Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de maintenance ANSSI-CC-2013/13-M02

Microcontrôleurs sécurisés ST33F1M/1M0/896/768/640/512E, SC33F1M/1M0/896/768/640/512/384E, SM33F1M/1M0/896/768/640/512E, SE33F1M/1M0/896/768/640/512E, SL33F1M/1M0/896/768/640/512E et SP33F1ME, avec le logiciel dédié révision D, incluant optionnellement la bibliothèque cryptographique NesLib version 3.0 ou 3.2, et optionnellement MIFARE DESFire EV1

Certificat de référence : ANSSI-CC-2013/13

Paris, le 19 août 2014

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

[Original signé]

Contre-amiral Dominique RIBAN

SÉCURITÉ CERTIFICATION

1. Références

[MAI] Procédure MAI/P/01 Continuité de l'assurance ;

[CER] Rapport de certification ANSSI-CC-2013/13, ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384, SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512, SL33F1M/1M0/896/768/640/512, SP33F1M, With dedicated software revision D, Optional cryptographic library Neslib 3.0 or 3.2, Optional MIFARE DESFire EV1, maskset K8C0A, révision externe E, révision interne G, 6 mars 2013, ANSSI ;

[M01] Rapport de maintenance ANSSI-CC-2013/13-M01, ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384,SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512, SL33F1M/1M0/896/768/640/512, SP33F1M, With dedicated software revision D, Optional cryptographic library Neslib 3.0 or 3.2, Optional MIFARE DESFireTM EV1, maskset K8C0A, révision externe E, révision interne G, 8 avril 2013, ANSSI ;

[S01] Rapport de surveillance ANSSI-CC-2013/13-S01, Microcontrôleurs sécurisés dérivés du ST33F1M, 6 août 2014, ANSSI ;

[IAR] Impact analysis report - Evolution for Sx33FxxxE and rev F - SMD_33F_SIA_13_002 Version 1.00, 18 décembre 2013, STMicroelectronics ;

[SOG-IS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 Janvier 2010, Management Committee ;

[CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.

2. Identification du produit maintenu

Le produit maintenu est le microcontrôleur sécurisé ST33F1M et ses dérivés, initialement certifié sous la référence ANSSI-CC-2013/13 (voir [CER]). Il a déjà fait l'objet d'une maintenance (voir [M01]). Le produit est développé par STMicroelectronics.

3. Fournitures prises en compte

Suite à la surveillance de ce produit (voir [S01]), les documents suivants font désormais partie des guides d'utilisation du produit :

[GUIDES_SRV]	ST33 Secure MCUs, NesLib 3.0 cryptographic library, User manual, UM_33_NesLib_3.0 rev 8, 4 août 2014, STMicroelectronics.
	ST33 Secure MCUs, NesLib 3.2 cryptographic library, User manual, UM_33_NesLib_3.2 rev 5, 4 août 2014, STMicroelectronics.
	MIFARE DESFire EV1 Software library revision 1.1, User Manual, UM_MIFARE_DEFIRE_EV1 rev 3, 29 juillet 2014, STMicroelectronics.

4. Description des évolutions

Des nouveaux sites interviennent dans le cycle de vie. De plus, un nouveau profil SC33F1M est créé. Le développeur explique ces changements dans son IAR [IAR].

Pour le développement, le cycle de vie inclut les nouveaux sites suivants :

Opération	Site
IC design	ST Grenoble : STMicroelectronics, 12 rue Jules Horowitz, BP 217, 38019 Grenoble Cedex, France.
	ST Sophia : STMicroelectronics, 635 route des lucioles, 06560 Valbonne, France.
	ST Rennes : STMicrolectronics, 10 rue de Jouanet, ePark, 35700 Rennes, France.
IC Manufacturing	ST Crolles : STMicroelectronics, 850 rue Jean Monet, 38926 Crolles, France.
IC Assembly	STATS ChipPAC (Singapore) : STATS ChipPAC Ltd. 5 Yishun Street 23, Singapore 768442, Singapour.
	STATS ChipPAC (Taiwan) : STATS ChipPAC Taiwan, No.176-5, 6 Ling, Lu Liao Ken, Hua-Lung Chun, Chiung-Lin, Hsin-Chu Hsien, Taiwan, R.O.C 307, Chine.

Pour le nouveau profil commercial SC33F1M, le principe de dérivation est celui déjà mis en place pour les autres dérivés. Le SC33F1M est caractérisé par une mémoire Flash de 1280 kOctets et par une interface SWP inactive.
Ceci est transparent pour l'utilisateur. L'architecture du code du produit est inchangée.
Le développeur ne s'attend donc à aucune dégradation du niveau de sécurité de la plate-forme.

A noter : le développeur remplace le terme *System ROM* par le terme *Firmware*.

5. Fournitures impactées

Les cibles sont modifiées pour prendre en compte les nouveaux sites, la nouvelle identification du SC33F1M.
Les manuels de l'utilisateur subissent un impact très limité (*DataSheet* pour la description du nouveau profil).
Le changement a un impact mineur sur la documentation Critères Communs. Il est à noter que les documents certifiés restent inchangés en termes de couverture SFR et TSFI.

[CONF]	*ST33F1M rev E derivatives CCEAL5+ Evaluation Projects - Documentation Report*, référence ST33F1M_DR_12_001 v 1.3, 20 décembre 2013, STMicroelectronics.
[GUIDES]	*ST33F1M and derivatives Datasheet*, référence DS_ST33F1M rev 4, décembre 2013, STMicroelectronics.

	ST32 and ST33F Firmware User manual, référence UM_32_33F_FW Rev 1, décembre 2013, STMicroelectronics.
	ST33 uniform timing Application note, référence AN_33_UT Rev 2, novembre 2013, STMicroelectronics.
[CIBLE]	*ST33F1M/1M0/896/768/640/512E, SC33F1M/1M0/896/768/640/512/384E, SM33F1M/1M0/896/768/640/512E, SE33F1M/1M0/896/768/640/512E, SL33F1M/1M0/896/768/640/512E, SP33F1ME, with firmware revision D, optional cryptographic library NESLIB 3.0 or 3.2, and optional technology MIFARE DESFire™ EV1 Security Target,* référence SMD_SM33Fxxx_ST_11_001_V01.05, décembre 2013, STMicroelectronics.
	ST33F1M/1M0/896/768/640/512E, SC33F1M/1M0/896/768/640/512/384E, SM33F1M/1M0/896/768/640/512E, SE33F1M/1M0/896/768/640/512E, SL33F1M/1M0/896/768/640/512E, SP33F1ME, with firmware revision D, optional cryptographic library NESLIB 3.0 or 3.2, and optional technology MIFARE DESFire™ EV1 Security Target - Public Version, référence SMD_SM33Fxxx_ST_12_001 Rev 01.03, décembre 2013, STMicroelectronics.

6. Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur**.
Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée, à la date de certification.
Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

7. Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une ré-évaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

8. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

Reconnaissance européenne (SOG-IS)

Le certificat initial a été 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 :

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été émis dans les conditions de l'accord du CC RA [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'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 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.