PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/52

jTOP e-Passport
-
Composant SLE66CLX641P masqué par l'application jTOP e-Passport version 8.05

Paris, le 19 décembre 2005

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2005/52

Produit : jTOP e-Passport
Composant SLE66CLX641P masqué par l'application jTOP e-Passport version 8.05

Développeurs : Trusted Logic, Infineon

Critères Communs version 2.2

EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2)

Commanditaire : Trusted Logic

Centre d'évaluation : Serma Technologies

Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA : ADV_IMP.2, ALC_DVS.2

Préface

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 rendus publics. (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 sont publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)
Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.
[2] En mai 2005, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, la Turquie, la République Tchèque, Singapour et l'Inde.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est l'application jTOP e-Passport version 8.05 développée par Trusted Logic et embarquée sur le micro-circuit SLE66CLX641P (référence m1522-a11, avec la bibliothèque RSA2048 V1.3) développé par Infineon.

1.2. Développeur

Le logiciel embarqué est développé par la société :

Trusted Logic S.A.

5, rue du Bailliage
78000 Versailles
France

Le micro-circuit et sa bibliothèque RSA sont développés et fabriqués par la société :

Infineon Technologies AG

St.-Martin-Straße 76,
81609 München,
Allemagne

1.3. Description du produit évalué

Le produit évalué est de type carte à puce sans contact, et implémente les fonctionnalités de passeport électronique, conformément aux spécifications de l'Organisation de l'Aviation Civile Internationale (cf. [ICAO]). Il s'agit d'un micro-circuit à interface sans contact, avec un logiciel embarqué permettant :

- de stocker les données signées du futur porteur du passeport (nation ou organisation émettrice, n° de passeport, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, données d'informations optionnelles), une donnée biométrique du porteur (photo du visage), des données d'authentification optionnelles et diverses données permettant de gérer la sécurité du document ;
- de vérifier l'authenticité du passeport et d'identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce micro-circuit et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels.

1.3.1. Architecture

Le produit est un MRTD (Machine Readable Travel Document), constitué d'une partie matérielle : le micro-circuit SLE66CLX641P, et d'une partie logicielle comprenant :

- un environnement d'exécution permettant d'exécuter des applications de type Java Card. Cet environnement est conforme aux spécifications Java Card (cf. [JCP]) ;

- une couche « GlobalPlatform » fournissant les services d'installation et de configuration d'application, de sélection d'applications en vue de leur exécution, et d'étanchéité entre leur contexte d'exécution. Elle offre aussi les services de gestion du cycle de vie de la carte et de diverses opérations administratives. Cette couche (incluant les blocs fonctionnels « Open » et « Issuer Security Domain ») est conforme aux spécifications « Visa Global Platform » (cf. [VGP]) ;
- l'application de passeport électronique elle-même (LDS), conforme aux spécifications de l'Organisation de l'Aviation Civile Internationale (cf. [ICAO]).

Cette architecture est résumée dans la figure suivante :

