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-2012/29

ST33TPM12LPC
Version (HW ST33ZP24 revJ, FW PVSC 1.2.D.0 et PVSH 1.2.D.8)

Paris, le 16 juillet 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 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 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

Référence du rapport de certification

ANSSI-CC-2012/29

Nom du produit

ST33TPM12LPC

Référence/version du produit

Version (HW ST33ZP24 revJ, FW PVSC 1.2.D.0 et PVSH 1.2.D.8)

Conformité à un profil de protection

BSI-CC-PP-0030-2008-MA-01

Critères d'évaluation et version

CC version 3.1 révision 3

Niveau d'évaluation

EAL4 Augmenté

ALC_FLR.1 et AVA_VAN.4

Développeur

STMicroelectronics

44-46 Excelsiorlaan, 1930 Zaventen
Belgique

Commanditaire

STMicroelectronics

44-46 Excelsiorlaan, 1930 Zaventen
Belgique

Centre d'évaluation

Thales (T3S-CNES)

18 avenue Edouard Belin, Bpi 1414, 31401 Toulouse Cedex 9
France

Accords de reconnaissance applicables

CCRA

SOG-IS

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

1.1. Présentation du produit

Le produit évalué est un microcircuit de nom commercial « ST33TPM12LPC », référence du matériel ST33ZP24, en version J et du logiciel PVSC 1.2.D.0 et PVSH 1.2.D.8, développé par STMicroelectronics.
Ce produit est destiné à garantir l'intégrité matérielle et logicielle des ordinateurs conformément aux spécifications TPM (*Trusted Platform Module*).

1.2. Description du produit

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

La cible de sécurité est strictement conforme au profil de protection [BSI-CC-PP-0030-2008-MA-01].

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, obtenus par la commande TPM_GetCapability et par la référence marquée sur le boîtier :

Version	TPM_GetCapability (en hexadécimal)	marquage du boîtier
PVSC	1.2.D.0	P24 J PVSC
PVSH	1.2.D.8	P24 J PVSH

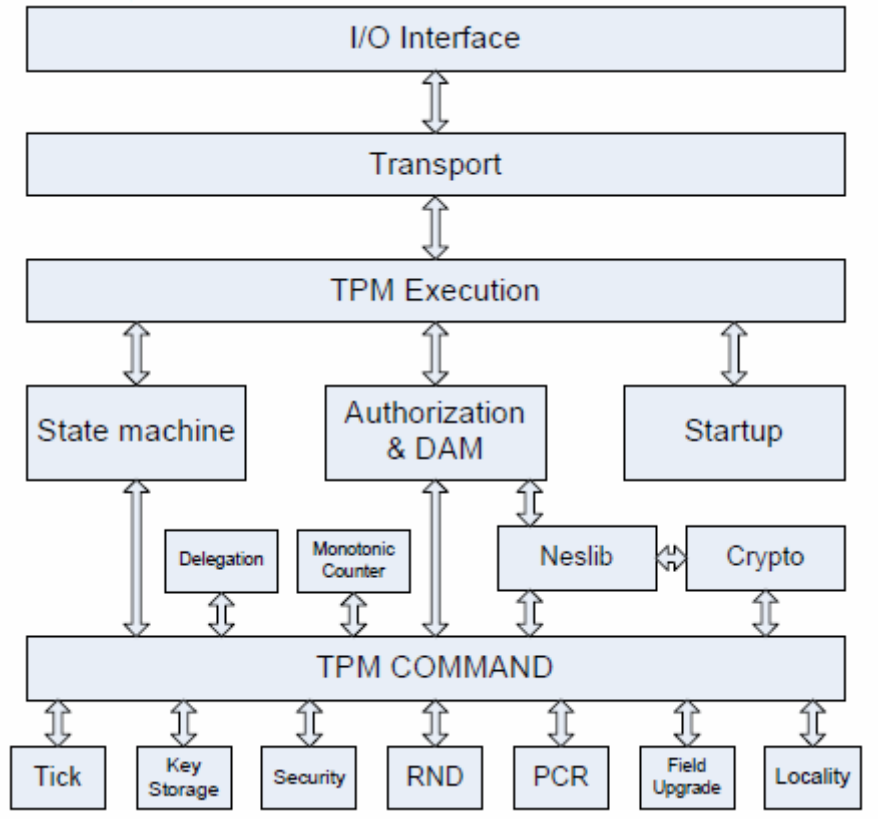
D'autres éléments d'identification sont gravés sur la surface de la puce :
- identifiant de la puce : K310A (avec les niveaux de masques correspondant au jeu de masque K310A_AJB)
- identifiant du logiciel de démarrage et autotest (OST) : AUG
- identifiant du masque applicatif : PVS
- identifiant du site de production : ST_4 (Rousset)

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont ceux offerts par le profil de protection [BSI-CC-PP-0030-2008-MA-01] et repris dans la cible de sécurité :
- support pour la mesure de la racine de confiance ;
- racine de confiance pour les rapports de mesures ;
- racine de confiance pour le stockage ;
- calcul de haché ;
- signature
- mémoire non volatile sécurisée ;
- gestion des tics d'horloge depuis le début de cession ;
- compteur monotone.

1.2.3. Architecture

L'architecture logicielle du produit est présentée ci-dessous.



Elle est constituée des éléments suivants :

- l'interface d'entrée sortie configurée pour le protocole LPC exclusivement ;
- l'emballage et le déballage pour le transport des sessions ;
- l'exécution des instructions TPM ;
- la machine d'état TPM ;
- la gestion des autorisations et les contre-mesures pour les attaques par dictionnaire ;
- la séquence de démarrage ;
- la gestion de délégation ;
- le compteur monotonique ;
- l'accès à la bibliothèque cryptographique Neslib (RSA et SHA1, AES, AES en mode CTR, HMAC, la signature PKCS, le chiffrement MGF, la dérivation de clés) ;
- la gestion des tics d'horloge ;
- le stockage des clés ;
- la gestion de registres de configuration ;
- la génération de nombres aléatoires ;
- la configuration de sécurité ;
- la gestion de la localité ;
- la mise à jour distante par chargement sécurisé par chiffrement et signature avec une clé RSA de 2048 bits.

1.2.4. Cycle de vie

Le cycle de vie du produit couvre toutes les phases de développement et de production.

Phase	Site
Développement	Pour le développement matériel : - STMicroelectronics SAS, Rousset - STMicroelectronics Pte ltd, Serangoon Pour le développement logiciel : - STMicroelectronics SAS, Rousset - STMicroelectronics, Zaventem - STMicroelectronics, Prague
Fabrication	Pour la fabrication, le test de conformité TPM, le chargement de clés TPM : - STMicroelectronics SAS, Rousset - STMicroelectronics, Toa Payoh

Le produit a été développé sur les sites suivants :

STMicroelectronics SAS, Secure Microcontroller Division

190 avenue Celestin Coq, ZI de Rousset,
13106 ROUSSET
France

STMicroelectronics Pte ltd

5A Serangoon North Avenue 5
554574 Singapore
Singapour

STMicroelectronics

44-46 Excelsiorlaan
B-1930 Zaventem
Belgique

STMicroelectronics

Pobřežní 620/3
186 00 Prague 3-Karlín
République Tchèque

STMicroelectronics

629 Lorong 4/6 Toa Payoh
319521 Singapore
Singapour

1.2.5. Configuration évaluée

Le certificat porte uniquement sur le microcircuit programmé avec l'application TPM, tel que présenté plus haut au paragraphe « Architecture » et configuré conformément au guide de personnalisation (cf. [GUIDES]).

Les tests ont été effectués sur des circuits comportant l'application TPM utilisable en phase « utilisation ».

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 [CEM].

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

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation du produit ST33F1M certifié le 5 avril 2011 sous la référence ANSSI-CC-2011/07 [ANSSI-CC-2011/07].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 avril 2012, détaille les travaux menés par le centre d'évaluation et atteste 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 selon les référentiels techniques de l'ANSSI [REF-CRY] et [REF-KEY] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était dans le périmètre de l'évaluation et a été analysé par le centre d'évaluation. L'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

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 « ST33TPM12LPC », référence du matériel ST33ZP24, en version J et du logiciel PVSC 1.2.D.0 et PVSH 1.2.D.8) soumis à l'évaluation répondent aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 augmenté des composants ALC_FLR.1 et AVA_VAN.4.

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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

La fonction de mise à jour distante par chargement sécurisé par chiffrement et signature avec une clé RSA de 2048 bits n'est pas couverte par ce certificat.

3.3. Reconnaissance du certificat

Ce certificat fait l'objet d'une reconnaissance internationale

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'accord[1], 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 :

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 signataires[2], 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 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.

[2] 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 4 +	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	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	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	1	Identification of security measures
	ALC_FLR								1	Basic flaw remediation
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
ASE Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	4	Methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - ST33TPM1.2 Security Target (Final) référence PTD_TPMCC_ST_10_001_V01.01, version 1,1 du 16 avril 2012 éditée par STMicroelectronics. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST33TPM1.2 Security Target (Public Version) référence PTD_TPMCC_ST_10_001_V00.01p, version 1.1p du 27 juin 2012 éditée par STMicroelectronics.
[RTE]	Rapport technique d'évaluation : - ST33TPM1_2 Evaluation technical report référence S3M_ETR, version 1.0 du 17 avril 2012 édité par Thales ITSEF.
[CONF]	Liste de configuration : - PVSC Configuration List référence PTD_ST33ZP24PVSC_CFGL_12_001_V01.01, version 1,1 du 16 avril 2012, édité par STMicroelectronics ; - PVSH Configuration List référence PTD_ST33ZP24PVSH_CFGL_12_001_V01.01, version 1,1 du 16 avril 2012, édité par STMicroelectronics ; - ST33ZP24 Configuration List référence SMD_33ZP24_CFGL_12_001, version 1 du 4 mars 2012, édité par STMicroelectronics.
[GUIDES]	Guide d'utilisation du produit : - ST33TPM12LPC Datasheet (PVSC) référence DS_33TPM12LPC, version 6 du 24 janvier 2012 édité par STMicroelectronics ; - ST33TPM12LPC Datasheet (PVSH) référence DS_33TPM12LPC, version 7 du 8mars 2012 édité par STMicroelectronics ; - Security guidelines for TPM configuration and usage référence PTD_ST33TPM12_AN_12_001_V01.01, version 1,1 du 16 avril 2012 édité par STMicroelectronics.
[ANSSI-CC-2011/07]	ST33F1M certifié le 5 avril 2011 sous la référence ANSSI-CC-2011/07.
[BSI-CC-PP-0030-2008-MA-01]	Protection Profile - PC Client Specific Trusted Platform Module TPM Family 1.2 Level 2 revision 116, version v1.2 du 18 mai 2011. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0030-2008-MA-01 le 6 octobre 2011.*

Annexe 3. 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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	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.
[CC AP]	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.
[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 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.