriétés formelles (i.e. « *features* » + « *properties* »).

Les termes plus explicites suivants sont employés dans la suite de ce document :

Représentation informelle	**Représentation formelle**	**Interprétation française**
characteristics	*features*	*caractéristiques (informelles ou formelles selon le cas)*
rules (principles)	*properties*	*propriétés (informelles ou formelles selon le cas)*

Il doit être noté que, malgré la correspondance établie ci-dessus, le niveau de granularité de la représentation de chacune de ces notions peut être très hétérogène.

3.2. Objectifs techniques du composant d'assurance SPM

La partie « caractéristiques » du modèle formel représente les fonctions de sécurité, décrites dans la cible de sécurité, avec leurs caractéristiques de sécurité telles qu'elles seront implémentées (niveau ADV_FSP : spécifications fonctionnelles, voir le chapitre 4).

On s'attache ici à vérifier que les objectifs de sécurité exprimés dans la cible de sécurité (comme propriétés formelles) sont couverts par ces fonctions de sécurité.

En termes plus précis, il s'agit de démontrer formellement que les caractéristiques formelles satisfont les propriétés formelles. L'interprétation informelle de cette preuve formelle est que les fonctions de sécurité remplissent les objectifs de sécurité.

3.3. Subjectivité de la tâche

Certains critères relatifs à SPM ont un caractère subjectif. Par exemple :

> Dans les [CC v2.3] (§370), la modélisation doit représenter *au minimum* les politiques de contrôle de flux et de contrôle d'accès *si l'état de l'art le permet*.
>
> En [CC v3.1], aucun critère d'évaluation ne permet au CESTI de critiquer le périmètre de ce qui a été modélisé (l'exigence d'assurance ADV_SPM.1.1D dispose d'un champ libre permettant au développeur de définir les politiques de sécurité qu'il souhaite modéliser, mais aucun critère ne permet à l'évaluateur de critiquer ce périmètre). Le schéma français impose que le CESTI fasse cette analyse selon la même démarche qu'en [CC v2.3].

Pour régler les éventuels problèmes dus à cette subjectivité, le centre de certification assurera l'arbitrage entre le CESTI et le développeur. Le rôle des différents acteurs de l'évaluation est le suivant :

- Le CESTI vérifiera la pertinence du modèle proposé uniquement au regard de l'état de l'art (point de vue « dans le meilleur des mondes formels »).
- Le centre de certification peut être amené à alléger des verdicts du CESTI et à conclure qu'un niveau minimum acceptable est atteint. Il peut pour ce faire se référer aux précédents modèles jugés acceptables dans le cadre du schéma français. Il pourrait également prendre en compte des arguments économiques (rapport investissement induit par SPM et investissement lié au développement du produit) s'ils sont associés à un engagement du développeur à renforcer la démarche dans les évaluations suivantes.

  Cette particularité impose que le centre de certification soit averti au plus vite du différend entre CESTI et développeur, et donc que le rapport correspondant, qui décrit la perception du CESTI vis-à-vis du modèle formel fourni, soit livré au plus tôt, celui-ci étant voué à subir plusieurs itérations[5].

4. Méthodologie

Ce chapitre précise ce que le centre de certification attend au titre de cette tâche d'évaluation SPM pour les différentes versions courantes des CC ([CC v2.3] et [CC v3.1]). Il constitue un complément à l'[AIS34] et une extension de cette méthodologie pour les [CC v3.1].

L'ensemble des fournitures attendues de la part du développeur est décrit en 4.1, les tâches d'évaluation sont décrites en 4.2. La figure 1 de l'annexe A fournit la synthèse de cette démarche.

4.1. Fournitures spécifiques

Ce paragraphe identifie les fournitures spécifiques à SPM (la figure 2 de l'annexe A fournit une synthèse de ces fournitures). Le développeur peut proposer une organisation documentaire qui lui convient.

Les fournitures attendues au titre de cette tâche sont :

- le code source du modèle formel [SRC] (caractéristiques et propriétés formelles) et la preuve du modèle [PROOF] (les traces issues de l'outil de preuve et/ou l'ensemble des preuves réalisées « à la main »[6] par le développeur) ;
- un document d'interprétation [ARG] du modèle expliquant le modèle formel retenu par le développeur, comportant :
  - la justification du niveau de la confiance associée à la méthode et aux outils retenus pour réaliser cette tâche [ARG_TOOL] ;
  - un texte explicatif du modèle retenu et du lien entre les différentes notions manipulées dans ce modèle [ARG_SPM] ;
  - un argumentaire [ARG_CDS] sur le lien entre le modèle et la cible de sécurité (correspondance entre caractéristiques formelles et informelles, ainsi qu'entre propriétés formelles et informelles). Pour les évaluations en [CC v3.1], cet argumentaire devra également préciser le contenu de l'exigence ADV_SPM.1.1D retenue par le développeur ;

[5] Une réunion préparatoire à l'analyse SPM pourra être organisée, à la demande du commanditaire de l'évaluation, afin de résoudre ces problèmes au plus tôt. Quelle que soit la version des CC retenue, la discussion s'engagera sur la base des objectifs de sécurité de la TOE (les *rules*), CESTI et développeur ayant préalablement fourni la liste de ces objectifs qui doivent être formellement prouvés (i.e. identification des *properties* ; les *features*, qui dépendent des *properties* retenues, seront eux étudiés avec les rapports formels).

[6] Lorsque la méthode est limitée en expressivité ou en complétude (prouvabilité), des preuves manuelles sont tolérées, mais doivent être justifiées. L'emploi de méthodes peu expressives ou non reconnues s'accompagne cependant de contraintes sur l'évaluation de la méthode et d'une réduction du niveau de confiance, qui implique un risque d'échec ou de surcoût de cette tâche.

- la présentation et la justification [ARG_PROOF] des « hypothèses »[7] (éléments utilisés dans les preuves mais qui ne sont pas eux-mêmes prouvés) qui peuvent avoir été introduites dans le modèle. Cette justification peut s'appuyer sur la cible de sécurité (par exemple, s'il s'agit d'hypothèses de la cible de sécurité ou d'exigences sur l'environnement de la TOE). Ce document devra également montrer que l'ensemble des « hypothèses » retenues n'est pas incohérent. [ARG_PROOF] doit de plus compléter [ARG_SPM] en mettant en évidence les hypothèses implicites résultant des choix de modélisation ;
- la correspondance [ARG_FSP] entre le modèle et les spécifications de la TOE (le formalisme dans lequel est exprimée cette correspondance est imposé par les critères d'évaluation retenus). Pour les évaluations en [CC v3.1], cet argumentaire devra également montrer la correspondance entre les interfaces modélisées et celles identifiées dans les spécifications fonctionnelles.

Le développeur devra également mettre les outils utilisés dans le cadre de SPM à disposition[8] du CESTI si ce dernier n'en dispose pas.

4.2. Travaux d'évaluation

Le tableau ci-dessous identifie les unités de travail associées à ce composant d'assurance pour les [CC v2.3] et [CC v3.1] (la figure 3 de l'annexe A fournit une synthèse de ces travaux pour les [CC v2.3]).

Les critères d'évaluation sont présentés dans les cases grisées, ainsi que les unités de travail qui sont soit directement issues de l'[AIS 34] pour les [CC v2.3], soit inspirées de l'[AIS 34] et adaptées aux [CC v3.1]. Les cases blanches, qui sont parfois mutualisées entre ces deux versions des CC, apportent des précisions sur ces unités de travail. Quelle que soit la version des CC considérée, ce tableau doit être lu en regard de l'[AIS 34] (la correspondance entre les notions manipulées par les différentes versions des CC étant fournie au paragraphe 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>
</table>

[7] Ce terme ne se réfère à aucune méthode formelle particulière et comprend également les éventuels axiomes (exemple, axiome du tiers exclu).

[8] Mise à disposition s'entend ici au sens large : elle pourrait correspondre à un prêt de licence, à un accès aux outils sur site dans des conditions satisfaisant les exigences de l'évaluation, …

CC v2.3 (AIS34)	**CC v3.1**
Cette unité de travail consiste à vérifier les fondements théoriques de la méthode pour s'assurer qu'ils sont bien établis. L'évaluateur devra ici identifier la méthode formelle et les outils mis en œuvre par le développeur, dans le but de rassembler la documentation scientifique pertinente dans le contexte de l'évaluation (sur la base de [ARG_TOOL] et de références complémentaires). La recherche de documentation sur ces méthodes et outils doit faciliter l'identification des « pièges » de la méthode ou de l'outil[9] : rassemblement des éléments relatifs à la méthode et à l'outil qui permettraient par exemple d'introduire des paradoxes.	
ADV_SPM.3-2 The evaluator shall examine the TOE security policy model to determine that it contains all necessary informal explanatory text.	*ADV_SPM.1-2 The evaluator shall examine the TOE security policies model description to determine that it contains all necessary explanatory text.*
Cette unité de travail consiste à vérifier la pertinence et la suffisance du document d'interprétation du modèle [ARG_SPM]. Des commentaires introduits directement dans le source du modèle [SRC] peuvent aussi aider à la compréhension du modèle, mais ils n'excluent pas la fourniture du document [ARG_SPM].	
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.*	*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.*
Une subjectivité est introduite ici : la modélisation minimale requise par les CC n'est pas clairement établie. Le centre de certification peut faire l'arbitrage entre la modélisation idéale (telle qu'établie par l'évaluateur, en prenant en compte l'état de l'art des techniques mises en œuvre) et le modèle fourni par le développeur en fonction de l'état de l'art des évaluations du schéma français, ainsi que celui des autres schémas.	La notion d'examen critique par l'évaluateur du périmètre de modélisation retenu par le développeur n'est plus présente dans cette version des critères d'évaluation. Cette notion est néanmoins conservée dans le cadre du schéma français afin que l'évaluateur puisse fournir son opinion. La même règle que celle établie ci-contre est alors appliquée. L'évaluateur se prononcera donc ici sur le périmètre d'évaluation retenu par le développeur au titre de ADV_SPM.1.1D. De plus, si le centre de certification constate que le modèle fourni n'est pas au niveau de l'état de l'art des évaluations déjà réalisées, il mettra cette unité de travail en échec.

[9] Voir, entre autres, la note DCSSI relative aux « pièges » des méthodes et outils formels : « Remarques relatives à l'emploi des méthodes formelles (déductives) en sécurité des systèmes d'information ».

CC v2.3 (AIS34)	**CC v3.1**
Cette unité de travail consiste à analyser la pertinence de la justification [ARG_CDS] fournie par le développeur, sur le périmètre retenu de modélisation. A cette fin, et bien que cela ne semble pas requis ici par l'énoncé de l'unité de travail, l'évaluateur fournit la liste idéale des propriétés à modéliser qu'il confronte à celles qui ont été effectivement modélisées. Le développeur devra alors fournir une justification en regard au périmètre formel qu'il a retenu afin que le centre de certification puisse trancher. Le même travail devra être réalisé sur les caractéristiques, ces caractéristiques devant bien sûr être liées à des propriétés formelles (l'évaluateur se réfèrera alors à sa liste « idéale »).	
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.	*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.*
Le document d'interprétation du modèle doit fournir la correspondance entre les notions formelles et informelles ([ARG_CDS]). Les niveaux de détail des notions formelles et informelles étant par nature très différents, le regard critique de l'évaluateur sur cette correspondance est aussi requis ici. En effet, une caractéristique informelle peut être décrite d'un point de vue beaucoup plus macroscopique que ses pendants formels, qui devront être représentés à un niveau suffisamment pertinent pour permettre l'identification des mécanismes de sécurité qui seront effectivement implémentés et démontrer leur suffisance pour couvrir le besoin de sécurité. La subjectivité de cette unité de travail peut nécessiter de nouveau que le centre de certification soit en charge de trancher pour établir le verdict final. Le document d'interprétation du modèle ([ARG_CDS]) doit également décrire la portée du modèle et la justifier (justification de toutes les « hypothèses » mises en œuvre par le modèle ; par exemple, il est acceptable d'introduire des « hypothèses » qui correspondent à des objectifs de sécurité sur l'environnement).	
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.	**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
ADV_SPM.3-6 The evaluator shall examine the TOE security policy model ~~rationale~~ to determine that it formally proves the correspondence between the security properties and the security features.	*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*
Preuve formelle que les caractéristiques formelles respectent les propriétés formelles.	Preuve formelle qu'un état non sûr n'est pas atteint. (Rappel : Un état non sûr correspond à un état ne satisfaisant pas les objectifs de sécurité)

CC v2.3 (AIS34)	**CC v3.1**
Cette unité de travail consiste à vérifier la pertinence des éléments identifiés dans [ARG_PROOF] ainsi que la complétude de ce document, puis à vérifier la preuve [PROOF] fournie à partir du source du modèle [SRC]. L'évaluateur est chargé de rejouer la preuve développée à l'aide des outils fournis par le développeur. Il doit reprendre « à la main » toutes les preuves papiers fournies. L'évaluateur doit ici mener ces preuves en regard des éléments qu'il a précédemment récoltés au titre de ADV_SPM.3-1 en [CC v2.3] ou ADV_SPM.1-1 en [CC v3.1] sur la méthode et l'outil, ainsi que sur le modèle (vérification que la preuve est bien complète, vérification de la pertinence des « hypothèses » introduites par le développeur, …).	
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.	*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.*
L'évaluateur vérifie que les « hypothèses » du modèle ne sont pas incohérentes entre elles à partir de la justification du développeur fournie dans [ARG_PROOF].	
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).*
Cette unité de travail consiste à analyser la cohérence du modèle avec l'ensemble des politiques de sécurité de la TOE décrites dans la cible de sécurité, y compris celles qui ne seraient pas modélisées. Le modèle ne représentant pas la totalité de la cible de sécurité, cette tâche mènera au verdict « Echec » si l'évaluateur identifie des SFR non modélisées qui sont incohérentes avec le comportement modélisé.	
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).*
L'évaluateur vérifie la correspondance entre le modèle et les SFR représentant la SFP en s'appuyant sur [ARG_CDS]. En échec si l'évaluateur identifie des SFR qui auraient dû être modélisées mais qui ne le sont pas.	
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.

<table>
<tr><th>CC v2.3 (AIS34)</th><th>CC v3.1</th></tr>
<tr><td>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.</td><td>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</td></tr>
<tr><td colspan="2">L’évaluateur vérifie ici la correspondance entre caractéristiques formelles (features) et FSP en s’appuyant sur [ARG_FSP] et [SRC].

Cette unité de travail consiste notamment à vérifier que [ARG_FSP] identifie toutes les fonctions de sécurité qui correspondent, même en partie, à des caractéristiques formelles.</td></tr>
<tr><td>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.</td><td>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</td></tr>
<tr><td colspan="2">Cette unité de travail consiste à vérifier que la description des fonctions de sécurité listées dans ADV_SPM.3-10 en [CC v2.3] ou ADV_SPM.1-10 en [CC v3.1] est cohérente avec la description de ces mêmes fonctions dans les spécifications fonctionnelles ; notamment, vérification que toutes les contraintes énoncées dans la représentation des caractéristiques formelles sont également décrites dans la documentation FSP.</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 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>
</table>

<table>
<tr><th>CC v2.3 (AIS34)</th><th>CC v3.1</th></tr>
<tr><td>Si FSP.4 est retenu, alors cette correspondance doit être formelle.

Si FSP.3 est retenu, alors cette correspondance doit être semi-formelle.</td><td>Si FSP.6 est retenu, alors cette correspondance doit être formelle pour les parties formelles de FSP, et semi-formelle pour les parties semi-formelles de FSP.

Si FSP.5 est retenu, alors cette correspondance doit être semi-formelle.

Sinon, aucune contrainte sur le formalisme n’est imposée.</td></tr>
<tr><td colspan="2">Si les spécifications sont fournies en style formel, les preuves fournies par le développeur doivent être rejouées par l’évaluateur en mettant en œuvre les éléments recueillis dans ADV_SPM.3-1 en [CC v2.3] ou ADV_SPM.1-1 en [CC v3.1].

Si les spécifications ne sont pas formelles, une vérification systématique des éléments de preuve est demandée.</td></tr>
<tr><td rowspan="3"></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>
<tr><td>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 and complete with the behaviour modeled (e.g. the features)</td></tr>
<tr><td>L’évaluateur vérifie qu’il n’y a pas d’incohérence entre les interfaces externes des caractéristiques formelles et celles des spécifications fonctionnelles (notamment que le modèle ne comporte pas d’interface externe qui ne serait pas décrite dans les spécifications fonctionnelles).

L’évaluateur vérifie également que les interfaces externes des spécifications fonctionnelles sont suffisamment détaillées au vu des caractéristiques formelles.</td></tr>
</table>

5. Conclusion

L'intérêt de ce composant d'assurance et de la démarche associée est la vérification formelle que des fonctions de sécurité spécifiées par les SFR suffisent à couvrir des besoins de sécurité exprimés dans la cible de sécurité et la détection d'éventuelles incohérences. On réalise donc une preuve formelle d'une partie jugée pertinente de la cible de sécurité : on montre, au sens mathématique du terme, que la partie de la TSF modélisée est en effet apte à assurer les propriétés de sécurité modélisées énoncées dans la cible de sécurité.

Ce composant d'assurance permet également :

- de proposer une modélisation des principes de sécurité sous-tendant la construction de la cible de sécurité et les fonctionnalités de sécurité choisies ;
- de donner une description plus précise de la démarche ayant prévalue pour construire la sécurité du produit ;
- d'établir un modèle mathématique et d'en fournir une interprétation qui se veut fidèle à la TSF et contribuer ainsi à une meilleure compréhension de cette dernière.

Ainsi, cette tâche permet de renforcer la confiance dans le fait que le produit couvre effectivement certains de ses objectifs de sécurité et ne comporte pas d'incohérence.

Annexe A Synthèses

Les figures suivantes offrent une vue synthétique du contenu de la présente note.

La première figure ci-dessous présente les transitions entre les différentes étapes identifiées dans cette note. Le degré de formalisme des travaux entre ces différentes étapes est symbolisé par l'épaisseur des transitions : les transitions représentées par des doubles flèches identifient des travaux formels, les flèches simples et en pointillés représentent des travaux informels.

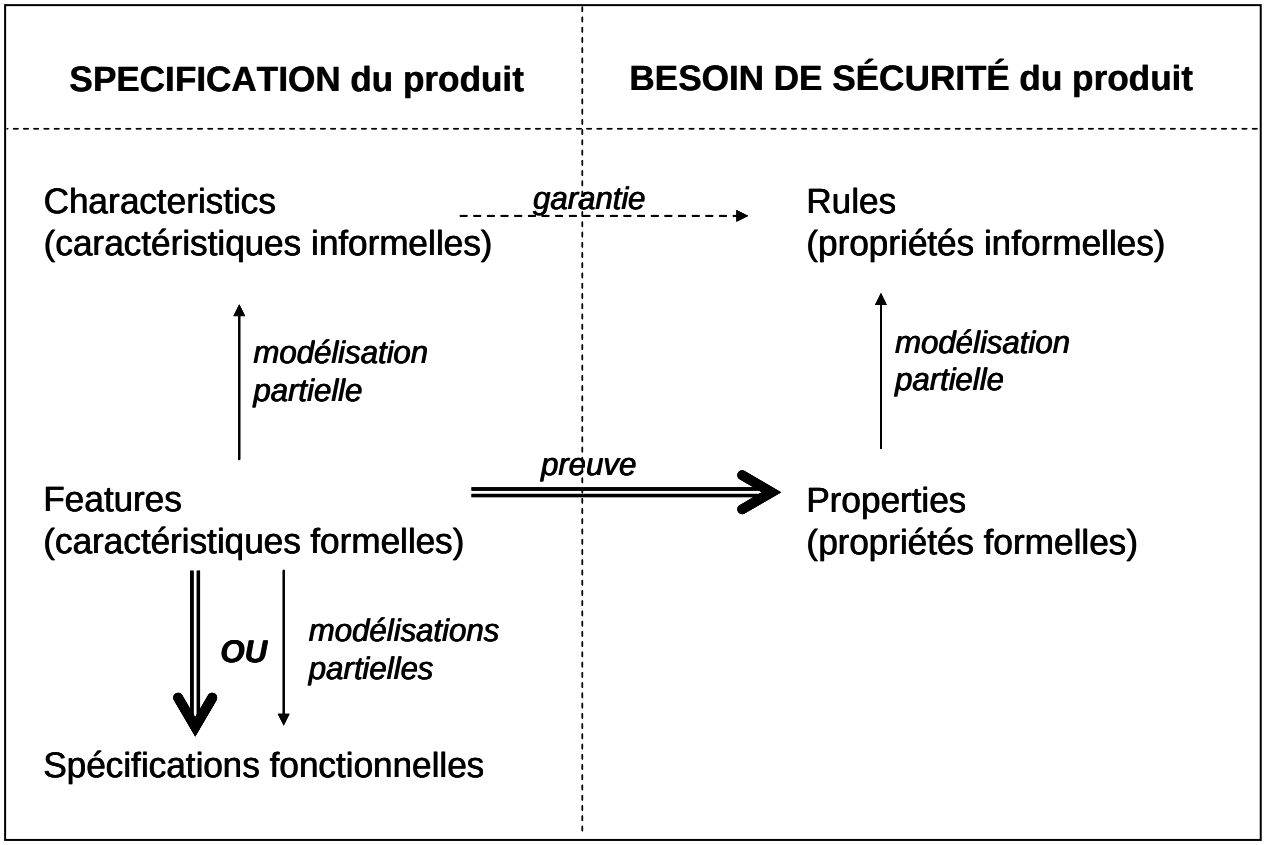

Figure 1 : Synthèse de la démarche

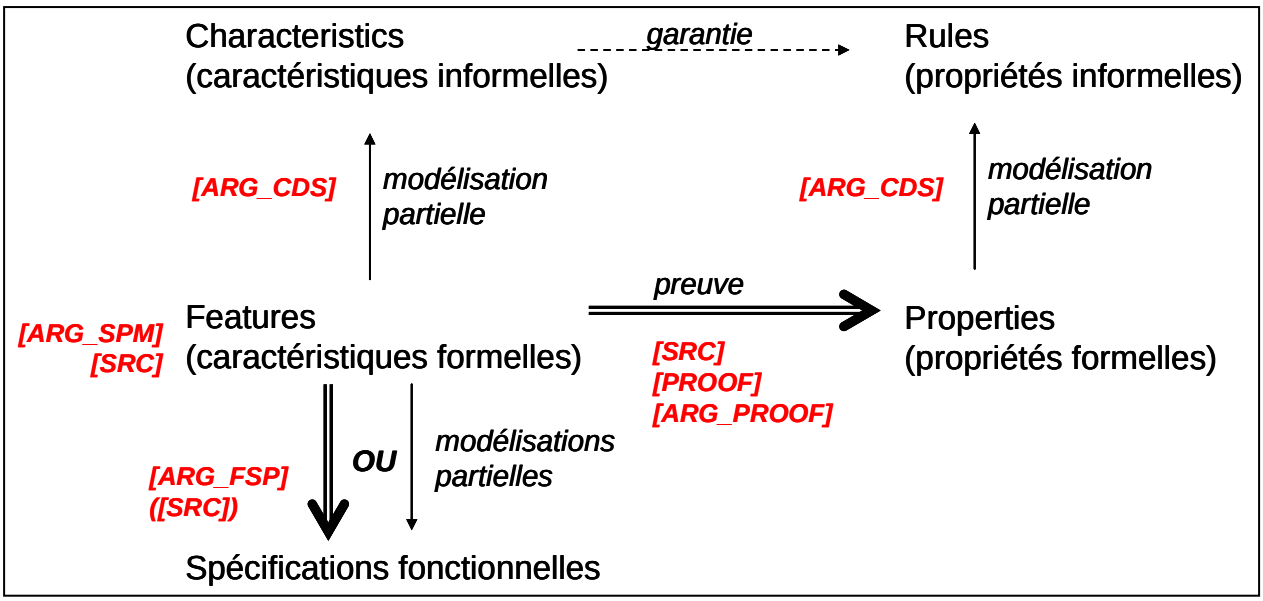

Figure 2 : Fournitures développeur

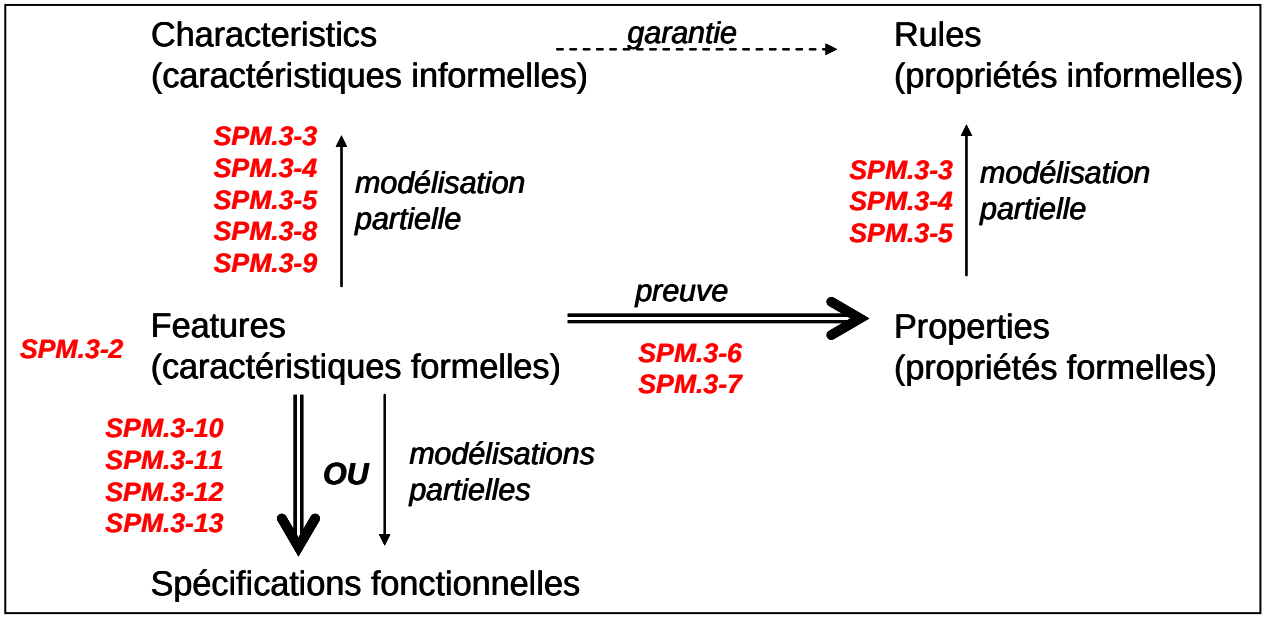

Figure 3 : Tâches d'évaluation selon [CC v2.3]