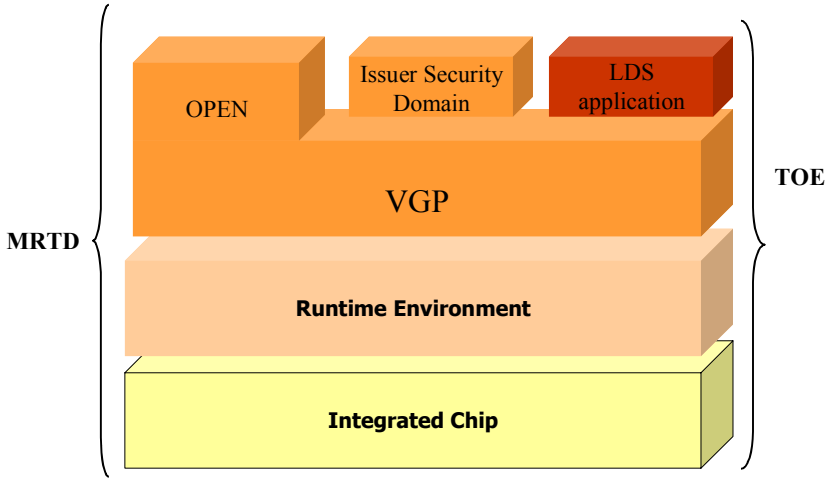

Figure 1 – Architecture du produit

1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

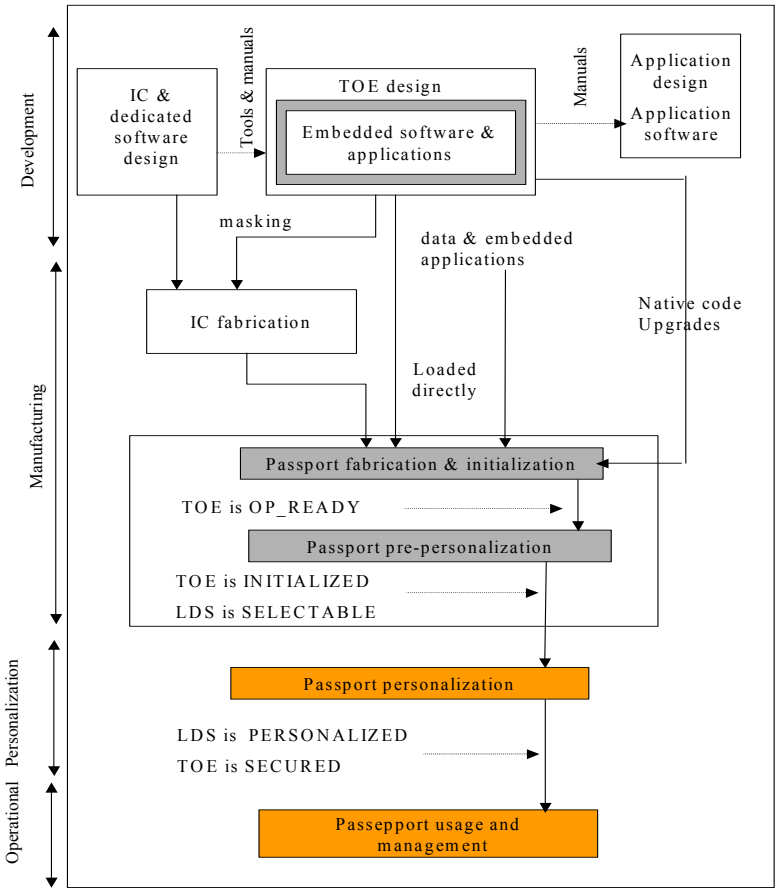

Figure 2 - Cycle de vie du produit

1.3.3. Périmètre et limites du produit évalué

Le produit évalué comprend la carte complète, c'est-à-dire le micro-circuit et son logiciel embarqué tel que décrit au paragraphe 1.3.1. Le système d'inspection permettant d'interroger la carte ne fait pas partie du périmètre d'évaluation.
En regard du cycle de vie, le produit évalué est le produit qui sort de la phase de fabrication, tests et pré-personnalisation (phase « Manufacturing »), c'est-à-dire le produit dans les phases de personnalisation et d'utilisation (en orange sur la figure 2).

2. L'évaluation

2.1. Contexte

L'évaluation a été effectuée selon le schéma de composition défini dans le document [COMP]. La composition consiste à réaliser l'évaluation d'un composant masqué en évaluant d'une part le micro-circuit, et d'autre part la partie logicielle, en vérifiant qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur le micro-circuit.
Cette évaluation a été réalisée sur la base des résultats de l'évaluation du micro-circuit SLE66CLX641P au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conformément au profil de protection [PP-BSI]. Ce micro-circuit a été certifié en Allemagne, le 9 novembre 2005, sous la référence BSI-DSZ-CC-0338-2005 (cf. [CERT-IC]).

2.2. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM.

2.3. Commanditaire

Trusted Logic S.A.

5, rue du Bailliage
78000 Versailles
France

2.4. Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Téléphone : +33 (0)5 57 26 08 64

Adresse électronique : m.dus@serma.com

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée de mars 2005 à décembre 2005.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.6. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Cette cible de sécurité s'inspire du PP MRTD en cours de développement lors de l'évaluation de ce produit (cf. [MRTD-PP]).

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite

2.7. Evaluation du produit

2.7.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL4[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ ALC_DVS.2	Sufficiency of security measures

2.7.2. L'évaluation de l'environnement de développement

Le logiciel embarqué est développé sur le site de :

Trusted Logic S.A.

5, rue du Bailliage
78000 Versailles
France

Les mesures de sécurité analysées par l'évaluateur permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation lors du développement.

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

L'évaluateur a analysé le plan de gestion de configuration fourni par le développeur qui précise l'utilisation du système de gestion de configuration. Le système permet de générer notamment la liste de configuration [CONF] qui identifie tous les éléments gérés par le système.

Des procédures de génération permettent par ailleurs de s'assurer que les bons éléments sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures analysées a été effectuée lors d'une visite du site de Versailles (cf Annexe 1).

L'environnement de développement du micro-circuit et de fabrication du produit final a été vu dans le cadre de l'évaluation du micro-circuit (cf. [CERT-IC]).

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite

2.7.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP), conception de haut-niveau (HLD), conception de bas-niveau (LLD), implémentation (IMP).

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- Exigences extraites des [CC] :
  - Cryptographic Key Generation (FCS_CKM.1)
  - Cryptographic key destruction (FCS_CKM.4)
  - Cryptographic operation (FCS_COP.1)
  - Subset access control (FDP_ACC.1)
  - Security attributes based access control (FDP_ACF.1)
  - Export of user data without security attributes (FDP_ETC.1)
  - Subset information flow control (FDP_IFC.1)
  - Import of user data without security attributes (FDP_ITC.1)
  - Basic internal transfer protection (FDP_ITT.1)
  - Basic rollback (FDP_ROL.1)
  - Stored data integrity monitoring and action (FDP_SDI.2)
  - Basic data exchange confidentiality (FDP_UCT.1)

  - Data exchange integrity (FDP_UIT.1)
  - Timing of authentication (FIA_UAU.1)
  - Single-use authentication mechanisms (FIA_UAU.4)
  - Multiple authentication mechanisms (FIA_UAU.5)
  - Timing of identification (FIA_UID.1)
  - Management of security attributes (FMT_MSA.1)
  - Secure security attributes (FMT_MSA.2)
  - Static attribute initialisation (FMT_MSA.3)
  - Specification of management functions (FMT_SMF.1)
  - Security management roles (FMT_SMR.1)
  - Unobservability (FPR_UNO.1)
  - Failure with preservation of secure state (FPT_FLS.1)
  - Basic TSF data internal protection (FPT_ITT.1)
  - Resistance to physical attack (FPT_PHP.3)
  - TSF domain separation (FPT_SEP.1)
  - TSF testing (FPT_TST.1)
  - Limited fault tolerance (FRU_FLT.2)
  - Inter-TSF trusted channel (FTP_ITC.1)
- Exigences de sécurité explicitement énoncées :
  - Limited capabilities (FMT_LIM.1)
  - Limited availability (FMT_LIM.2)

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_SPM.1	Informal TOE security policy model	Réussite
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.7.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du code de l'application, ainsi que des guides d'initialisation du produit, entre le développeur du masque Trusted Logic et le fabricant du produit Infineon.

Ces procédures permettent de connaître l'origine de la livraison et de détecter une modification du produit au cours de cette livraison.
La livraison du produit aux clients des phases ultérieures à la fabrication et à la pré-personnalisation se fait sous la responsabilité d'Infineon et les procédures associées ont été analysées dans le cadre de l'évaluation du micro-circuit (cf. [CERT-IC]).

L'installation du produit correspond à la phase d'initialisation du produit jusqu'à ce qu'il soit dans l'état OP_READY (cf. 1.3.2 - Cycle de vie), c'est-à-dire dans un état lui permettant d'être pré-personnalisé. Les procédures analysées [INSTALL] permettent d'obtenir la configuration évaluée du produit.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		Verdicts
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

2.7.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, les administrateurs sont considérés comme étant :

- les administrateurs du passeport en phase d'initialisation : ils sont chargés de personnaliser le passeport conformément aux règles établies dans leur pays, et notamment de configurer l'application (LDS), et de charger la clé d'authentification de l'agent de personnalisation ;
- les agents de personnalisation : ils agissent conformément aux règles établies dans leur pays en établissant l'identité du futur porteur et ses éléments biographiques, en enregistrant les données biométriques du futur porteur, et en intégrant ces données dans le passeport après les avoir signées numériquement ;
- les administrateurs du passeport en phase d'utilisation : ils sont responsables de la gestion du cycle de vie de la carte. Ils peuvent être incarnés successivement par les administrateurs identifiés précédemment.

Pour l'évaluation, les utilisateurs sont considérés comme étant :

- le système d'inspection en général : le système permettant de communiquer avec le passeport et d'effectuer les différentes opérations requises en contrôle frontalier . Les développeurs de ce système sont également considérés comme utilisateurs ;
- les officiers de contrôle frontalier : ils sont chargés d'effectuer les contrôles frontaliers à l'aide du système d'inspection ;
- le porteur final du passeport.

L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		Verdicts
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.7.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.

L'évaluateur a réalisé ses tests fonctionnels indépendants sur la plate-forme suivante : cartes identifiées au §1.1, dans les deux états représentatifs du produit certifié : produit en phase de personnalisation ou déjà personnalisé. Un émulateur du micro-circuit a également été utilisé.

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		**Verdicts**
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.7.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [INSTALL] [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Aucune fonction n'a nécessité une estimation du niveau de résistance intrinsèque.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests sur la plate-forme suivante : cartes identifiées au §1.1, dans les deux états représentatifs du produit certifié : produit en phase de personnalisation ou déjà personnalisé. Un émulateur du micro-circuit a également été utilisé.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaquants disposant d'un potentiel d'attaque de niveau **élémentaire**.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.2	Independent Vulnerability Analysis	Réussite

2.7.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (Art. 8 du décret 2002-535)

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation résumés ci-dessous et suivre les recommandations se trouvant dans les guides fournis [INSTALL] [GUIDES] :

- le fabricant et les administrateurs du passeport ne doivent pas réaliser d'opérations qui pourraient affaiblir le niveau de sécurité offert par le passeport. Toutes les clés permettant à un utilisateur d'avoir le rôle d'administrateur du passeport sont gardées secrètes et protégées par un environnement sécurisé garantissant leur non-divulgation et leur intégrité. Cela concerne les clés d'administration (ISD key), la clé d'accès basique au document (BAC key), la clé privée d'authentification active, ainsi que la clé privée de signature des données du passeport ;
- l'Etat émetteur ou l'organisation doit s'assurer que les utilisateurs agissant en tant qu'agent de personnalisation (i) établissent l'identité correcte du porteur du passeport, et identifient ses données biographiques pour le passeport électronique, (ii) enregistrent les données biométriques de référence du porteur, c'est-à-dire son portrait, et, (iii) personnalisent le passeport pour le porteur avec les mesures sécuritaires physiques et logiques requises (incluant la signature électronique des données du porteur dans le passeport). L'agent de personnalisation active la fonction de contrôle d'accès basique (BAC) et génère la clé de contrôle d'accès basique dans le passeport. L'agent de personnalisation doit générer des clés cryptographiques de 112 bits conformément à l'algorithme de dérivation des clés BAC spécifié dans l'annexe E du document [ICAO] relatif à la PKI ;
- l'Etat émetteur ou l'organisation doit :
    - générer une bi-clé de signature nationale, cryptographiquement sûre ;
    - garantir le secret de la clé privée de cette bi-clé nationale de signature et signer les certificats des signataires de document dans un environnement opérationnel sécurisé ;
    - distribuer un certificat de la clé publique nationale de signature aux Etats et organisations hôtes. Ce certificat assure l'intégrité et l'authenticité de cette clé ;

  L'Etat émetteur ou l'organisation doit également :
    - générer une bi-clé de signature des documents, cryptographiquement sûre ;

  - garantir le secret de la clé privée de cette bi-clé de signature de document, et signer les données sécuritaires d'un passeport authentique dans un environnement opérationnel sécurisé ;
  - distribuer aux Etats et organisations hôtes le certificat de la clé publique de signature de document signé avec la clé publique nationale, en maintenant son intégrité et son authenticité en utilisant l'infrastructure de clés décrite dans [MRTD] ;
- l'Etat émetteur ou l'organisation doit :
  - générer une bi-clé d'authentification active du passeport ;
  - signer et stocker dans le passeport la clé publique d'authentification active ;
- le système d'inspection de l'Etat ou organisation hôte doit utiliser le passeport qui lui est présenté pour vérifier l'identité du porteur et l'authenticité du passeport. Le système d'inspection est un terminal de confiance qui n'utilise pas ses privilèges pour divulguer les données auxquelles il a accès, ni pour suivre les utilisations successives du passeport ;
- le système d'inspection doit vérifier la signature des données signées du passeport préalablement à leur utilisation pour identifier le porteur. Les Etats et organisations hôtes doivent maintenir l'authenticité et la disponibilité des clés publiques de signatures nationales et de signature des documents au sein de tous les systèmes d'inspection (la clé publique de signature des documents peut être lue dans le passeport lui-même) ;
- le système d'inspection des Etats et organisations hôtes doit garantir la confidentialité et l'intégrité des données lues dans le passeport. Le terminal d'inspection utilisé par l'Etat hôte doit implémenter la partie « terminal » du protocole BAC ;
- le système d'inspection des Etats et organisations hôtes doit utiliser le mécanisme d'authentification active pour vérifier l'authenticité du passeport présenté par le voyageur, dans la mesure où le terminal a la capacité de réaliser cette opération ;
- le fabricant du passeport doit garantir la qualité et l'intégrité du processus de fabrication. Il est également responsable de la désactivation de tout mécanisme de test, de debug ou de chargement de correctifs dans le passeport, une fois que ce dernier est dans l'état « OP_READY » (juste avant la pré-personnalisation). Les différents rôles contribuant à la fabrication du passeport (fabricant, administrateur chargé de l'initialisation du passeport) doivent utiliser des procédures sécuritaires garantissant la confidentialité et l'intégrité du passeport et de ses données de tests jusqu'à sa distribution à l'utilisateur final (afin d'empêcher toute copie, modification, conservation, vol ou usage non autorisé). En particulier, le produit doit être protégé par des mesures adéquates lors de sa transmission d'un acteur à un autre.

