



PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2011/75

ID One™ ePass v2.2 en configuration EAP et AA sur composants STMicroelectronics ST23YR80/48B

Paris, le 07 FEV 2012

*Le directeur général de l'agence nationale
de la sécurité des systèmes d'information*

Patrick Pailloux
[ORIGINAL SIGNE]



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 présumées 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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

<i>Référence du rapport de certification</i> ANSSI-CC-2011/75	
<i>Nom du produit</i> ID One™ ePass v2.2 en configuration EAP et AA sur composants STMicroelectronics ST23YR80/48B	
<i>Référence/version du produit</i>	
<i>Conformité à un profil de protection</i> Néant	
<i>Critères d'évaluation et version</i> Critères Communs version 3.1 révision 3	
<i>Niveau d'évaluation</i> EAL 5 augmenté ALC_DVS.2, AVA_VAN.5	
<i>Développeur(s)</i> Oberthur Technologies 50 quai Michelet, 92300 Levallois-Perret, France	STMicroelectronics 190 Avenue Célestin Coq, ZI de Rousset, BP2, 13106 Rousset Cedex France
<i>Commanditaire</i> Oberthur Technologies 50 quai Michelet, 92300 Levallois-Perret, France	
<i>Centre d'évaluation</i> Serma Technologies 30 avenue Gustave Eiffel, 33608 Pessac, France	
<i>Accords de reconnaissance applicables</i>   Le produit est reconnu au niveau EAL4.	

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 modifié. Ce décret indique que :

- L'agence nationale 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 disponibles sur le site Internet www.ssi.gouv.fr.



Table des matières

1. LE PRODUIT	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Identification du produit</i>	6
1.2.2. <i>Services de sécurité</i>	7
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Cycle de vie</i>	9
1.2.5. <i>Configuration évaluée</i>	10
2. L’EVALUATION	11
2.1. REFERENTIELS D’EVALUATION	11
2.2. TRAVAUX D’EVALUATION	11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	11
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	11
3. LA CERTIFICATION	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS D’USAGE.....	12
3.3. RECONNAISSANCE DU CERTIFICAT	12
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	12
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	13
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	14
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	15
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	16

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte « ID One™ ePass v2.2 en configuration EAP et AA sur composants STMicroelectronics ST23YR80/48B » développé par **Oberthur Technologies** sur un composant STMicroelectronics.

Le produit évalué est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de permis de conduire électronique. Ce produit est destiné à vérifier l'authenticité du permis de conduire à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué peuvent être intégrés sous forme de module ou d'*inlay*. Le produit final peut être un permis de conduire, une carte plastique, etc.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité s'inspire du profil de protection [PP EAC]. Le commanditaire a considéré que la problématique de sécurité du produit « permis de conduire » était proche de celle du passeport et que l'utilisation du PP EAC était pertinente pour l'établissement de cette cible de sécurité.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments suivants :

- nom commercial : ID One™ ePass v2.2 en configuration EAC et AA sur composants STMicroelectronics ST23YR80/48B ;
- référence du produit : *ePass V2.2 on ST23YR80/48B* ;
- référence du composant : *ST23YR80/48* ;
- code SAAAAR : 072263 ;
- code optionnel (*patch*) : 076081.

Ces informations peuvent être vérifiées par les données de traçabilités (CPLC¹).

- le composant **ST23YR80B** est identifié par un GET DATA de valeur 9F7F².

Les 13 premiers octets retournés doivent être 9F 7F 2A 47 50 B2 14 82 31 01 69 30 03 dont le détail est le suivant :

- rappel des données du GET DATA : **9F 7F** ;
- information sur la taille de la réponse : **2A** ;
- fabricant du composant : **47 50** (STMicroelectronics) ;
- type du composant : **B214** (ST23YR80B) ;
- identifiant du système d'exploitation : **82 31** (OBERTHUR OS) ;
- date de la version du système d'exploitation : **01 69** (169^{ème} jour de 2010) ;

¹ Card manager Production Life Cycle.

² en hexadécimal.

