PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification PP/0304

JavaCard System Standard 2.1.1 Configuration Protection Profile

Version 1.0b

Paris, le 30 septembre 2003

Le Directeur central de la sécurité des systèmes d'information

Henri Serres

Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.
Un profil de protection est un document public qui définit pour une catégorie de produits un ensemble d'exigences et d'objectifs de sécurité indépendants de leur technologie et de leur implémentation. Les produits ainsi définis satisfont les besoins de sécurité communs à un groupe d'utilisateurs.
La certification d'un profil de protection ne constitue pas en soi une recommandation de ce profil de protection par l'organisme de certification.

Avant-propos

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendu public (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification selon les ITSEC et les Critères Communs sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Le site international concernant la certification selon les Critères Communs est accessible à l'adresse Internet :

www.commoncriteria.org

Table des matières

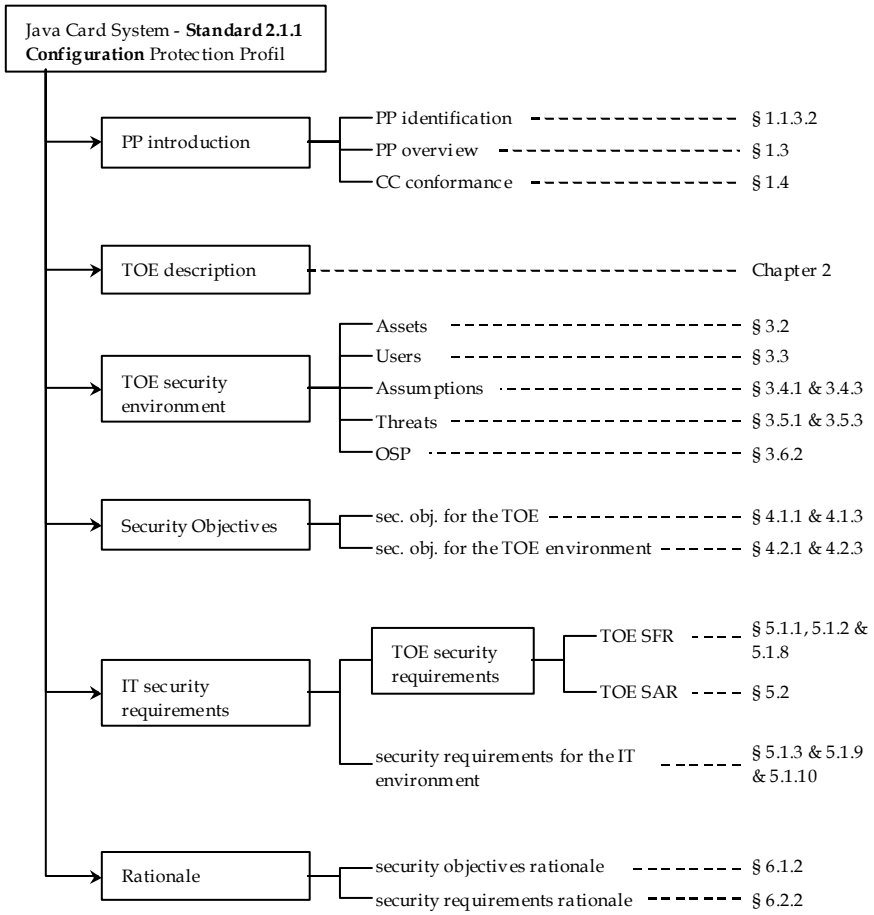
1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : JavaCard System – Standard 2.1.1 Configuration Protection Profile
Version : 1.0b
Date : août 2003

Ce profil de protection fait partie du document :
Titre : JavaCard System Protection Profile Collection
Version : 1.0b
Date : août 2003

qui regroupe quatre profils de protection identifiant chacun une configuration distincte de plate-forme Java Card. Il met en commun les chapitres introduction et description de la cible d'évaluation ainsi que les menaces, hypothèses, OSP, objectifs de sécurité et exigences fonctionnelles et d'assurance communs aux quatre configurations.
Les chapitres suivants du document *JavaCard System Protection Profile Collection* définissent le *JCS – Standard 2.1.1 Configuration Protection Profile* :



1.2. Rédacteur

Ce profil de protection a été rédigé par Trusted Logic SA pour le compte de Sun Microsystems, Inc. :

Trusted Logic SA

5, rue du Bailliage
78000 Versailles
France

Sun Microsystems, Inc.

4150 Network Circle
Santa Clara, CA 95054
Etats-Unis

1.3. Description du profil de protection

1.3.1. Généralités sur les plates-formes Java Card

La plate-forme Java Card

La plate-forme Java Card est la partie logicielle située « au-dessus » du micro-circuit et de son système d'exploitation (cf Figure 2). Elle permet à plusieurs applications (applets) d'être chargées sur une même carte à puce et assure une compatibilité de ces applications entre deux cartes à puce différentes – c'est-à-dire qu'une même application peut être exécutée sur deux plates-formes différentes.
En terme de sécurité, une plate-forme Java Card a pour principaux objectifs de contrer les accès ou les modifications non autorisés du code source et des données sensibles des applications chargées sur la plate-forme. Les principaux mécanismes de sécurité implémentés dans une plate-forme Java Card permettent d'accomplir :

- une séparation logique des données utilisées par différentes applications (*firewall*) ;
- une analyse statique du code source d'une application avant son installation (*bytecode verification*) ;
- le maintien de l'intégrité du code source d'une application entre sa vérification (*bytecode verification*) et son installation ;
- une gestion spécifique des clés cryptographiques et des codes PIN par application ;
- et des mécanismes d'authentification et de chiffrement.

Le profil de protection introduit le terme *Java Card System* (JCS) pour désigner la plate-forme Java Card. Elle est formée par le JCRE (*Java Card Runtime Environment*), la JCVM (*Java Card Virtual Machine*) et les API (*Application Program Interface*).
La plate-forme native, « sur » laquelle se trouve la plate-forme Java Card (cf Figure 2) est désignée par le terme SCP (*Smart Card Platform*) ; elle est composée du circuit intégré (IC), du système d'exploitation (OS) et de toutes les autres bibliothèques de fonctions natives présentes (DS).

Les applets

Les applications sont écrites en langage Java Card. Les étapes de développement et de chargement d'une application sont les suivantes :

1. développement du code source de l'application ;
2. compilation du code source, qui devient un fichier *class* ;
3. ce dernier fichier est traité par un *converter*, validant le code et générant un fichier *converted applet* (CAP) – l'équivalent d'un fichier *class* en programmation Java. Le fichier CAP contient une représentation binaire et exécutable des classes du *package* (ensemble de *classes* et d'*interfaces*, représentant dans le contexte Java Card soit une bibliothèque de fonctions utilisateur soit une ou plusieurs applets) ;
4. ensuite, le fichier CAP est vérifié en intégrité par le *bytecode verifier*, avant d'être chargé de manière sécurisée (permettant de garantir l'intégrité du fichier durant le chargement) sur la plate-forme. Dans certaines configurations de plates-formes Java Card, la vérification peut être effectuée sur la carte à puce, par le *card manager*. Dans ce cas, le fichier CAP est d'abord chargé sur la carte, puis vérifié ;
5. après ces opérations, le fichier est lié (*linked*) puis installé (*installed*). Pendant cette dernière phase, l'applet est enregistrée sur la carte par un numéro d'identification (AID – Application IDentifier) qui permettra d'identifier de manière unique l'instance de l'applet sur la carte (par exemple pour la sélection de l'applet, préalablement à son exécution).

L'exécution de l'applet est effectuée par l'interpréteur (*bytecode interpreter*) présent sur la carte.