3.3. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

3.4. Reconnaissance internationale (CC RA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, les augmentations suivantes n'entrent pas dans le cadre de l'accord : ADV_IMP.2 et ALC_DVS.2.

Annexe 1. Visite du site de développement de la société Trusted Logic à Versailles

Le site de développement de la société Trusted Logic situé 5, rue du Bailliage, 78000 à Versailles, a fait l'objet d'une visite par l'évaluateur les 24 et 25 mai 2005 et le 23 septembre 2005 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le produit jTOP e-Passport v8.05.

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ACM_AUT.1 et ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 2. Niveaux d'assurance prédéfinis EAL

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 documentaires du produit évalué

[CERT-IC]	Certification Report – Infineon Smart Card IC (Security controller), SLE66CLX640P/m1523-a11 and SLE66CLX641P/m1522-a11 both with RSA2048 v1.3 and specific IC dedicated software, Référence : BSI-DSZ-CC-0338-2005, 9 november 2005 Bundesamt für Sicherheit in der Informationstechnik (BSI)
[CONF]	jTOP v#8.05 e-Passport - Configuration Management Plan, Référence : DR-2005-NT-165-1.2 Trusted Logic
[GUIDES]	• jTOP v#8.05 - Administration Guide, Référence : CP-2005-RT-136-1.2 Trusted Logic • jTOP v#8.05 e-Passport - User Guide, Référence : CP-2005-RT-137-1.1 Trusted Logic
[ICAO]	• PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 1st 2004 International Civil Aviation Organization, • Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, May 18th 2004 International Civil Aviation Organization, • Machine Readable Travel Documents, supplement 9303, version 3.0, 12nd June 2005
[INSTALL]	jTOP v#8.05 e-Passport – Card Initialization Phase, Référence : CP-2003-RT-52-3.0 Trusted Logic
[JCP]	• Java Card 2.1.1 Runtime Environment Specification, Revision 1.0, May 18th 2000 Sun Microsystems, • Java Card 2.1.1 Virtual Machine Specification, Revision 1.0, May 18th 2000 Sun Microsystems • Java Card 2.1.1 Application Programming Interface, Revision 1.0, May 18th 2000 Sun Microsystems.

[MRTD-PP]	Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Basic Access Control, Reference : BSI-PP-0017 Version 1.0, 18 August 2005 BSI
[PP-BSI]	Smartcard IC Platform Protection Profile, Référence : BSI-0002-2001, version 1.0, juillet 2002 Bundesamt für Sicherheit in der Informationstechnik (BSI)
[RTE]	Evaluation Technical Report - jTOP v#8.05 e-Passport (EAL4+ evaluation), Référence : COCOON_ETR_V1.0 Serma Technologies
[ST]	Cible de référence pour l'évaluation : • JTOP e-Passport Security Target, Référence : CP-2005-RT-75/1.10 Trusted Logic Pour les besoins de la reconnaissance internationale, la cible suivante a été fournie et validée dans le cadre de cette évaluation : • JTOP e-Passport Security Target Lite, Référence : PU-2005-RT-624/1.0 Trusted Logic
[VGP]	• OpenPlatform Card Specification, Version 2.0.1', 7 April 2000 • VISA OpenPlatfrom 2.0.1' Card Implementation Requirements, Configuration 2 – Compact with PK, Version 1.0, February 2000, • VISA OpenPlatfrom 2.0.1' Card Implementation Requirements, Configuration 2 – Compact with PK, Errata 2.0, June 2003
[Visite]	Evaluation report - Classes ACM, ADO, ALC – Annexe A, Référence : COCOON_ACM-ALC-ADO_v1.1 Serma Technologies

Annexe 4. Références liées à la certification

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.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[COMP]	Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

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