EVALUATION DE LA SECURITE DU COMPOSANT MASQUE IGEA 440 SUR ST19XS04D

CIBLE DE SECURITE ET D'EVALUATION

Version Publique

Historique :

Afin de faciliter la compréhension du lecteur, on rappelle ici les différentes désignations qui ont existé depuis l'émission de la première carte Vitale jusqu'à aujourd'hui.

SCOT : nom historiquement utilisé pour désigner la famille des premières cartes Vitale (Bull CP8) chargée avec un système d'exploitation de type dit « M9 ».

M9V1 : nom historiquement utilisé pour désigner le premier masque Vitale (Bull CP8).

M9V2 : nom initialement utilisé pour désigner le nouveau masque Vitale concerné par la présente cible de sécurité.

IGEA : nom utilisé pour désigner les nouvelles carte Vitale concernée par la présente cible de sécurité (remplace SCOT).

IGEA 440 : nom actuellement utilisé pour désigner le nouveau masque Vitale (sur composant ST) concerné par la présente cible de sécurité (remplace M9V2 sur ST).

IGEA 340 : nom actuellement utilisé pour désigner le nouveau masque Vitale (sur composant ATMEL, remplace M9V2 sur ATMEL).

PIC : référence STMicroelectronics du masque IGEA 440 chargé sur le composant ST19XS04D

PIL : référence STMicroelectronics du masque IGEA 440 V2 chargé sur le composant ST19XS04D

SOMMAIRE

1 OBJET

Ce document est la version publique du document original « CIBLE DE SECURITE ET D'EVALUATION ». Certaines informations confidentielles présentes dans la version originale ne sont pas disponibles dans la version publique.

1.1 IDENTITE DE LA CIBLE D'EVALUATION

La cible d'évaluation est le ***COMPOSANT MASQUE*** IGEA 440 sur ST19XS04D constitué du microcircuit électronique ST19XS04D développé par la société STMicroelectronics, sur lequel est installé le ***MASQUE*** IGEA 440 développé par AXALTO (ex. CP8), destiné à fournir la carte IGEA 440.

1.2 NATURE DE LA CIBLE D'EVALUATION

La cible d'évaluation est un produit.

1.3 FONCTION DE LA CIBLE D'EVALUATION

La cible d'évaluation est destinée à préciser les paramètres d'une évaluation sécuritaire d'un composant masqué équipant les cartes IGEA 440 afin d'en assurer la sécurité.

1.4 OBJECTIF DU DOCUMENT

L'objectif du document est le suivant :

- décrire l'argumentaire du produit,
- décrire les différentes fonctions dédiées à la sécurité ainsi que les mécanismes obligatoires associés réalisés par le produit pour répondre aux menaces,
- fournir la cotation annoncée de la résistance minimum des mécanismes ainsi que le niveau d'évaluation visé.

2 ARGUMENTAIRE DU PRODUIT

2.1 LE COMPOSANT MASQUE

Le composant masqué est destiné à être inséré dans un support plastique ; l'ensemble constituant une carte à circuit intégré à contacts, conforme aux normes internationales référencées en annexe A2 (*NORMES ISO*).

2.2 LES DIFFERENTS INTERVENANTS ET LEUR ROLE

On distingue 3 intervenants différents :

- AXALTO SCHLUMBERGER (Ex. CP8) concepteur et réalisateur du masque (*LE MASQUEUR*),
- STMicroelectronics concepteur et réalisateur du microcircuit électronique (*LE CONCEPTEUR DE MICROCIRCUITS ELECTRONIQUES*),
- STMicroelectronics industriel responsable de la fabrication du composant masqué (*LE FONDEUR*),

Le composant a été préalablement évalué conformément à la cible de référence : STM_ST_ST19X0104_003V0_4_1

2.3 ENVIRONNEMENT D'UTILISATION PREVU

La vie du composant masqué débute par la phase de fabrication (masquage et tests composant via le logiciel de test fondeur), qui se déroule sous la responsabilité du fondeur. Elle se poursuit par une phase englobant les opérations d'encartage, de pré personnalisation et de personnalisation respectivement réalisées chez l'encarteur pour les deux premières, puis chez le personnalisateur.

A la suite de cette dernière phase, la carte est transmise au porteur auquel elle est destinée, elle est utilisée pour accéder au(x) service(s) auxquel(s) elle est dédiée. Elle entre alors dans sa phase principale dite d'utilisation.

La vie de la carte s'achève par la phase d'invalidation.

Une carte invalidée peut demeurer en possession de son porteur, elle ne lui permet plus alors de faire usage des droits qu'elle contient, les fonctions d'authentification carte et de signature d'une part et les moyens d'enregistrement de données d'autre part, étant définitivement désactivés.

2.4 MODE D'UTILISATION PREVU

La carte IGEA 440 offre aux prestataires de services durant sa phase d'utilisation, une fonction d'authentification de la carte, une fonction de signature de données externes (de service) ainsi que des moyens sécurisés de gestion de cette mémoire.

Le mode d'utilisation du composant masqué est configurable selon plusieurs paramètres en fonction de l'application à laquelle il est destiné.
Ces paramètres concernent l'établissement des protections d'accès en écriture, lecture et effacement pour les deux zones de travail

La configuration de la cible s'opère au cours de la phase de vie dite de personnalisation.

