
PREMIER MINISTRE

**SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE**

SERVICE CENTRAL DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Schéma Français
d'Évaluation et de Certification
de la Sécurité des Technologies de l'Information

---

# Rapport de certification 2000/08

Application GemVision Smart D/C masquée sur le composant ST19SF08AC
(Référence ST19SF08AC/RMY)

Décembre 2000

Ce document constitue le rapport de certification du produit “Application GemVision Smart D/C masquée sur le composant ST19SF08AC (Référence ST19SF08AC/RMY)”.

Ce rapport de certification est disponible sur le site internet du Service Central de la Sécurité des Systèmes d'Information à l'adresse suivante :

www.scssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

Secrétariat général de la défense nationale
SCSSI
Centre de Certification de la Sécurité des Technologies de l’Information
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Mél: ssi20@calva.net



Ce document est folioté de 1 à 28 et certificat.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

Schéma Français
d'Évaluation et de Certification
de la Sécurité des Technologies de l'Information

# CERTIFICAT 2000/08

## Application GemVision Smart D/C masquée sur le composant ST19SF08AC (Référence ST19SF08AC/RMY)

**Développeur : Gemplus**

## EAL4 augmenté

## Commanditaires : Gemplus, STMicroelectronics SA

Le 14 février 2001,

Les Commanditaires :
Le Directeur de la Division bancaire de Gemplus
M. Sami BAGHDADI

Group Vice-President
Memory Products
General Manager Smartcard Products Division
M. Maurizio FELICI

L'Organisme de certification :
Le Directeur chargé de la sécurité des systèmes d'information
M. Henri SERRES

*Ce produit a été évalué par un centre d'évaluation de la sécurité des TI conformément aux critères communs pour l'évaluation de la sécurité des TI version 2.1 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 1.0.*

*Ce certificat ne s'applique qu'à la version évaluée du produit dans sa configuration d'évaluation et selon les modalités décrites dans le rapport de certification associé. L'évaluation a été conduite en conformité avec les dispositions du Schéma français d'évaluation et de certification de la sécurité des TI. Les conclusions du centre d'évaluation enregistrées dans le rapport technique d'évaluation sont cohérentes avec les éléments de preuve fournis.*

*Ce certificat ne constitue pas en soi une recommandation du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise. Ce certificat n'exprime directement ou indirectement aucune caution du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.*

Organisme de certification :
Secrétariat général de la défense nationale
SCSSI
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

IT Security Certified

Common Criteria

## Chapitre 1

# Introduction

1 Ce document représente le rapport de certification du produit “Application GemVision Smart D/C masquée sur le composant ST19SF08AC (Référence ST19SF08AC/RMY)”. Cette application, développée par Gemplus, a été conçue pour être conforme aux spécifications EMV [8].

2 Le niveau d’assurance atteint est le niveau EAL4 augmenté des composants d’assurance ADV_IMP.2 “Implémentation de la TSF”, ALC_DVS.2 “Caractère suffisant des mesures de sécurité” et AVA_VLA.4 “Résistance élevée” tels que décrits dans la partie 3 des Critères Communs [3]. Par ailleurs, la résistance des fonctions de sécurité est cotée élevée (SOF-high).

3 Ce produit est conforme au profil de protection “Smartcard Embedded Software” enregistré auprès du SCSSI dans le catalogue des profils de protection certifiés sous la référence PP/9810 [9].

# Chapitre 2

# Résumé

## 2.1 Contexte de l'évaluation

4 L'évaluation a été menée conformément aux Critères Communs ([1] à [3]) et à la méthodologie définie dans le manuel CEM [4].

5 Elle s'est déroulée consécutivement au développement du produit de mars 1999 à novembre 2000.

6 Le développeur de la cible d'évaluation est Gemplus (ci-après "le développeur") :

- Gemplus
  Parc d'Activités de Gémenos
  B.P. 100
  F-13881 Gémenos Cedex.

7 Le masquage de l'application sur le composant ST19SF08AC est réalisé par STMicroelectronics (ci-après le "fondeur") :

- STMicroelectronics SA
  ZI de Rousset
  BP2
  F-13106 Rousset Cedex.

8 En particulier, la cible d'évaluation a été fabriquée par le fondeur sur le site suivant :

- STMicroelectronics SRL
  Via C. Olivetti 2
  I-20041 Agrate Brianza.

9 Le développeur et le fondeur sont co-commanditaires de l'évaluation (ci-après "les commanditaires") :

- Gemplus
  Parc d'Activités de Gémenos
  B.P. 100
  F-13881 Gémenos Cedex,

- ST Microelectronics SA
  ZI de Rousset
  BP2
  F-13106 Rousset Cedex.

10 L'évaluation a été conduite par les centres d'évaluation de la sécurité des technologies de l'information (ci-après "CESTI") :

- AQL
  Rue de la Châtaigneraie
  B.P. 127
  F-35513 Cesson Sévigné,

- Serma Technologies
  30, avenue Gustave Eiffel
  F-33608 Pessac Cedex.

11 Cette évaluation a fait intervenir deux CESTI pour respecter les contraintes imposées par leurs portées d'agrément respectives.

## 2.2 Description de la cible d'évaluation

12 La cible d'évaluation est le produit "Application GemVision Smart D/C masquée sur le composant ST19SF08AC (Référence ST19SF08AC/RMY)".

13 Ce produit est conforme au profil de protection "Smartcard Embedded Software" enregistré auprès du SCSSI dans le catalogue des profils de protection certifiés sous la référence PP/9810 [9].

14 Le détail des fonctions de sécurité évaluées résumées ci-après est disponible dans la cible de sécurité [5] :

- signature de transactions,
- authentification des utilisateurs de la carte,
- confidentialité et intégrité des clés, des codes secrets (PIN) et du logiciel,
- protection des fichiers de données par gestion du contrôle d'accès.

## 2.3 Conclusions de l'évaluation

15 Le produit soumis à évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance ADV_IMP.2 "Implémentation de la TSF", ALC_DVS.2 "Caractère suffisant des mesures de sécurité" et AVA_VLA.4 "Résistance élevée" tels que décrits dans la partie 3 des Critères Communs [3]. Par ailleurs, la résistance des fonctions de sécurité est cotée élevée (SOF-high).

16 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL4 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élevé tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.

17 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

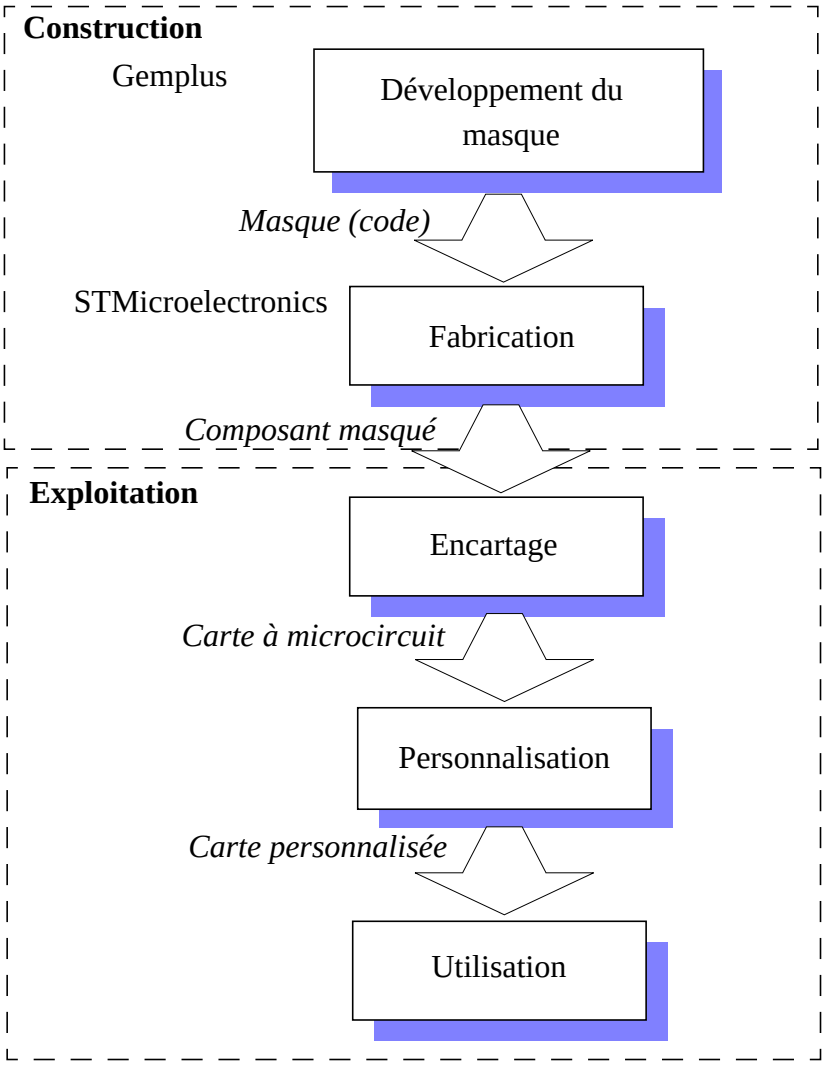
# Chapitre 3

# Identification de la cible d'évaluation

## 3.1 Objet

18 La cible d'évaluation est l'"Application GemVision Smart D/C masquée sur le composant ST19SF08AC (Référence ST19SF08AC/RMY)" développée par Gemplus sur le site de Gémenos, et masquée sur le composant ST19SF08AC par STMicroelectronics sur le site de Agrate.