1.3.2. Périmètre du profil de protection

Le produit défini dans le profil de protection [PP] est le JCS (Java Card System), c'est-à-dire la plate-forme Java Card. Elle est entièrement logicielle et ne contient aucune partie matérielle.
Le SCP (Smart Card Platform) – le circuit intégré, le système d'exploitation et les logiciels dédiés natifs (*firmware*) – ne fait pas partie du produit évalué. Le JCS sert de support aux applets, et interagit avec le SCP, le Card Manager, et les autres composants environnants (comme les applications natives par exemple). Ces derniers font donc tous partis de l'environnement TI du produit évalué.
Les applets ne font pas partie du produit évalué, elles ne sont que des données manipulées par le produit évalué.
Il existe deux types de biens à protéger :

- les *User Data* (données utilisateurs) qui sont le code source des applets et les données associées aux applets, les codes PIN du porteur de la carte à puce et les clés cryptographiques de chaque applet ;
- le second type de bien représente les *TSF Data* (pour TOE Security Functions Data) correspondant au code source du produit évalué, ses données et les clés cryptographiques utilisées lors du chargement d'applications sur la carte.

1.3.3. Cycle de vie

Le cycle de vie du produit est :

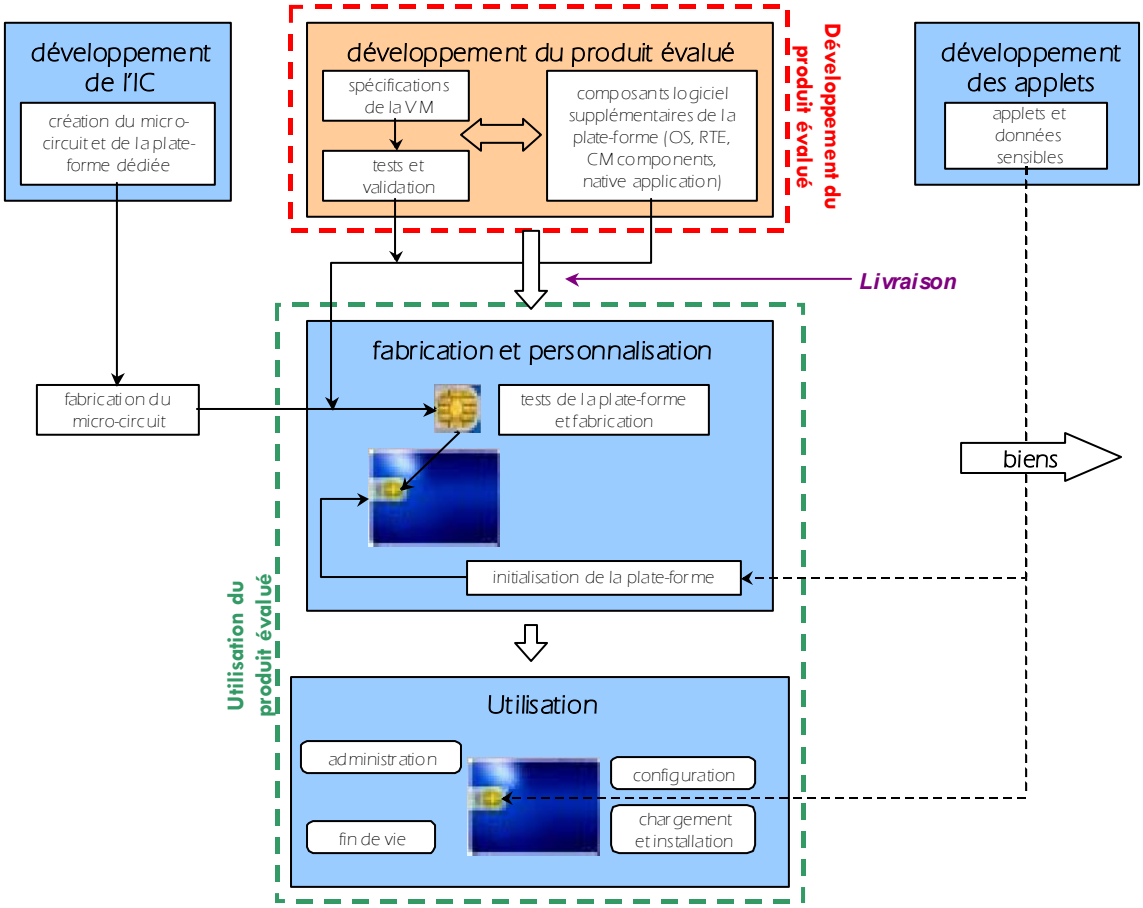


Figure 1 - Cycle de vie

1.3.4. Configuration couverte

Le profil de protection [PP] définit plusieurs configurations possibles du JCS. A chaque configuration est associé l'un des quatre profils de protection du document *JavaCard System Protection Profile Collection version 1.0b*.
Dans la configuration *Standard 2.1.1*, le produit évalué est la plate-forme Java Card sur laquelle il est possible de charger des applets en phase d'utilisation. Elle inclut par conséquent un *loader* et un *installer* permettant respectivement de charger une applet et de l'installer sur la plate-forme. Toute applet doit être vérifiée (*bytecode verification*) avant d'être chargée sur la carte (cette exigence est couverte par un objectif sur l'environnement du produit évalué).
La Figure 2 schématise le produit couvert par le profil de protection.

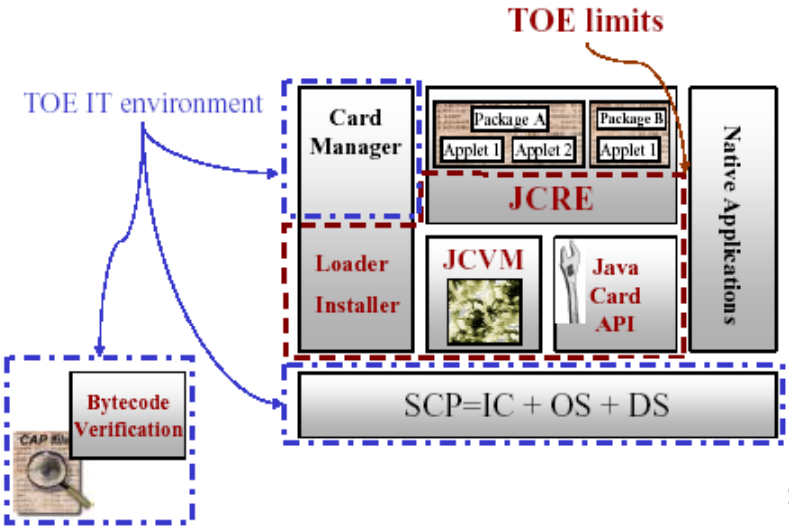


Figure 2 – Le produit et son environnement

1.4. Exigences d'assurance

L'ensemble des exigences fonctionnelles et d'assurance du profil de protection sont extraits respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
Le niveau d'assurance exigé par le profil de protection est le niveau **EAL4**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
AVA_VLA.3	Moderately resistant

Tableau 1 - Augmentations

Le niveau de résistance exigé pour les fonctions de sécurité est **moyen** (**SOF-Medium**).

1.5. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** du profil de protection sont les suivantes[2] :

- Security alarms (FAU_ARP.1)
- Enforced proof of origin (FCO_NRO.2)
- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key distribution (FCS_CKM.2)
- Cryptographic key access (FCS_CKM.3)
- Cryptographic key destruction (FCS_CKM.4)

[1] Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].
[2] Annexe 1 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)
- Security attribute based access control (FDP_ACF.1)
- Subset information flow control (FDP_IFC.1)
- Complete information flow control (FDP_IFC.2)
- Simple security attributes (FDP_IFF.1)
- Import of user data with security attributes (FDP_ITC.2)
- Subset residual information protection (FDP_RIP.1)
- Basic rollback (FDP_ROL.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Data exchange integrity (FDP_UIT.1)
- User attribute definition (FIA_ATD.1)
- Timing of identification (FIA_UID.1)
- User identification before any action (FIA_UID.2)
- User-subject binding (FIA_USB.1)
- Management of TSF data (FMT_MTD.1)
- Secure TSF data (FMT_MTD.3)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Security roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Automated recovery without undue loss (FPT_RCV.3)
- Non-bypassability of the TSP (FPT_RVM.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)
- TSF domain separation (FPT_SEP.1)
- TSF testing (FPT_TST.1)
- Maximum quotas (FRU_RSA.1)
- Inter-TSF trusted channel (FTP_ITC.1)

1.6. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité sur l'environnement du profil de protection [PP §4.2.1 et §4.2.3] sont les suivants :

- Les API écrites en code natif ainsi que les applications natives sur la carte à puce doivent être en accord avec la cible d'évaluation afin d'assurer que les politiques de sécurité et les objectifs décrits dans le profil de protection ne sont pas transgressés (OE.NATIVE) ;
- En cas de perte de puissance ou de retrait de la carte du lecteur lorsqu'une opération est en cours, le SCP (*Smart Card Platform*) doit permettre à la cible d'évaluation soit d'effectuer l'opération jusqu'à son terme, soit de revenir dans un état stable et sécurisé (OE.SCP.RECOVERY) ;

- Le SCP (*Smart Card Platform*) doit soutenir les fonctions de sécurité de la cible d'évaluation (OE.SCP.SUPPORT) : il ne doit pas permettre que les fonctions de sécurité soient contournées ou altérées, il doit fournir les primitives cryptographiques nécessaires, il doit aussi permettre des transactions atomiques si nécessaire et la gestion des données fixes ou temporaires ;
- Le SCP (*Smart Card Platform*) doit posséder des fonctions de sécurité (OE.SCP.IC), correspondant à des politiques de sécurité ou des standards bien définis ;
- Le *card manager* doit contrôler l'accès à ses fonctions (comme par exemple l'installation, la mise à jour ou la suppression d'applets). Il doit aussi implémenter la politique de l'émetteur de carte (OE.CARD_MANAGEMENT) ;
- Aucune applet chargée après émission de la carte ne doit contenir de code en langage natif (OE.APPLET) ;
- Tout code source doit être vérifié (*bytecode verification*) avant d'être exécuté (OE.VERIFICATION).

2. L'évaluation

2.1. Centre d'évaluation

AQL Groupe SILICOMP

1 rue de la châtaigneraie
CS 51766
F 35513 Cesson Sévigné Cedex
France

Téléphone : +33 (0)2 99 12 50 00

Adresse électronique : cesti@aql.fr

2.2. Commanditaire

Sun Microsystems, Inc.

4150 Network Circle
Santa Clara, CA 95054
Etats-Unis

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans le rapport technique d'évaluation [RTE].

2.4. Synthèse de l'évaluation et rapport technique d'évaluation

L'évaluation du profil de protection a été menée sur la base des exigences de la classe APE définie dans la partie 3 des Critères Communs [CC] :

Class APE	Security Target evaluation
APE_DES.1	TOE description
APE_ENV.1	Security environment
APE_INT.1	ST introduction
APE_OBJ.1	Security objectives
APE_REQ.1	IT security requirements
APE_SRE.1	Explicitly stated IT security requirements

Tableau 2- Composants d'assurance de la classe APE

Pour tous les composants d'assurance du Tableau 2, un verdict « réussite » a été émis par l'évaluateur.
Le rapport technique d'évaluation [RTE] décrit les résultats détaillés de l'évaluation du profil de protection.

3. Conclusions de l'évaluation

3.1. Certification

Le centre de certification atteste que le profil de protection identifié au paragraphe 1.1 satisfait les exigences des critères d'évaluation des profils de protection définis dans la classe APE de la partie 3 des Critères Communs [CC].

3.2. Enregistrement

Le profil de protection « JavaCard System – Standard 2.1.1 Configuration Protection Profile » version 1.0b est enregistré comme profil de protection certifié sous la référence PP/0304.
Un profil de protection enregistré est un document public dont une copie pourra être téléchargée sur le serveur Internet de la Direction centrale de la sécurité des systèmes d'information : www.ssi.gouv.fr.
Suite à modification, une nouvelle version de ce profil de protection peut être enregistrée.
Sur demande du commanditaire, il pourra être retiré du catalogue des profils de protection certifiés.

3.3. Recommandations

Le rédacteur d'une cible de sécurité doit identifier dans la cible de sécurité la plate-forme (SCP) sur laquelle se trouve la plate-forme Java Card (JCS).

3.4. Limitations

Le certificat d'un profil de protection ne s'applique qu'à la version évaluée du profil de protection.
Le profil de protection se dit conforme aux spécifications Java Card publiées par Sun Microsystems, Inc.. Toutefois, le présent rapport de certification n'atteste pas cette conformité.

Annexe 1. Exigences fonctionnelles de sécurité exigées par le profil de protection

Attention : les descriptions des composants fonctionnels suivants sont donnés à titre indicatif. Seule une lecture attentive du profil de protection peut apporter la description exacte des exigences fonctionnelles.

Class FAU	**Security audit**
Security audit automatic response	
FAU_ARP.1	*Security alarms* Le produit doit entreprendre des actions dans le cas où une violation potentielle de la sécurité est détectée.
Class FCO	**Communication**
Non-repudiation of origin	
FCO_NRO.2	*Enforced proof of origin* Le produit doit générer systématiquement la preuve de l'origine des informations transmises.
Class FCS	**Cryptographic support**
Cryptographic key management	
FCS_CKM.1	*Cryptographic key generation* Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiés qui peuvent être basés sur une norme identifiée.
FCS_CKM.2	*Cryptographic key distribution* Le produit doit distribuer des clés cryptographiques conformément à une méthode de distribution spécifiée qui peut être basée sur une norme identifiée.
FCS_CKM.3	*Cryptographic key access* Les accès aux clés cryptographiques doivent être effectués conformément à une méthode d'accès spécifiée qui peut être basée sur une norme identifiée.
FCS_CKM.4	*Cryptographic key destruction* Le produit doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée qui peut être basée sur une norme identifiée.
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée.
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les

	objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Information flow control policy	
FDP_IFC.1	*Subset information flow control* Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'information.
FDP_IFC.2	*Complete information flow control* Chaque règle de contrôle de flux d'information identifiée doit traiter toutes les opérations sur les sujets et les informations couvertes par cette règle. Tous les flux d'information et toutes les opérations doivent être couverts par au moins une règle de contrôle de flux d'information identifiée. Conjointement avec le composant FPT_RVM.1, ceci correspond à l'aspect « systématiquement appelé » d'un moniteur de référence.
Information flow control functions	
FDP_IFF.1	*Simple security attributes* Ce composant impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la fonction et décrit comment les attributs de sécurité sont choisis par la fonction.
Import from outside TSF control	
FDP_ITC.2	*Import of user data with security attributes* Les attributs de sécurité doivent représenter correctement les données de l'utilisateur et doivent être associés de façon précise et non ambiguë avec les données de l'utilisateur importées.
Residual information protection	
FDP_RIP.1	*Subset residual information protection* Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets lors de l'allocation ou de la désallocation de la ressource.
FDP_ROL.1	*Basic rollback* Ce composant répond au besoin d'annulation d'un nombre limité d'opérations effectuées dans les limites définies.
Stored data integrity	
FDP_SDI.2	*Stored data integrity monitoring and action* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées et entreprendre des actions suite à une détection d'erreur.
Inter-TSF user data integrity transfer protection	
FDP_UIT.1	*Data exchange integrity* Ce composant concerne la détection d'erreurs liées à des modifications, suppressions, insertions et rejeux des données de l'utilisateur transmises.