- version du système d'exploitation : **30 03**.
- le composant **ST23YR48B** est identifié par un GET DATA de valeur 9F7F¹
Les 13 premiers octets doivent être 9F 7F 2A 47 50 AC 14 82 31 01 69 30 03 dont le détail est le suivant :
 - rappel des données du GET DATA : **9F 7F** ;
 - information sur la taille de la réponse : **2A** ;
 - fabricant du composant : **47 50** (STMicroelectronics) ;
 - type du composant : **AC 14** (ST23YR48B) ;
 - identifiant du système d'exploitation : **82 31** (OBERTHUR OS) ;
 - date de la version du système d'exploitation : **01 69** (169^{ème} jour de 2010) ;
 - version du système d'exploitation : **30 03**.
- les autres données d'identification de la TOE sont identifiées par un GET DATA de valeur DF52¹
Les 17 premiers octets doivent être DF 52 0C 57 01 00 07 22 63 30 37 36 30 38 31 90 00 dont le détail est le suivant :
 - rappel des données du GET DATA : **DF 52** ;
 - information sur la taille de la réponse : **0C** ;
 - numéro du masque : **57** ;
 - version du masque : **01** ;
 - *LDS configuration* : **00** ;
 - code SAAAAR du ROM code : **07 22 63** ;
 - code SAAAAR du code optionnel : **30 37 36 30 38 31**².

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- le contrôle d'accès en lecture et en écriture ;
- le mécanisme EAP ;
- le mécanisme de *secure messaging* ;
- l'authentification de l'agent de personnalisation ;
- l'authentification active (si activée) ;
- la protection physique.

1.2.3. Architecture

Le produit est une carte à puce fermée constituée des éléments suivants :

- un microcontrôleur (ST23YR80B ou ST23YR48B de STMicroelectronics) ;
- une application native « *BIOS FAT full* » donnant l'accès aux fonctionnalités du microcontrôleur ;
- une librairie cryptographique dédiée ;
- une application de personnalisation *Perso* ;
- l'application LDS³ supportant les mécanismes EAC, EAP, BAC et BAP et dont certaines fonctionnalités ne font pas partie de la TOE. Leur présence a été, cependant, prise en compte lors de l'analyse de vulnérabilité :
 - *PACE generic* (mappage générique pour SAC, pace V2) ;

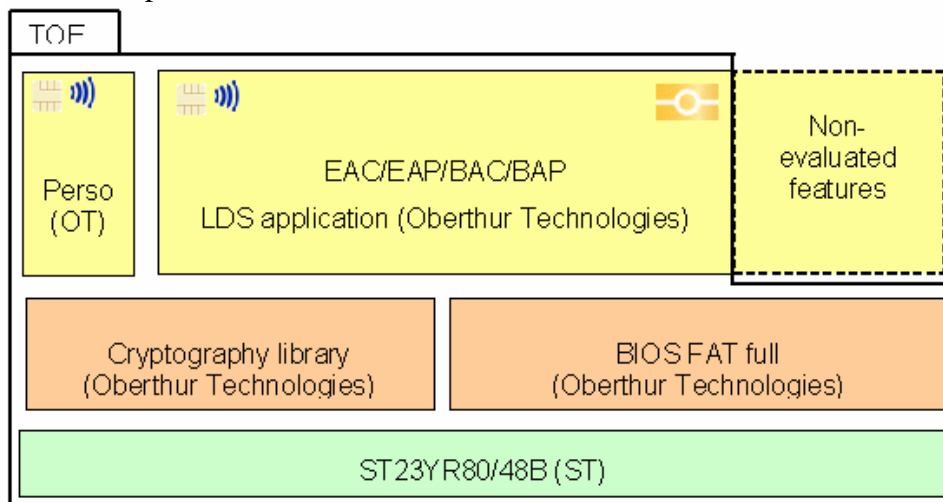
¹ en hexadécimal.

² code ASCII du code SAAAAR 076081 attendu.

³ *Logical Data Structure*

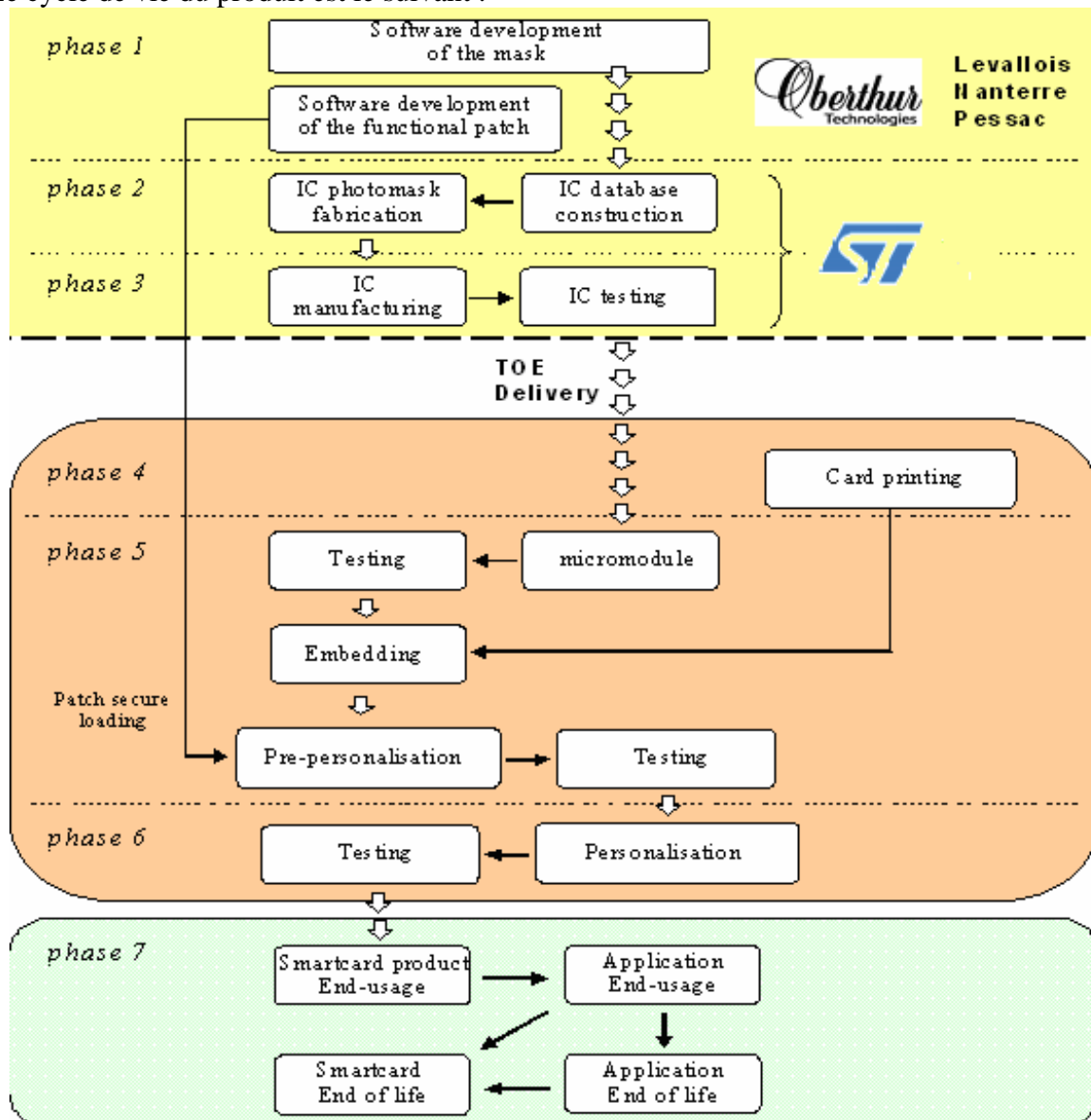
- *PIN management* (gestion d'un PIN alphanumérique en tant que condition d'accès) ;
- Biométrie (gestion d'un PIN biométrique en tant que condition d'accès).

La figure suivante représente cette architecture :



1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le produit a été développé sur les sites suivants :

Oberthur Technologies – Site de Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies – Site de Levallois

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies – Site de Pessac

Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus – Porte 2
33600 Pessac
France

STMicroelectronics SAS

Smartcard IC division
190 Avenue Célestin Coq, ZI de Rousset, BP2
13106 Rousset Cedex
France

1.2.5. Configuration évaluée

Le produit peut être personnalisé selon différentes configurations.

Le certificat porte sur la configuration suivante :

- mécanisme BAC activé ;
- mécanisme BAP activé ;
- mécanisme EAC activé ;
- mécanisme EAP activé ;
- mécanisme *active authenticate* activé (ECC ou RSA).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « *Microcontrôleurs sécurisés ST23YR48B et ST23YR80B* » au niveau EAL6 augmenté des composants ALC_FLR.1 conforme au profil de protection [PP]. Ce microcontrôleur a été certifié le 1^{er} février 2010 sous la référence [ANSSI-CC-2010/01].

Le niveau de résistance du microcontrôleur a été confirmé le 30 juin 2011 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 25 mai 2011, détaille les travaux menés par le centre d'évaluation. Ce rapport et les échanges complémentaires associés attestent que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée par l'ANSSI conformément à ses référentiels techniques [REF-CRY], [REF-KEY] et [REF-AUT]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Il en ressort que pour assurer la conformité aux référentiels techniques de l'ANSSI décrits ci-dessus, les recommandations suivantes devront être suivies lors de la personnalisation du produit :

- la taille des clés RSA et de groupe DH devra être d'au moins 2048 bits ;
- la taille des clés ECDSA de groupe ECDH devra être d'au moins 200 bits (256 bits recommandés).

2.4. Analyse du générateur d'aléas

Le générateur d'aléas utilisé par le produit final s'appuie sur le générateur physique fourni par le produit hôte (Cf [ANSSI-CC-2010/01]) et emploie un retraitement d'aléa cryptographique reconnu conforme aux référentiels techniques de l'ANSSI [REF-CRY] et [REF-KEY].

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « ID One™ ePass v2.2 en configuration EAP et AA sur composants STMicroelectronics ST23YR80/48B » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

3.3.2. *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires¹, des certificats Critères Communs. La reconnaissance 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 Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit		
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	2	3	3	4	3	3	Testing modular Design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - <i>BIFROST Security Target EAP, reference: FQR 110 5140, Issue 4, 9th december 2011, Oberthur Technologies.</i> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - <i>ID One™ ePass V2.2 on ST23 In EAP configuration with AA, reference : FQR 110 5858, Ed 2, Oberthur Technologies.</i>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - <i>Evaluation Technical Report – BIFROST Project, reference: BIFROST_ETR_v1.1/1.1, 18th august 2011, Serma Technologies.</i>
[ANA-CRY]	<p>Cotation des mécanismes cryptographiques, référence : 894/ANSSI/ACE du 1^{er} avril 2011, ANSSI.</p>
[CONF]	<p>Liste de configuration</p> <ul style="list-style-type: none"> - <i>Configuration list, reference FQR 110 5529, version 1, 31th january 2011, Oberthur Technologies ;</i> - <i>ePass v2.x on ST23YR80 PRODUCT GENERATION DESCRIPTION, reference 072263 00 PGD, version AA, 14th june 2010, revision 3- AA Oberthur Technologies ;</i> - <i>Optional Code r1.0 for ePass V2.2 on ST23YR80, reference 076081 00 PGD 8th december 2010, revision 1-AA, Oberthur Technologies.</i>
[GUIDES]	<ul style="list-style-type: none"> - <i>BIFROST Guidance, reference: FQR 110 5487, Issue 1, 14th december 2010, Oberthur Technologies ;</i> - <i>BIFROST Administration and Personnalization Guidance document, reference: FQR 110 5117, Issue 2, 24^h december 2010, Oberthur Technologies.</i>
[ANSSI-CC-2010/01]	<p>Microcontrôleurs sécurisés ST23YR48B et ST23YR80B. Certifié le 1er février 2010 par l'ANSSI sous la référence ANSSI-CC-2010/01.</p>
[PP EAC]	<p><i>Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.10, 25 Mars 2009.</i> Certifié par le BSI.(Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0055-2009.</p>
[PP]	<p><i>Security IC Protection Profile, version 1.0, 23rd august 2007.</i> Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0035-2007.</p>

Annexe 3. Références liées à la certification

	Décret 2002-535 du 18 avril 2002 modifié 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]	<i>Common Criteria for Information Technology Security Evaluation :</i> <i>Part 1: Introduction and general model,</i> <i>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001;</i> <i>Part 2: Security functional components,</i> <i>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002;</i> <i>Part 3: Security assurance components,</i> <i>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.</i>
[CEM]	<i>Common Methodology for Information Technology Security Evaluation :</i> <i>Evaluation Methodology,</i> <i>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.</i>
[CC IC]	<i>Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.</i>
[CC AP]	<i>Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.</i>
[COMP]	<i>Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.</i>
[CC RA]	<i>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</i>
[SOG-IS]	« <i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> », version 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr



[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr
-----------	--