## 3.2 Cycle de vie



19 La cible d'évaluation est le masque (logiciel embarqué constitué de l'application GemVision Smart D/C) sur le composant ST19SF08AC. L'évaluation porte sur les fonctions de sécurité de l'application GemVision Smart D/C mises en œuvre pendant les phases d'exploitation, mais développées pendant la phase *Développement du masque*.

20 Il s'agit donc d'une évaluation du type composant masqué dans laquelle le composant est considéré comme une boîte noire. La construction de la cible d'évaluation est constituée de la phase *Développement du masque*, incluant la livraison du logiciel au fondeur, et de la phase *Fabrication*.

## 3.3 Description du matériel

21 L'application GemVision Smart D/C est masquée sur le composant ST19SF08AC produit par STMicroelectronics dont elle utilise certains mécanismes de sécurité. Ce composant n'est pas inclus dans la cible d'évaluation.

22 Ce microcircuit électronique est un microcontrôleur de la famille des composants ST19SFxx. Cette famille est couverte par un programme de maintenance entre STMicroelectronics et le CESTI de Serma technologies, référencé PM 2000/01.

## 3.4 Description du logiciel

23 La cible d'évaluation est constituée du logiciel GemVision Smart D/C, référence MST099.

24 La cible d'évaluation ne contient pas de filtre, c'est-à-dire de code chargé en EEPROM qui pourrait être utilisé pour compléter ou modifier la fonctionnalité de la carte.

## 3.5 Description de la documentation

25 La documentation d'exploitation de la cible d'évaluation est la suivante :

- guide d'utilisation [11] ;
- guide d'administration [12].

# Chapitre 4

# Caractéristiques de sécurité

## 4.1 Préambule

26 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [5] qui est la référence pour l'évaluation. Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

## 4.2 Hypothèses

27 La cible d'évaluation doit être utilisée dans un environnement qui satisfait aux hypothèses énoncées dans le profil de protection [9], et à des hypothèses complémentaires concernant sa phase d'exploitation.

28 Ces hypothèses énoncées dans le profil de protection couvrent les aspects suivants :

- livraison de la cible d'évaluation entre les différentes étapes de son cycle de vie,
- développement du microcircuit sur lequel l'application sera masquée,
- utilisation de la cible d'évaluation pendant les phases de production (phases d'*encartage* et de *personnalisation)*,
- protection des données sensibles de la cible d'évaluation échangées avec les équipements avec lesquels elle dialogue (terminaux, …).

29 Les hypothèses complémentaires énoncées dans la cible de sécurité [5] couvrent les aspects suivants :

- protection du PIN et des clés secrètes,
- unicité des cartes et limitation de leur validité à 3 ans,
- enregistrement des transactions.

30 Le détail de ces hypothèses est disponible dans le profil de protection [9] et dans la cible de sécurité [5].

## 4.3 Menaces

31 Les menaces couvertes par la cible d'évaluation ou par son environnement sont celles définies par le profil de protection [9].

32 Les biens à protéger sont les spécifications, la conception, les outils de développement et la technologie des logiciels, les logiciels embarqués ainsi que les données applicatives de la carte.

33 Les principales menaces portent sur la divulgation et la modification non autorisées des biens de la cible d'évaluation. Le détail de ces menaces est disponible dans le profil de protection [9].

## 4.4 Politiques de sécurité organisationnelles

34 Le profil de protection ne définit pas de politique de sécurité organisationnelle.

35 La cible de sécurité définit une politique, imposant que l'application soit masquée sur un composant basé sur le profil de protection "Smartcard Integrated Circuit" enregistré auprès du SCSSI dans le catalogue des profils de protection certifiés sous la référence PP/9806 [10], et qu'elle respecte le guide d'utilisation de ce composant.

## 4.5 Fonctions de sécurité évaluées

36 Les fonctions de sécurité évaluées sont décrites ci-dessous. Le détail de ces fonctions est disponible dans la cible de sécurité [5].

### 4.5.1 Contrôle d'accès aux données :

37 Cette fonction assure la gestion des données stockées.

### 4.5.2 Authentification de l'administrateur :

38 Cette fonction assure la gestion de l'authentification de l'administrateur. En fonction de la phase du cycle de vie concernée, le mécanisme d'authentification utilisé est différent.

39 Le nombre de tentatives d'authentification est limité par un compteur de ratification.

### 4.5.3 Gestion des sauvegardes :

40 Cette fonction assure la gestion des données secrètes mises à jour en EEPROM :

- elle stocke dans une zone mémoire dédiée les données sensibles avant leur mise à jour ;
- elle invalide ces données copiées une fois que la mise à jour s'est déroulée avec succès ;
- elle restaure les données secrètes en cas de mise à jour infructueuse.

### 4.5.4 Gestion des commandes :

41 Cette fonction contrôle l'exécution du processus interne à la carte en réponse aux commandes envoyées par l'utilisateur.

### 4.5.5 Comparaison sûre :

42 Cette fonction garantit que l'opération de comparaison entre deux données est inobservable.

### 4.5.6 Calculs cryptographiques :

43 Les opérations cryptographiques suivantes sont mises en œuvre :

- génération de clés de session ;
- déchiffrement des données ;
- calcul de MAC.

### 4.5.7 Pilotage du microcircuit :

44 Cette fonction assure la gestion des caractéristiques de sécurité du microcircuit :

- analyse de l'état de la carte au démarrage ;
- enregistrement des évènements d'audit ;
- réaction suite à une violation potentielle de la sécurité ;
- contrôle de la fréquence d'horloge utilisée.

### 4.5.8 Intégrité des données :

45 Cette fonction permet de vérifier l'intégrité de certaines données stockées en EEPROM (PIN, clés, …).

### 4.5.9 Gestion des clés cryptographiques :

46 Cette fonction contrôle toutes les opérations relatives à la gestion des clés cryptographiques : création, recherche et lecture, ratification et destruction des clés.

### 4.5.10 Gestion des phases de vie de la carte :

47 Cette fonction assure la gestion des différentes phases de vie de la carte, elle en garantit la chronologie et interdit tout retour à une phase antérieure.

### 4.5.11 Gestion du PIN :

48 Cette fonction contrôle toutes les opérations relatives à la gestion du PIN (recherche, déblocage et modification), y compris l'authentification du porteur de la carte.

### 4.5.12 Gestion des ratifications :

49 Cette fonction assure la gestion des compteurs de ratification associés au PIN et aux clés cryptographiques :

- lecture du compteur de ratification ;
- décrémentation du compteur ;

- positionnement du compteur à sa valeur maximale.

### 4.5.13 Gestion de la sécurité :

50 Cette fonction maintient les attributs de sécurité des utilisateurs.

### 4.5.14 Chargement sûr des données secrètes :

51 Cette fonction assure la protection en intégrité et confidentialité du PIN pendant son chargement et sa mise à jour. Elle assure également la protection en intégrité et confidentialité des clés pendant leur chargement.

### 4.5.15 Autotest :

52 Cette fonction permet :

- de vérifier au démarrage d'une session que la RAM fonctionne correctement ;
- de vérifier une signature numérique du code en ROM,
- de vérifier la configuration de la carte.

# Chapitre 5

# Résultats de l'évaluation

## 5.1 Rapport Technique d'Évaluation

53 Les résultats de l'évaluation sont exposés dans les rapports techniques d'évaluation [6] et [7] produits respectivement par AQL et Serma Technologies.

54 Le composant sur lequel l'application GemVision Smart D/C est masquée, est un microcontrôleur de la famille de composants ST19SFxx couverte par le programme de maintenance PM 2000/01. Les tâches d'évaluation relatives au composant qui auraient dû être conduites dans le cadre de ce projet n'ont donc pas eu lieu ; les aspects correspondant étant traités par le programme de maintenance.

## 5.2 Principaux résultats de l'évaluation

55 Le produit répond aux exigences des Critères Communs pour le niveau EAL4 augmenté des composants d'assurance ADV_IMP.2 "Implémentation de la TSF", ALC_DVS.2 "Caractère suffisant des mesures de sécurité" et AVA_VLA.4 "Résistance élevée" tels que décrits dans la partie 3 des Critères Communs [3]. Par ailleurs, la résistance des fonctions de sécurité est cotée élevée (SOF-high).

### 5.2.1 ASE : Evaluation de la cible de sécurité

56 Les critères d'évaluation sont définis par les sections ASE_DES.1.iE, ASE_ENV.1.iE, ASE_INT.1.iE, ASE_OBJ.1.iE, ASE_PPC.1.iE, ASE_REQ.1.iE, ASE_SRE.1.iE et ASE_TSS.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des Critères Communs [3].

57 La cible d'évaluation est l'"Application GemVision Smart D/C masquée sur le composant ST19SF08AC (Référence ST19SF08AC/RMY)", développée par Gemplus.

58 Les travaux d'évaluation de la cible de sécurité ont pu être facilités du fait de sa conformité à un profil de protection [9] certifié.

### 5.2.2 ACM_AUT.1 : Automatisation partielle de la gestion de configuration

59 Les critères d'évaluation sont définis par la section ACM_AUT.1.1E de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

60 Le développeur a fourni la documentation du système de gestion de configuration utilisé pour le développement de l'application par Gemplus.

61 Le système est fondé sur une gestion automatique de la configuration à travers un outil de gestion de configuration permettant de s'assurer que seuls les changements autorisés sur le produit sont possibles.

62 L'évaluateur a analysé la documentation et vérifié au cours de l'audit du site de développement l'utilisation effective de l'outil de gestion de configuration, en accord avec les procédures du développeur.

63 Les aspects relatifs à la gestion de configuration de la cible d'évaluation lors de la phase *Fabrication* sont couverts par le programme de maintenance PM 2000/01.

### 5.2.3 ACM_CAP.4 : Aide à la génération et procédures de réception

64 Les critères d'évaluation sont définis par la section ACM_CAP.4.iE de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

65 Le développeur a fourni la documentation du système de gestion de configuration.

66 Ce système impose un contrôle des objets produits au cours du développement chez le développeur. Des procédures permettent de prendre en compte dans le système de gestion de configuration les objets composant la cible d'évaluation (procédure de réception).

67 L'évaluateur a vérifié au cours de l'audit du site de développement que les procédures décrites étaient effectivement appliquées.

68 Les aspects relatifs à la gestion de configuration de la cible d'évaluation lors de la phase *Fabrication* sont couverts par le programme de maintenance PM 2000/01.

### 5.2.4 ACM_SCP.2 : Couverture du suivi des problèmes par la CM

69 Les critères d'évaluation sont définis par la section ACM_SCP.2.1E de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

70 Le système de gestion de configuration appliquée par le développeur couvre la cible d'évaluation ainsi que l'ensemble de sa documentation (documentation de conception et éléments de réalisation, documentation de test, documentation d'utilisation et d'administration) ; il couvre également toute erreur de sécurité du produit qui pourrait être découverte.

71 Les aspects relatifs à la gestion de configuration de la cible d'évaluation lors de la phase *Fabrication* sont couverts par le programme de maintenance PM 2000/01.

### 5.2.5 ADO_DEL.2 : Détection de modifications

72 Les critères d'évaluation sont définis par la section ADO_DEL.2.iE de la classe ADO, telle que spécifiée dans la partie 3 des Critères Communs [3].

73 Le développeur a fourni les procédures de livraison de la cible d'évaluation au fondeur. Celles-ci ont été vérifiées au cours de l'audit du site de développement.

74 Les aspects relatifs à la livraison de la cible d'évaluation en sortie de la phase *Fabrication* sont couverts par le programme de maintenance PM 2000/01.

### 5.2.6 ADO_IGS.1 : Procédures d'installation, de génération et de démarrage

75 Les critères d'évaluation sont définis par les sections ADO_IGS.1.iE de la classe ADO, telle que spécifiée dans la partie 3 des Critères Communs [3].

76 Les procédures d'installation, de génération et de démarrage pour ce type de cible d'évaluation se limitent à la procédure de mise sous tension.

77 L'évaluateur a vérifié que l'ATR renvoyé par la carte à la mise sous tension était conforme à l'ATR décrit dans la documentation fournie par le développeur.

### 5.2.7 ADV_FSP.2 : Définition exhaustive des interfaces externes

78 Les critères d'évaluation sont définis par les sections ADV_FSP.2.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

79 Le développeur a fourni la documentation spécifiant les fonctions de sécurité du produit et leurs interfaces externes.

80 L'évaluateur a examiné ces spécifications et montré qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du produit.

### 5.2.8 ADV_HLD.2 : Conception de haut niveau - identification des sous-systèmes dédiés à la sécurité

81 Les critères d'évaluation sont définis par les sections ADV_HLD.2.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

82 Le développeur a fourni la conception de haut niveau de la cible d'évaluation.

83 Cette conception présente la structure générale du produit en terme de sous-systèmes. L'évaluateur s'est assuré que cette conception de haut niveau est une instantiation correcte et complète des exigences fonctionnelles de sécurité de la cible d'évaluation.

### 5.2.9 ADV_IMP.2 : Implémentation de la TSF

84 Les critères d'évaluation sont définis par les sections ADV_IMP.2.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

85 Le développeur a fourni l'intégralité du code source de la cible d'évaluation.

86 L'évaluateur s'est assuré que le code source est une instantiation correcte et complète des exigences fonctionnelles de sécurité de la cible d'évaluation.

87 De plus, l'évaluateur a vérifié que l'application GemVision Smart D/C respecte les exigences définies dans le guide d'utilisation du composant fourni par le fondeur [13].

### 5.2.10 ADV_LLD.1 : Conception de bas niveau descriptive

88 Les critères d'évaluation sont définis par les sections ADV_LLD.1.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

89 Le développeur a fourni la conception de bas niveau de la cible d'évaluation.

90 Cette conception décompose chaque sous-système en modules. Ces modules ainsi que leurs interfaces sont décrits. L'évaluateur s'est assuré que cette conception de bas niveau est une instantiation correcte et complète des exigences fonctionnelles de sécurité de la cible d'évaluation.

### 5.2.11 ADV_RCR.1 : Démonstration de correspondance informelle

91 Les critères d'évaluation sont définis par la section ADV_RCR.1.1E de la classe ADV, telle que spécifiée dans la partie 3 des Critères Communs [3].

92 Le développeur a fourni une documentation qui indique les correspondances entre les différents niveaux de représentation des fonctions de sécurité de la cible d'évaluation.

93 L'évaluateur a donc pu s'assurer que les exigences de sécurité fonctionnelles exprimées dans la cible de sécurité sont correctement et complètement implémentées à travers les spécifications fonctionnelles, la conception de haut niveau, la conception de bas niveau et l'implémentation de la cible d'évaluation.

### 5.2.12 ADV_SPM.1 : Modèle informel de politique de sécurité de la TOE

94 Les critères d'évaluation sont définis par les sections ADV_SPM.1.1E de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

95 Le développeur a fourni un modèle informel de politique de sécurité de la cible d'évaluation. Les politiques suivantes sont couvertes par le modèle :

- la politique de contrôle d'accès aux commandes ;
- la politique de contrôle d'accès aux fichiers ;
- la politique de gestion des secrets ;
- la politique de gestion des objets TLV ;
- la politique d'identification et d'authentification ;
- la politique d'audit ;
- la politique de gestion des erreurs.

96 L'évaluateur a examiné ce modèle. Il a montré qu'il fournit une description claire et homogène des règles et caractéristiques des politiques de sécurité, que cette description correspond à la description des fonctions de sécurité dans les spécifications fonctionnelles.

### 5.2.13 AGD_ADM.1 : Guide de l'administrateur

97 Les critères d'évaluation sont définis par la section AGD_ADM.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [3].

98 Le développeur a fourni la documentation d'administration des fonctions de sécurité du produit [12]. Ce guide d'administration est à usage des encarteurs et personnalisateurs (y compris les émetteurs de cartes).

99 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié que ces procédures permettent une administration sûre du produit.

### 5.2.14 AGD_USR.1 : Guide de l'utilisateur

100 Les critères d'évaluation sont définis par la section AGD_USR.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [3].

101 Le développeur a fourni la documentation d'utilisation des fonctions de sécurité du produit [11]. Ce guide d'utilisation est à usage des porteurs de cartes.

102 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié que ces procédures permettent une utilisation sûre du produit.

### 5.2.15 ALC_DVS.2 : Caractère suffisant des mesures de sécurité

103 Les critères d'évaluation sont définis par la section ALC_DVS.2.iE de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

104 Les évaluateurs ont analysé la sécurité des locaux dans lesquels a eu lieu le développement de la cible d'évaluation. Ces locaux, qui appartiennent à Gemplus, sont situés dans la zone sécurisée dédiée à la Recherche et Développement du site de Gémenos.

105 Des procédures physiques, organisationnelles, techniques, liées au personnel assurent la protection en intégrité et en confidentialité de la cible d'évaluation, de ses constituants ainsi que de sa documentation. Un audit du site de Gémenos a permis de vérifier l'application de ces procédures.

106 Les aspects relatifs à la sécurité de l'environnement de construction de la cible d'évaluation lors de la phase *Fabrication* sont couverts par le programme de maintenance PM 2000/01.

### 5.2.16 ALC_LCD.1 : Modèle de cycle de vie défini par le développeur

107 Les critères d'évaluation sont définis par la section ALC_LCD.1.1E de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

108 Le développeur a fourni le modèle de cycle de vie de la cible d'évaluation. Le modèle de développement respecte les exigences définies dans les documents ARGOS 05-xx (05-00 à 05-09).

109 L'évaluateur a analysé ce modèle et s'est assuré de l'absence d'incohérence dans ce modèle.

### 5.2.17 ALC_TAT.1 : Outils de développement bien définis

110 Les critères d'évaluation sont définis par la section ALC_TAT.1.iE de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

111 Le développeur a fourni la documentation relative aux outils de développement de la cible d'évaluation.

112 Le développement de la cible d'évaluation est réalisé à l'aide de deux langages de programmation : le langage C respectant la norme ANSI/ISO 9899-1990 et le langage assembleur 6805 dont les commandes sont définies dans le manuel référencé HI-ASM/ST7/Assembler.

113 L'application est masquée sur un composant issu de la famille ST19SFxx, le développeur a donc utilisé le manuel de programmation fourni par le fondeur, qui décrit le jeu d'instructions du composant ainsi que les différents modes d'adressage.

114 L'évaluateur a vérifié que les outils de développement utilisés sont bien définis.

### 5.2.18 ATE_COV.2 : Analyse de la couverture

115 Les critères d'évaluation sont définis par la section ATE_COV.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

116 Le développeur a fourni une analyse de la documentation de test justifiant la couverture de la spécification des fonctions de sécurité par des tests.

117 L'évaluateur a vérifié que pour chaque aspect des fonctions de sécurité, le développeur a défini au minimum un test.

### 5.2.19 ATE_DPT.1 : Tests : conception de haut niveau

118 Les critères d'évaluation sont définis par la section ATE_DPT.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

119 Le développeur a fourni une analyse de la documentation de test justifiant la réalisation de tests fonctionnels pour les sous-systèmes identifiés dans la conception de haut niveau de l'application.

120 L'évaluateur a examiné cette documentation et s'est assuré de sa cohérence.

### 5.2.20 ATE_FUN.1 : Tests fonctionnels

121 Les critères d'évaluation sont définis par la section ATE_FUN.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

122 Le développeur a fourni la documentation de test du produit. Les tests fournis correspondent à un ensemble de tests logiciels des fonctions de sécurité de l'application.

123 Une documentation détaillée de test a été fournie pour chacun des tests ; cette documentation décrit le plan des tests, l'objectif des tests, les procédures de tests à réaliser ainsi que les résultats des tests.

124 L'évaluateur s'est assuré de la complétude de cette documentation.

### 5.2.21 ATE_IND.2 : Tests indépendants - échantillonnage

125 Les critères d'évaluation sont définis par les sections ATE_IND.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

126 L'évaluateur a effectué un ensemble de tests sur la cible d'évaluation. Il a procédé à un échantillonnage des programmes de test du développeur. La procédure d'échantillonnage a été jugée conforme aux exigences du niveau d'évaluation EAL4.

127 Des tests complémentaires ont également été effectués par l'évaluateur pour démontrer que les fonctions de sécurité fonctionnent conformément à leurs spécifications.

### 5.2.22 AVA_MSU.2 : Validation de l'analyse

128 Les critères d'évaluation sont définis par la section AVA_MSU.2.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

129 Le développeur a fourni une analyse des guides d'exploitation de la cible d'évaluation. L'objectif de cette analyse est de garantir que des éléments trompeurs, déraisonnables ou contradictoires sont absents de ces guides et que des procédures sûres pour tous les modes d'exploitation de la cible d'évaluation ont été définies.

130 L'évaluateur s'est assuré de la complétude de cette analyse et a appliqué de nouveau ces procédures afin de confirmer que l'utilisation des guides conduit à une utilisation et une configuration sûres de la cible d'évaluation.

### 5.2.23 AVA_SOF.1 : Évaluation de la résistance des fonctions de sécurité de la TOE

131 Les critères d'évaluation sont définis par la section AVA_SOF.1.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

132 Le développeur a fourni une analyse de la résistance des fonctions de sécurité de la cible d'évaluation. Les fonctions pour lesquelles une résistance des fonctions s'appliquent sont :

- authentification de l'administrateur ;
- gestion du PIN (et en particulier authentification du porteur de la carte) ;
- chargement sûr des données secrètes.

133 L'évaluateur a analysé cette documentation et mené des analyses complémentaires. La cotation indépendante faite par l'évaluateur est en accord avec l'analyse du développeur.

134 La résistance des fonctions de sécurité est considérée comme élevée (SOF-high).

### 5.2.24 AVA_VLA.4 : Résistance élevée

135 Les critères d'évaluation sont définis par les sections AVA_VLA.4.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

136 Le développeur a fourni une documentation d'analyse des vulnérabilités potentielles du produit. L' évaluateur a examiné cette fourniture et réalisé sa propre analyse de vulnérabilités indépendante.

137 Les tests de pénétration ont été conduits en deux étapes :

- l'évaluateur a mené des tests sur un échantillon de la cible d'évaluation dans son environnement d'exploitation normal,
- puis l'évaluateur a réalisé des tests en environnement perturbé sur la cible d'évaluation.

138 L'objectif de ces tests de pénétration est de vérifier que la cible d'évaluation résiste aux attaques correspondant à un potentiel élevé de l'attaquant tel que défini par le composant AVA_VLA.4 "Résistance élevée".

### 5.2.25 Verdicts

139 Pour tous les aspects des critères communs identifiés ci-dessus, un avis "réussite" a été émis.

## Chapitre 6

# Recommandations d'utilisation

140 Le produit "Application GemVision Smart D/C masquée sur le composant ST19SF08AC (Référence ST19SF08AC/RMY)" est soumis aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

- le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [5] ;
- le produit doit être utilisé et administré conformément aux guides d'utilisation [11] et d'administration [12] ;
- lors de l'initialisation du produit, les filtres doivent être désactivés ;
- si d'autres applications venaient à être masquées simultanément sur le même composant, alors il faudra veiller à ce que les clés mères utilisées par chacune d'elles soient différentes.

# Chapitre 7

# Certification

## 7.1 Objet

141 Le produit soumis à évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance ADV_IMP.2 "Implémentation de la TSF", ALC_DVS.2 "Caractère suffisant des mesures de sécurité" et AVA_VLA.4 "Résistance élevée" tels que décrits dans la partie 3 des Critères Communs [3]. Par ailleurs, la résistance des fonctions de sécurité est cotée élevée (SOF-high).

142 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL4 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élevé tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.

## 7.2 Portée de la certification

143 La certification ne constitue pas en soi une recommandation du produit. Elle ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

144 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 3.

145 La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

## Annexe A

# Glossaire

| | |
|---|---|
| **Assurance** | Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité. |
| **Augmentation** | L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 des Critères Communs à un EAL ou à un paquet d'assurance. |
| **Biens** | Informations ou ressources à protéger par la cible d'évaluation ou son environnement. |
| **Cible d'évaluation** | Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation. |
| **Cible de sécurité** | Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée. |
| **Emetteur** | Banque ou organisme émetteur de la carte de débit/crédit. |
| **Encarteur** | Industriel insérant le composant masqué dans un support plastique, en forme de carte. |
| **Evaluation** | Estimation d'un profil de protection ou d'une cible d'évaluation par rapport à des critères définis. |
| **Filtre** | Code chargé en EEPROM qui peut être utilisé pour compléter ou modifier la fonctionnalité de la carte. |
| **Logiciel embarqué** | Logiciel présent sur une puce. |
| **Masque** | Ensemble d'instructions organisées, reconnaissables et exécutables par le processeur d'un microcircuit électronique. |
| **Niveau d'assurance de l'évaluation** | Un paquet composé de composants d'assurance tirées de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des Critères Communs. |
| **Objectif de sécurité** | Une expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses. |

| | |
|---|---|
| **Personnalisateur** | Industriel inscrivant dans la mémoire de données du composant masqué les données spécifiques à une application. |
| **Politique de sécurité organisationnelle** | Une ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement. |
| **Porteur** | Utilisateur final de la carte. |
| **Produit** | Un ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes. |
| **Profil de protection** | Un ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs. |
| **Transaction** | Une séquence de commandes pour réaliser une transaction financière, telle que spécifiée dans les spécifications [8]. |

# Acronymes

| | |
|---|---|
| **ATR** | Answer To Reset |
| **CM** | Configuration Management |
| **EAL** | Evaluation Assurance Level |
| **EEPROM** | Electrically Erasable and Programmable Read Only Memory |
| **EMV** | Europay-Mastercard-Visa |
| **MAC** | Message Authentication Code |
| **PIN** | Personal Identification Number |
| **SOF** | Strength of Function |
| **TLV** | Tag Lengh Value |
| **TOE** | Target of Evaluation |

## Annexe B

# Références

[1] [CC-1] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 1 : Introduction et modèle général CCIB-99-031, version 2.1 Août 1999.

[2] [CC-2] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 2 : Exigences fonctionnelles de sécurité CCIB-99-032, version 2.1 Août 1999.

[3] [CC-3] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 3 : Exigences d'assurance de sécurité CCIB-99-033, version 2.1 Août 1999.

[4] [CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information Partie 2 : Méthodologie d'évaluation CEM-99/045, version 1.0 Août 1999.

[5] Cible de sécurité Application GemVision Smart D/C masquée sur le composant ST19SF08AC (Référence ST19SF08AC/RMY), version 1.5 (document public).

[6] Rapport technique d'évaluation GMP010-RTE-1.01 v 1.01, AQL (diffusion contrôlée).

[7] Rapport technique d'évaluation TESTS_ALICANTE_SERMA v1.0, Serma Technologies (diffusion contrôlée).

[8] Spécifications Europay-Mastercard-Visa des cartes à microcircuit pour les systèmes de paiement, version 3.1.1, 31 mai 1998 (document public).

[9] Profil de protection "Smartcard Embedded Software", version 1.2 du 19 novembre 1998, enregistré sous la référence PP/9810 (document public).

[10] Profil de protection "Smartcard Integrated Circuit", version 2.0 de septembre 1999, enregistré sous la référence PP/9806 (document public).

[11] Guide d'utilisation GEMPLUS-ALICANTE-AGD_USR.01 v1.0, Gemplus (document public).

[12] Guide d'administration GEMPLUS-ALICANTE-AGD_ADM.01 v2.1, Gemplus (document public).

[13] Security application manual APM.19.SECU/0006V1.2, STMicroelectonics (diffusion contrôlée).