Class FIA	**Identification and authentication**
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité doivent être maintenus individuellement pour chaque utilisateur.
User identification	
FIA_UID.1	*Timing of identification* Le produit autorise les utilisateurs à exécuter certaines actions avant d'être identifiés.
FIA_UID.2	*User identification before any action* Les utilisateurs doivent s'identifier avant que toute action ne soit autorisée.
User-subject binding	
FIA_USB.1	*User-subject binding* La relation entre les attributs de sécurité de l'utilisateur et un sujet agissant pour le compte de cet utilisateur doit être maintenue.
Class FMT	**Security management**
Management of TSF data	
FMT_MTD.1	*Management of TSF data* Les utilisateurs autorisés peuvent gérer les données des fonctions de sécurité du produit.
FMT_MTD.3	*Secure TSF data* Les valeurs allouées aux données du produit doivent être valides par rapport à l'état sûr.
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.2	*Secure security attributes* Le produit doit garantir que les valeurs assignées aux attributs de sécurité sont valides par rapport à l'état sûr.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs.
Class FPR	**Privacy**
Unobservability	
FPR_UNO.1	*Unobservability* Le produit n'autorise pas certains utilisateurs à déterminer si certaines opérations sont en cours d'exécution.
Class FPT	**Protection of the TSF**
Fail secure	
FPT_FLS.1	*Failure with preservation of secure state* Le produit doit préserver un état sûr dans le cas de défaillances identifiées.
Trusted recovery	

FPT_RCV.3	*Automated recovery without undue loss* Le produit doit revenir dans un état sûr sans intervention humaine, au moins pour un type d'interruption de service ; la reprise à la suite d'autres types d'interruption peut nécessiter le recours à une intervention humaine. Le produit ne doit pas autoriser la perte indue d'objets protégés.
Reference mediation	
FPT_RVM.1	*Non-bypassability of the TSP* Les règles de sécurité du produit ne doivent pas pouvoir être contournées.
Inter-TSF TSF data consistency	
FPT_TDC.1	*Inter-TSF basic TSF data consistency* Le produit doit offrir la capacité de garantir la cohérence des attributs lors des échanges avec un autre produit de confiance.
Domain separation	
FPT_SEP.1	*TSF domain separation* Le produit doit offrir un domaine protégé et distinct pour les fonctions de sécurité du produit et procurer une séparation entre sujets.
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.
Class FRU	**Resource utilisation**
Resource allocation	
FRU_RSA.1	*Maximum quotas* Le produit doit garantir, à l'aide de mécanismes de quotas, que les utilisateurs et les sujets ne monopoliseront pas une ressource contrôlée.
Class FTP	**Trusted path/channels**
Inter-TSF trusted channel	
FTP_ITC.1	*Inter-TSF trusted channel* Le produit doit offrir un canal de communication de confiance entre lui-même et un autre produit TI de confiance.

Annexe 2. Niveaux d'assurance prédéfinis IS0 15408 ou CC

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 3. Références

<table>
<tr><td colspan="2">Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.</td></tr>
<tr><td colspan="2">Décret 2001-272 du 30 mars 2001- Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.</td></tr>
<tr><td>[CC]</td><td>Critères Communs pour l’évaluation de la sécurité des technologies de l’information:
Part 1: Introduction and general model,
august 1999, version 2.1, ref CCIMB-99-031 ;
Part 2: Security functional requirements,
august 1999, version 2.1, ref CCIMB-99-032 ;
Part 3: Security assurance requirements,
august 1999, version 2.1, réf: CCIMB-99-033.</td></tr>
<tr><td>[CEM]</td><td>Méthodologie d’évaluation de la sécurité des technologies de l’information:
Part 2: Evaluation Methodology,
august 1999, version 1.0, ref CEM- 99/045.</td></tr>
<tr><td>[IS 15408]</td><td>Norme IS/IEC 15408 :1999, comportant 3 documents :
IS 15408–1: (Part 1) Introduction and general model ;
IS 15408–2: (Part 2) Security functional requirements ;
IS 15408–3: (Part 3) Security assurance requirements ;</td></tr>
<tr><td>[PP]</td><td>JavaCard System Protection Profil Collection
JavaCard System – Standard 2.1.1 Configuration Protection Profile
Version 1.0b
Août 2003
Sun Microsystems, Inc.</td></tr>
<tr><td>[RTE]</td><td>Evaluation Technical Report
Java Card System – Standard 2.1.1 Configuration Protection Profile
Référence TDL01-ETR2-1.02
version 1.02
AQL – Groupe Silicomp</td></tr>
</table>

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr