PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2004/01

Composant ST19XS04D masqué par l'application IGEA 440 (référence ST19XS04\PIL)

Paris, le 16 janvier 2004

Le Directeur central de la sécurité des systèmes d'information

Henri Serres

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 terme d'objectifs de sécurité.
Toutefois, la certification ne constitue pas en soi une recommandation du produit par l'organisme de certification, et ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables.

Table des matières

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 rendu public (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 selon les ITSEC et les Critères Communs sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'**accord de reconnaissance** européen du SOG-IS de 1999 permet la reconnaissance entre les états signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

La direction centrale de la sécurité des systèmes d'information passe aussi des **accords de reconnaissance** avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties.

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

1. Le produit évalué

1.1. Contexte

L'application IGEA 440 a été développée par Axalto pour répondre au besoin du GIE Sesam-Vitale de disposer d'une carte pour les patients du système de santé (carte Vitale).
La version précédente de l'application a été certifiée en février 2003 [2003/03].

1.2. Identification du produit

Le produit évalué est le **composant ST19XS04D masqué par l'application IGEA 440 (référence ST19XS04\PIL)**.

1.3. Les développeurs

Pour le micro-circuit :

STMicroelectronics

29 boulevard Romain Rolland
75669 Paris Cedex 14
France.

Pour l'application :

Axalto, a Schlumberger company

36-38, rue de la Princesse
78431 Louveciennes
France.

1.4. Description du produit évalué

La carte contenant l'application IGEA 440 offre à ses utilisateurs (les porteurs, l'émetteur des cartes et le personalisateur) des fonctions d'authentification de la carte, de signature de données externes ainsi que des moyens sécurisés de gestion des mémoires.

1.4.1. Architecture

Le produit est constitué :

- du micro-circuit ST19XS04D conçu et fabriqué par STMicroelectronics ; ce micro-circuit a été certifié en 2002 [2002/19] ;
- de l'application IGEA 440 (masque M9V2) développée par Axalto.

1.4.2. Cycle de vie

Le cycle de vie du produit est le suivant :

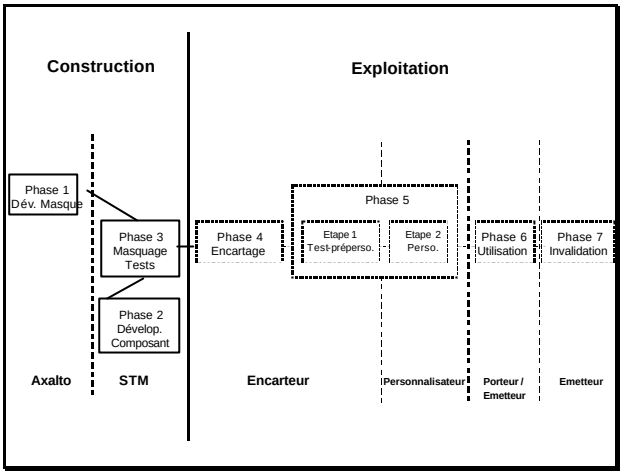

Figure 1 - Cycle de vie du produit

1.4.3. Périmètre et limites du produit évalué

La fonctionnalité de changement de PIN n'a pas été évaluée. Le produit évalué correspond au produit à sa sortie de la phase 3.

1.5. Utilisation et administration

1.5.1. Utilisation

Pour l'évaluation, les utilisateurs du produit sont l'émetteur de la carte ainsi que le porteur final.

1.5.2. Administration

Les administrateurs de la carte sont l'encarteur et le personnalisateur.

2. L'évaluation

2.1. Centre d'évaluation

CEA - LETI

17 rue des martyrs
38054 Grenoble Cedex 9
France.

Téléphone : +33 (0)4 38 78 40 87

Adresse électronique : alain.merle@cea.fr

L'évaluation s'est déroulée d'octobre à décembre 2003.

2.2. Commanditaire

Axalto, a Schlumberger company

36-38, rue de la Princesse
78431 Louveciennes
France.

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux ITSEC [ITSEC], à son manuel d'évaluation associé [ITSEM], et aux interprétations définies dans la bibliothèque d'interprétations communes [JIL].

2.4. Fonctionnalité du produit

La cible de sécurité [ST] définit les fonctions dédiées à la sécurité par rapport auxquelles le produit est évalué et les liens entre le produit et son environnement d'exploitation.

2.5. Évaluation du produit

Le micro-circuit étant certifié par ailleurs [2002/19], les travaux effectués dans le cadre de cette évaluation ont porté essentiellement sur l'évaluation du masque et sur son intégration sûre dans le micro-circuit conformément aux interprétations sur la composition d'un circuit intégré et d'un logiciel embarqué [JIL-COMP].
De plus, l'évaluateur s'est appuyé sur les travaux qui avaient été réalisés lors de l'évaluation de la version précédente du produit (référence ST19XS04\PIC) qui avait fait l'objet du certificat 2003/03.
Les tâches suivantes d'évaluation ont fait l'objet de nouveaux travaux du fait des modifications du produit :

- construction – le processus de développement : « spécification des besoins » et « réalisation » ;
- construction – l'environnement de développement ;

- exploitation – la documentation d'exploitation : « documentation d'utilisation » ;
- construction – estimation de la vulnérabilité en construction ;
- exploitation – estimation de la vulnérabilité en exploitation.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du composant ST19XS04D masqué par l'application IGEA 440 (référence ST19XS04\PIL).

3.2. Niveau d'évaluation

Le composant ST19XS04D masqué par l'application IGEA 440 (référence ST19XS04\PIL) répond aux critères de conformité du niveau E3. Ces critères sont listés dans le tableau suivant :

Construction : Le processus de développement	Spécification des besoins
	Conception générale
	Conception détaillée
	Réalisation
Construction : L'environnement de développement	Gestion de configuration
	Langages de programmation et compilateurs
	Sécurité des développeurs
Exploitation : La documentation d'exploitation	Documentation de l'utilisateur
	Documentation d'administration
Exploitation : L'environnement d'exploitation	Livraison et configuration
	Démarrage et exploitation

Le composant ST19XS04D masqué par l'application IGEA 440 (référence ST19XS04\PIL) répond aux critères d'efficacité des ITSEC [ITSEC]. Ces critères sont listés dans le tableau suivant. La résistance minimale des mécanismes est cotée moyenne.

Construction	Pertinence de la fonctionnalité
	Cohésion de la fonctionnalité
	Résistance des mécanismes
	Estimation de la vulnérabilité de la construction
Exploitation	Facilité d'emploi
	Estimation de la vulnérabilité en exploitation

3.3. Fonctions dédiées à la sécurité

Les fonctions dédiées à la sécurité évaluées sont les suivantes :

- authentification de l'encarteur ou du personnalisateur ;
- authentification de l'émetteur principal ;
- authentification des émetteurs secondaires ;
- authentification du porteur ;
- authentification simultanée du porteur et de l'émetteur principal ;
- authentification de la carte ;
- signature de données externes ;
- inhibition du mode tests ;

- irréversibilité des phases ;
- cloisonnement des types de mémoires ;
- cloisonnement de la mémoire utilisateur ;
- phase d'invalidation ;
- signature des mots en zones protégées ;
- supervision.

3.4. Analyse des mécanismes cryptographiques

Une analyse des mécanismes cryptographiques a été réalisée par la DCSSI (cf Annexe 2).

3.5. Reconnaissance européenne (SOG-IS)

Ce certificat a été émis dans les conditions de l'accord du SOG-IS. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].

3.6. Restrictions d'usage

Le produit doit être utilisé dans un environnement qui respecte les recommandations se trouvant dans les guides utilisateur [USR] et administrateur [ADM] et dans la cible de sécurité [ST].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

3.7. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le composant ST19XS04D masqué par l'application IGEA 440 (référence ST19XS04\PIL) satisfait à sa cible de sécurité [ST].

Annexe 1. Références documentaires du produit évalué

[ADM]	"Spécification d'administration des cartes IGEA", référence LV-RD-STG-02-3007, version 3.4, 14 janvier 2003.
[RTE]	Rapport technique d'évaluation, référence LETI.CESTI.MUS.RTE.003, version 1.0, 09/12/03.
[ST]	Cible de sécurité et d'évaluation, référence it_CS-SCT-SC&RSW-00-1-092-DR, version 01.05, 08/12/03.
[USR]	"Guide d'utilisation de la carte IGEA 340/440", référence LV-RD-MAN-02-3009, version 2.3, février 2003.
[2003/03]	Rapport de certification du composant ST19XS04D masqué par l'application IGEA 440, référence 2003/03, février 2003.
[2002/19]	Rapport de certification du microcircuit ST19XS04D, référence 2002/19, août 2002.

Annexe 2. Analyse des mécanismes cryptographiques

Le produit évalué utilise les mécanismes cryptographiques suivants :

- authentification chiffrée.
  Ce mécanisme est d'un niveau de résistance élevé.

- déblocage de la carte.
  Ce mécanisme est d'un niveau de résistance élevé.

- signature d'un message.
  Ce mécanisme est d'un niveau de résistance élevé.

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.	
[ITSEC]	Critères d'évaluation de la sécurité des systèmes informatiques, version 1.2, juin 1991.
[ITSEM]	Manuel d'évaluation de la sécurité des technologies de l'information, version 1.0, septembre 1993.
[JIL]	Joint Interpretation Library, version 2.0, novembre 1998.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[JIL-COMP]	Les guides pour la composition sont : • ETR-lite for composition, version 1.0, mars 2002, Joint Interpretation Library • ETR-lite for composition : Annex A, Composite smartcard evaluation : Recommended best practice, version 1.2, mars 2002, Joint Interpretation Library

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr