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 certification ANSSI-CC-2016/31

Application Mobile PayPass 1.0.13vA.2.4 (S1133159, release B) sur plateforme UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F

Paris, le 1er juin 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2016/31

Nom du produit

Carte Mobile PayPass 1.0.13vA.2.4 (S1133159, release B) sur plateforme UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F

Référence/version du produit

S1133159, release B

Conformité à un profil de protection

néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 4 augmenté
ALC_DVS.2, AVA_VAN.5

Développeurs

Gemalto
La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France

STMicroelectronics
190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 Rousset, France

Commanditaire

Gemalto
La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France

Centre d'évaluation

Serma Safety & Security
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL2.

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 la « Carte Mobile PayPass 1.0.13vA.2.4 (S1133159, release B) sur plateforme UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F» développée par *GEMALTO* et *STMICROELECTRONICS*.

Ce produit est une carte (U)SIM[1] destinée à être insérée dans un téléphone portable disposant de la technologie NFC[2]. Il embarque l'application Mobile PayPass v1.0.13vA.2.4 qui met en œuvre la solution « Payez Mobile » (en dehors de la TOE) spécifiée par l'Association Européenne Payez Mobile (AEPM). Cette application permet de réaliser des transactions de paiement sans contact (CMP, *Contactless Mobile Payment*) par radiofréquence.

1.2. Description du produit

1.2.1. Introduction

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

1.2.2. 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 détaillés dans la [ST] au chapitre « 1.2 TOE reference » :

Nom du produit	Mobile PayPass 1.0.13vA.2.4 on UpTeq NFC3.2.2_Generic v1.0
Version du produit	Release B
Nom de l'application	Mobile PayPass 1.0.13vA.2.4
Référence de l'application	S1133159
Version de l'application	Release B
Nom de la plateforme	UpTeq NFC3.2.2_Generic v1.0
Référence de la plateforme	T1032507
Version de la plateforme	Release A

[1] *Universal Subscriber Identity Module.*
[2] *Near Field Communication*, communication en champs proche.

Les données d'identification pour les applications considérées dans le cadre de cette évaluation sont décrites ci-dessous :

- pour l'application Mobile PayPass v1.0.13vA.2.4 la réponse à la commande ABOUT 00 AB 00 00 2F est :
  4D5050312E305F416D656E64432D554943432D496E7465726F705F52656C656173652D412E322E345F3133313231339000
  soit en ASCII :
  MPP1.0_AmendC-UICC-Interop_Release-A.2.4_131213 ;
- pour l'application PPSE (hors TOE) la réponse à la commande ABOUT 00 AB 00 00 00 est :
  454D56436F2D505053455F416D656E64435F6553452D496E7465726F705F76312E302E345F323330313135
  soit en ASCII :
  EMVCo-PPSE_AmendC_eSE-Interop_v1.0.4_230115 ;
- pour l'application CREL Payez Mobile (hors TOE) obtenues en réponse à la commande ABOUT 00 AB 00 00 00 est :
  4352454C504D5F4145504D5F554943432D496E7465726F705F76312E302E315F303331323133
  soit en ASCII :
  CRELPM_AEPM_UICC_Interop_v1.0.1_031213.

Les moyens d'identification des autres composants du produit sont fournis dans le rapport de certification [ANSSI-CC-2016/22].

De plus, le tableau suivant fournit les empreintes SHA1 et SHA2 en hexadécimal des applications considérées dans le cadre de cette évaluation à partir des fichiers IJC[1] et/ou CAP :

- application Mobile PayPass (il y a 16 AID prédéfinis dans la carte) :

Package AID	Applet AID	SHA1-CAP file	SHA1-IJC file	SHA2-CAP file	SHA2-IJC file
A0000000 309000A3 01000010	A0000000 309000A3 01000110	**2CA3A3172B683C9911F49940176F552234C67CD0**	**DBE2993AC55CC433AEF54D7744E2FD2113F44F8A**	**88F380044DB66AAB5BB9B83F2DB82E61FC1D256A97551398F61412A2C8346343**	**4A177E3CF3D3F03416E9B39D9A535B63BA6EE8A078D17947CF42AF7E9B86F7C2**
A0000000 309000A3 01010010	A0000000 309000A3 01010110	**9EF514D80D310B250DC1C48A79748F65BA30F2A3**	**E311D75874B7155467 5643EDEB634E76EA178780**	**4915B84581B677E9870F4F5E06C0E5E6BB5107F50EB71FD778321FED7B049880**	**2BDAD924E59F5A57877C722BFD53CFF0D65EF066ECED9C9144255CE4D3D05D5**
A0000000 309000A3 01020010	A0000000 309000A3 01020110	**8406cd89d1271bd0794317dd558d2bf92c9afbe8**	**09b0f36db08b57a5278e7b2146d0ec3f244571ed**	**7D3CAA3E134CE6E7E82DDD513C6BD0FCBE4FA1033D6EB6C9916C575A0862079E**	**FB08AF58BAF137BFBB3EC1D6E3DA38FA71235C1716AC9EB3CA232421B54ACD04**
A0000000 309000A3 01030010	A0000000 309000A3 01030110	**0d0a5fdd268828a6cda8b94bd71f8870e51**	**72d2e8a2e7c657537fe2b16dfb63a0**	**477AC4DF3F1E67465546BA23E07286A91C9ED8E15D4E265718DD14717**	**28DB23C8BD12317D1E1CB592B18C90E55CE4EF8BD7D9F9E86F**

[1] Fichiers correspondant à des adaptations de fichiers CAP en vue de leur chargement en environnement mobile.

		28e3d	**7708224934**	**962BEF6**	**5A11EE17E20**
A0000000 3090 00A30104 0010	A0000000 3090 00A30104 0110	**7a5aa96dcdc6 4e3b15b55d6 e04cd1717bde 48cd3**	**d1fbd54d29 f10deb6613 af6b0c3404 6f57b82b6e**	**C9406D97AA9B1E8A65 EA31A9E40548AE4F4F8 792F3C6A5A02F293B3F 9F949E40**	**FF9F84188D78B40CA 66176BDBFAA2F96D F535AF573EBFF3AE D764AAC13B4A834**
A0000000 309000A3 01050010	A0000000 309000A3 01050110	**39696b46784e 65ebadfd37ba 76db94dc34c 4140c**	**6a2ccae8a5 1c2e4d3c34 6859b0c8ba acf7801090**	**7BC6E9AF127D2667AE 46CDFE8BEC4B3E3562 65E98510B087011D165D D904DCD9**	**0691AEE44826CCAA BE45E3AA3C358EA6 C65EF6C18E67DA9C 14611F0DA43A075D**
A0000000 309000A3 01060010	A0000000 309000A3 01060110	**41a90f264423 6313e702a756 4df2bcf4f0b5 23d0**	**00ddee8ef7 15f224b353 53bf64d3da f3b8b77dfd**	**7FC59A2755CEE1372B0 4BCF699B05F28F36D10 5664463510C7EA116D85 F7EC64**	**B370BB8AD01486CD 0D6494B75EE2F29066 C9A27C873976A2E0B C583B833B7F90**
A0000000 3090 00A30107 0010	A0000000 3090 00A30107 0110	**9afe3ab6c657 669ce4b8f8af 7a673bad5b3 91462**	**833f92007b 9ba1913608 c58d09de18 33b1bff1f6**	**24DAB02482AF9AF6620 64ABEBDDD729BE9E24 D0C673E139F5884725D D601131A**	**C5897BE5973693360A 3DD7ABFBEE1A4C7 D4363FC597524C6C2 36AE9981A9074F**
A0000000 3052F114 65390110	A0000000 3052F1146 5390100	**D58C5450902 E08B608DBF 44D25DAD4F 48E279ADF**	**51CC9BFB 0844A8BB CDE5966F 24E508D1E 0EF74D3**	**A950B89E9E97C54AAC ECC1E1573046EC89189 58603A3E7BDE564E198 50DA5901**	**3B832D9CF55FCF36E 88B0CD9F55685F9E5 A45BA372B2723F0B1 8793C001567E8**
A0000000 3052F114 65450110	A0000000 3052F1146 5450100	**475AB0CA04 AA8D0BE624 288BAD7158 7E38ECA502**	**8CA780CE DA1B5DE EDD8F966 415757EFB FD9BC85E**	**15F7D97538E85F3FC4A 1D0A12637DDF79D43E0 D3675CFD205D347F7AF 9E042E2**	**48410B29B60093B732 3ACE1B733D6A06149 509A0D46C309BD43C F4963326B2A8**
A0000000 3052F114 65460110	A0000000 3052F1146 5460100	**EEE30207E2 BFA9B7375D 412F251A9E1 77CCB509C**	**60BD86064 521F67CB A21B976A 7E0766F08 D5D355**	**AC490A97A9F31609463 78449F2F7AD7A5C624D 1D5C061A145628257CF 0D9922C**	**AB971171853B77A1B 2C80B80FB9665B82A 09B24456EC33F56AA 673A9A17C3305**
A0000000 3052F114 65470110	A0000000 3052F1146 5470100	**B183163167A 43DD7D6A17 F897CAF339 B9F887AE9**	**0BDEAE5F 0E295FF13 2DBC6851 E1078F1A DADEB34**	**6A7AD37EBBA8AA05C 6093711D99EA681D664 B84D975F8DE923BB246 76EC828E0**	**8375F495DBCD3DA7 C704EFB9C2042217C 43E4E9D7A BF5DC876F232309 FC04143**
A0000000 3052F114 65480110	A0000000 3052F1146 5480100	**9621EA13F54 D268C3D051 5FA6F4ADF2 07324658**	**A6332C601 2E3AB3B6 0BF18E8E F78C59BC 5180058**	**78100D8F6A5F7638350A 0F2BBE1F76FC2B013A F1F65D426ED831A0DF CA870A6D**	**5B5FB5E2D3EB5DF2 5E9F45B6527FCED01 A6ECE511E467B9066 DB3964CFFA2515**
A0000000 3052F114 65490110	A0000000 3052F1146 5490100	**2F2E5ADC35 00E9D9A196 CB52D36D11 182005FAE6**	**0641140747 074496D19 BC62F9F9 87EC92A8 4473F**	**2625F1505EED8A156B7 C2EB72C9CBD9EFE376 35FC7241C2D9241B1D5 D39269CB**	**C1AFD060F9622F8B0 3D16024B0EB7D9D99 667105C477FDEC597 FDF177696271C**
A0000000 3052F114 65500110	A0000000 3052F1146 5500100	**4E268CE244 C8DF3F78C2 77FF657075B F2EEB845F**	**BEE7B74D 214F465DF 030F9FDC 9D16A2F22 2CF1A8**	**0D92B6536D89A0E771D DE68AF88B755470FD03 11FE8ECAACC0E8AD7 FF9417DF1**	**E77838251074C59899 F77437F58D6BC16155 29AE5810657B283555 9942589A5D**
A0000000 3052F114 65520110	A0000000 3052F1146 5520100	**0740F3A5823 0F65BFEAF0 8B9A36FE41 B3B72C0C9**	**DDE37B7F 5BC19F960 2FAAA652 699AC9C0 F9FB721**	**24F7EB887E795C547B8 E9F06D06E6FBEFB110 C8EF8063993D1D04B98 AF64066E**	**A413E9B2F3F786D0B 5EAF59CA376B895E7 BB6B492A359C61670 A413D570C059D**

- applications CREL Payez Mobile et PPSE :

	SHA1 – CAP File	SHA1 – IJC File	MD5 - CAP File	MD5 - IJC File
PayezMobile	**6d 0f f7 f5 4f f0 15 26 66 03 ac da 3f d8 2a 59 3a 78 17 d4**	**7f 5c 9c 3a 4e d5 4a 7b 07 42 6a 6e 53 cb 89 d2 b6 7c ed 8c**	**c3 c7 3d 93 a2 0f e9 d0 8b 3c 36 48 7d 37 c9 a3**	**2d 10 4b 55 a2 fc 36 5e a1 f1 83ba 04 b8 76 c4**
PPSE	**22 93 b6 44 ef 13 14 7f 7a df 50 8d 62 5f 10 2d 16 08 cd 0f**	**3c e7 bf 09 6d 03 38 49 ef bf 2b c9 f4 b4 4b 70 95 ca db 98**	**97 71 5b 8f 70 02 7d 7a 29 c8 47 2d fc 7e 72 99**	**fb be 43 6d 7e 1a a4 bb 23 0a c3 af 48 46 df b6**

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

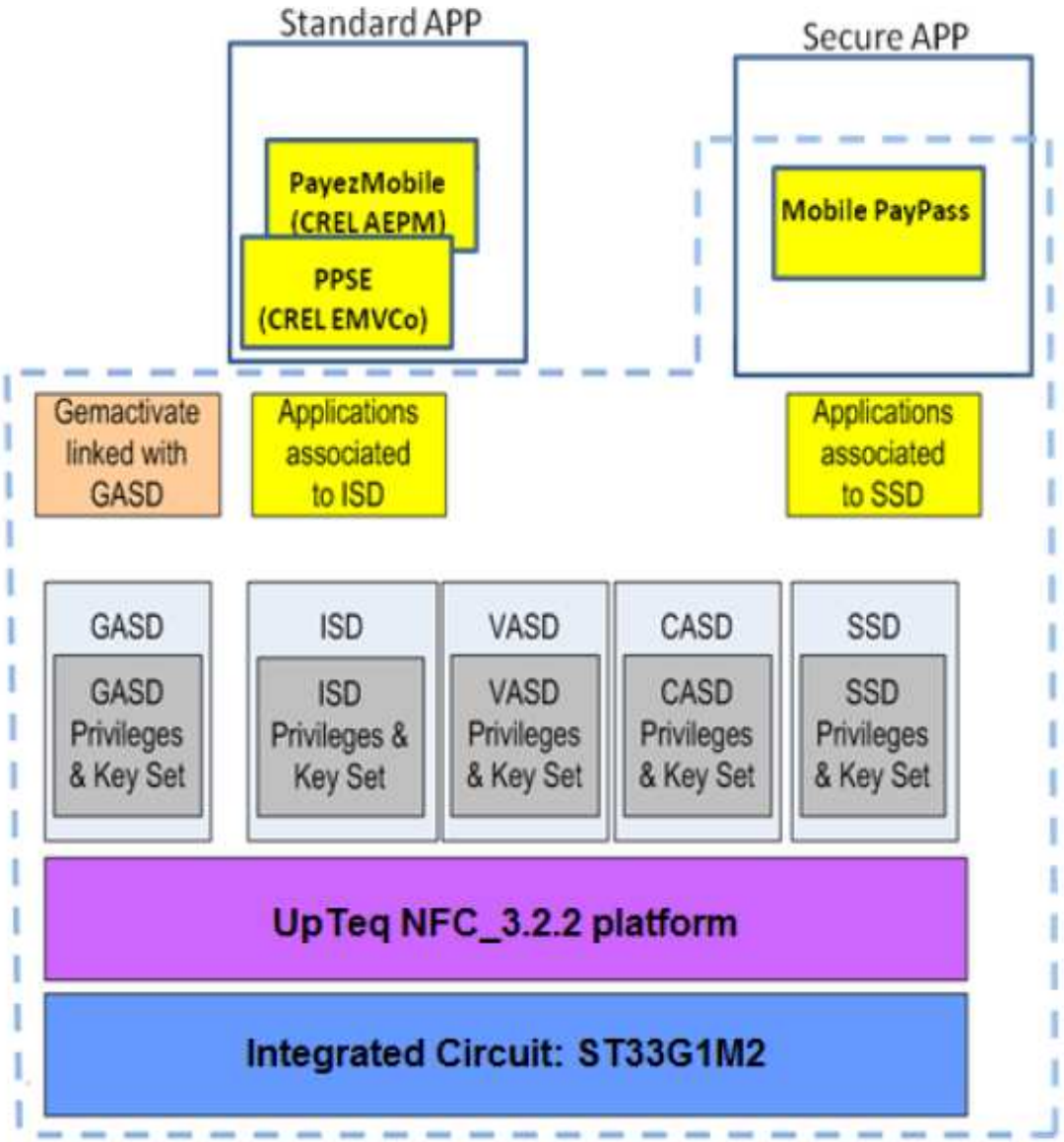
- ceux fournis par la plateforme (U)SIM précédemment certifiée, voir [ANSSI-CC-2016/22] ;
- ceux de l'application Mobile PayPass :
  - la communication hors ligne avec le terminal de paiement (POS, *Point Of Sale*) ;
  - l'authentification hors ligne ;
  - l'authentification en ligne et la communication avec la banque émettrice de la carte ;
  - la vérification et la gestion du code personnel ;
  - la gestion de risque transactionnel ;
  - la certification des transactions ;
  - le traitement de la remise à zéro des compteurs ;
  - le traitement de scripts reçus par OTA (*Over-The-Air*) ;
  - l'audit ;
  - la lecture et la mise à jour des journaux d'audit ;
  - la gestion du cycle de vie sans contact de l'application.

1.2.4. Architecture

Le produit est composé des éléments suivants :

- le microcontrôleur ST33G1M2-F ;
- un système JavaCard qui gère et exécute des applications. Il fournit également des interfaces de programmation (API) pour développer des applications conformes aux spécifications Java Card destinées à être chargées sur ce produit ;
- un package *Global Platform* qui fournit une interface de communication avec la carte à puce et permet de gérer des applications de façon sécurisée ;
- des API plateforme qui fournissent des mécanismes pour interagir avec des applications (U)SIM ;
- un environnement télécom comprenant l'authentification réseau des applications (non évalué) et des protocoles de communication ;
- l'application GemActivate qui permet l'activation de services post-émission[1] ;
- l'application sécuritaire Mobile PayPass v1.0.13vA.2.4 ;
- les applications standard (également dénommées applications basiques) PPSE et CREL PayezMobile.

[1] Chargement réalisé après la phase 7 du cycle de vie de la carte. Correspond au terme *post-issuance* en anglais.



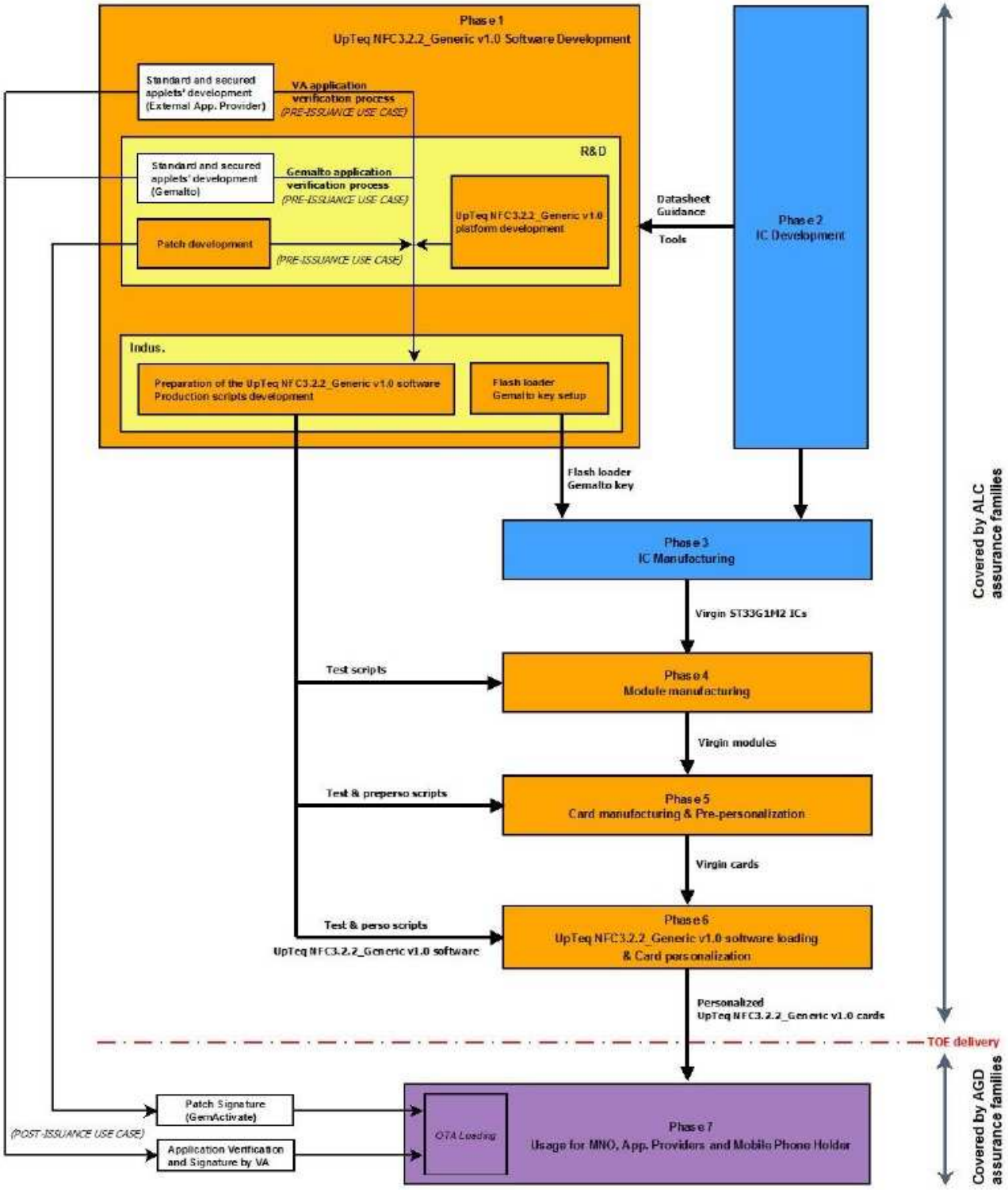
Dans la figure précédente, les pointillés détourent la cible d'évaluation (TOE, *Target Of Evaluation*). La différence entre le produit et la TOE correspond aux applications standards CREL PayezMobile et PPSE chargées sur cette carte à puce.

Bien que ces applications standards ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet la conformité de ces deux applications standard a été vérifiée conformément aux contraintes de développement d'applications décrites dans le rapport de certification [ANSSI-CC-2016/22].

Les applications déjà chargées dans le produit sont toutes identifiées dans le document [App_list].

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :



Les sites de développement et de production du microcontrôleur et de la plateforme sont identifiés dans le rapport de certification [ANSSI-CC-2016/22].

Les applications Mobile PayPas, CREL PayezMobile et PPSE ont été développées sur le site *GEMALTO* suivant :

- 12 Ayar Rajah Crescent
  Singapour 139941
  Singapour

Les applications standards CREL PayezMobile et PPSE peuvent être chargées de deux façons sur cette carte :

- pré-émission[1] (i.e. avant diffusion de la carte à l'utilisateur final) conformément aux processus audités de *GEMALTO* identifiés dans le rapport de certification [ANSSI-CC-2016/22] ;
- ou post-émission à travers le réseau de l'opérateur mobile (chargement via le réseau de communication[2]). Le responsable du processus de chargement doit alors se référer au chapitre 1.2.2 du présent rapport de certification pour vérifier, avant signature de l'application et diffusion aux cartes (U)SIM, que l'application à charger correspond à l'une de celles ayant été vérifiées au cours de cette évaluation.

1.2.6. Configuration évaluée

Le certificat porte sur les configurations suivantes du produit :

- « Carte Mobile PayPass 1.0 sur plateforme Mobile PayPass 1.0.13vA.2.4 (S1133159, release B) sur plateforme UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F **Configuration Mastercard EMVCo** », qui contient l'application sécuritaire Mobile Paypass v1.0.13vA.2.4 et l'application standard PPSE v1.0.4 ;
- « Carte Mobile PayPass 1.0 sur plateforme Mobile PayPass 1.0.13vA.2.4 (S1133159, release B) sur plateforme UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F - **Configuration AEPM France/WW** », qui contient l'application sécuritaire Mobile Paypass v1.0.13vA.2.4 et les applications standards CREL PayezMobile v1.0.1 et PPSE v1.0.4.

Ces deux configurations du produit ont été prises en compte par le CESTI dans le cadre de cette évaluation.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2, et réalisé selon les processus audités si le chargement est réalisé pré-émission, ne remet pas en cause le présent rapport de certification.

[1] Chargement réalisé avant la phase 7 du cycle de vie de la carte. Correspond au terme *pré-issuance* en anglais.
[2] *Over-The-Air* (OTA).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Le niveau VAN est ainsi calculé selon l'échelle de cotation de [JIWG AP], qui est plus exigeante que celle définie par défaut dans la méthode standard [CC] utilisée pour les autres catégories de produits (produits logiciels par exemple).

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 sur la plateforme déjà certifiée par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la « Carte UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F » au niveau EAL4 augmenté des composants, ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PPUSIMB]. Cette plateforme a été certifiée sous la référence [ANSSI-CC-2016/22].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 mai 2016, 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 le référentiel technique de l'ANSSI [REF-CRY] 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 a été étudié dans le cadre de l'évaluation de la plateforme (voir [ANSSI-CC-2016/22]).

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 « Carte Mobile PayPass 1.0.13vA.2.4 (S1133159, release B) sur plateforme UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F, S1133159, release B » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur 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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides [GUIDES] et [GUIDES-PF]. En particulier :

- les développeurs d'applications additionnelles sur la carte doivent appliquer le guide de développement d'applications basiques [AGD-Dev_Basic] ou le guide de développement d'applications sécurisées [AGD-Dev_Sec], selon la sensibilité des applications concernées ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA].

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'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 EAL2 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, 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 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	**2**	Sufficiency of security measures
	ALC_FLR									
	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 Evaluation de la cible de sécurité	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	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - « Mobile PayPass 1.0.13vA.2.4 on UpTeq NFC3.2.2_Generic v1.0 platform – Security target », référence D1350241, version 1.2.
[RTE]	Rapport technique d'évaluation : - « Evaluation technical report – RIGEL Project », référence RIGEL_ETR_MPP_v1.2, révision 1.2.
[CONF]	Liste de configuration - « LIS_MPPv1_AEPMv3__1-115-1-4 », 19 mai 2016. Liste des applications et *packages* vérifiées [App_list] : - Profile name: Max DES MPP, référence : « D1349732_ProfileDescription_MaxDES_MPP1013 v1.0 for UpTeq NFC 3.2.2_Generic v1.0 ».
[GUIDES]	Guide de préparation du produit : - « Mobile Paypass 1.0.13vA.2.4 onUpTeq NFC3.2.2_Generic v1.0 platform - Preparation Guidance », référence D1357242, release 1.0 ; - « Mobile MasterCard Paypass – Card Applications V1.0 - Installation Guide », référence D1294923, version B-6 ; Guides opérationnel du produit : - « Mobile Paypass 1.0.13vA.2.4 on UpTeq NFC3.2.2_Generic v1.0 platform - Guidance for administration", référence D1357097, release 1.0 ; - « Mobile MasterCard Paypass Card Applications V1.0 - Administration Guide », référence D1294924, version B-4 ; - « Mobile MasterCard Paypass Card Applications V1.0, Developing Client Applications Guide », référence D1294921, version B-4.
[GUIDES-PF]	Guide de préparation : - Guide de réception et d'installation [AGD-PRE] : « UpTeq NFC3.X platform – Preparation Guidance », référence D1351549, release 1.1 ; Guides opérationnels du produit : - Guides d'administration [AGD-OPE] : • « Guidance for administration of Upteq NFC 3.X platform with Controlling Authority and Optional Verification Authority », référence D1341170_w_CA, release 1.1 ; • « Guidance for administration of Upteq NFC 3.X platform without Controlling Authority and Optional Verification Authority », référence D1341170_wo_CA, release 1.1 ; - Guide pour l'autorité de vérification [AGD-OPE_VA] :

	• « Guidance for Verification Authority for Upteq NFC 3.X platform », référence D1341169_VA, release 1.0 ; - Guide de développement d'applications • Guide [AGD_APP]: « Applications management for certified Secure Elements », référence D1258682, release C01 ; • Guide de développement d'applications basiques [AGD-Dev_Basic]: « GlobalPlatform Card – Composition Model Security Guidelines for Basic Applications », référence GPC_GUI_050, version 2.0 ; • Guide de développement d'applications sécuritaires [AGD-Dev_Sec] : « Guidance for secure application development on Upteq NFC platforms », référence D1188231, release A13.1 ; - Patch loading Management for certified Secure Element, référence D1344508, release A00.
[PPUSIMB]	(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations (Basic configuration), référence PU-2009-RT-79, version 2.0.2, 17 juin 2010. Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/04.
[ANSSI-CC-2016/22]	Carte UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F. Certifiée par l'ANSSI sous la référence ANSSI-CC- 2016/22.

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, janvier 2012.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
[OPEN]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.