2.5 CARACTERISTIQUES DE SECURITE

Le microcircuit électronique assure, pour la cible d'évaluation, des fonctions de protection d'accès aux ressources contenues dans sa mémoire.
Il garantit qu'à l'issue de la phase de fabrication du composant masqué, l'accès aux données de sa mémoire sera entièrement contrôlé par le masque.

Le composant masqué met en œuvre, suivant les différentes phases de vie de la carte, des fonctions d'authentification et de contrôle d'accès vis à vis de l'encarteur, du personnalisateur, de l'émetteur de la carte, des émetteurs secondaires et du porteur, et de calcul de signature.

Les fonctions ci-dessus, ne peuvent être efficaces que si la sécurité et l'intégrité des ressources sensibles qu'elles exploitent sont assurées. L'intégrité de l'ensemble des informations supportées par la carte devra être également préservée.

2.6 MENACES

DIVULGATION DES DONNEES CONFIDENTIELLES

ME1 Divulgation non autorisée du code porteur, des clés émetteur principal et émetteurs secondaires et du jeu secret.

ME2 Divulgation non autorisée du logiciel de test fondeur ou du masque embarqués par le composant masqué.

SUBSTITUTION DE CARTE DANS LE SYSTEME

ME3 Substitution, dans le système, d'une carte déjà personnalisée, par une « fausse » carte n'appartenant pas au système, qui permettrait d'accéder illicitement aux services offerts par le système.

USURPATION D'IDENTITE

ME4 Personnalisation illicite du composant masqué par une personne non habilitée par l'émetteur.

ME5 Ouverture illicite de services, à des autorités non habilitées, sur une carte authentique ou sur une carte trouvée ou volée

PROTECTION DES DONNEES

ME6 Modification illicite des droits d'accès :
- aux données confidentielles (masque, code, clés ou jeu secret),
- aux données de configuration de la cible d'évaluation,.

ME7 Atteinte à l'intégrité du composant dans le but de révéler des données confidentielles (code, clés, jeu secret, Rom).

Les menaces ME1 à ME7 concernent les phases d'utilisation et d'invalidation.

2.7 CONTRE MESURES

La description des mesures permettant de contrer les menaces précédentes n'est pas disponible dans la version publique de ce document.

3 FONCTIONS DEDIEES A LA SECURITE

3.1 AUTHENTIFICATION

3.1.1 Phase de personnalisation

FS1 AUTHENTIFICATION DE L'ENCARTEUR OU DU PERSONNALISATEUR

La fonction de sécurité SF-OBS-A (Unobservability) de la cible de sécurité composant contribue à la fonction FS1

Cette fonction de sécurité permet d'authentifier l'autorité habilitée à intervenir sur la carte, durant la phase de personnalisation.

La fonction d'authentification réalisée par le masque, consiste à comparer la clé présentée à la carte à la clé de fabrication enregistrée dans la zone secrète de la mémoire utilisateur de cette carte.

3.1.2 Phases d'utilisation et d'invalidation

Durant la phase de vie d'utilisation, quatre acteurs peuvent accéder à la carte et effectuer des opérations sur cette carte.
Les quatre acteurs sont :, l'émetteur principal, deux émetteurs secondaires et le porteur.
Seuls, les émetteurs peuvent s'authentifier durant la phase d'invalidation.

FS2 AUTHENTIFICATION DE L'EMETTEUR PRINCIPAL

Les fonctions de sécurité SF_OBS_A (Unobservability) et SF_ALEAS_A (Unpredictable Number Generation support) de la cible de sécurité composant contribuent à la fonction FS2

Cette fonction de sécurité permet d'authentifier l'autorité, dite « émetteur principal », habilitée à intervenir durant les phases d'utilisation et d'invalidation.

La fonction d'authentification réalisée par le masque consiste à comparer la clé présentée à la carte, à la clé enregistrée dans la zone secrète de la mémoire utilisateur de cette carte.

La clé peut être présentée en clair ou chiffrée. Dans le second cas le déchiffrement de la clé est réalisé préalablement à la comparaison.

Afin d'interdire la recherche de cette clé par des essais exhaustifs, toute présentation incorrecte de la clé conduit au blocage immédiat de la carte.

FS3 AUTHENTIFICATION DES EMETTEURS SECONDAIRES

Les fonctions de sécurité SF_OBS_A (Unobservability) et SF_ALEAS_A (Unpredictable Number Generation support) de la cible de sécurité composant contribuent à la fonction FS3

Cette fonction de sécurité permet d'authentifier l'autorité, dite « émetteur secondaire », habilitée à intervenir durant les phases d'utilisation et d'invalidation

La fonction d'authentification réalisée par le masque, consiste à comparer la clé présentée à la carte, à la clé enregistrée dans la zone secrète adéquate de la mémoire utilisateur de cette carte.

La clé peut être présentée en clair ou chiffrée. Dans le second cas le déchiffrement de la clé est réalisé préalablement à la comparaison.

FS4 AUTHENTIFICATION DU PORTEUR

La fonction de sécurité SF_OBS_A (Unobservability) de la cible de sécurité composant contribue à la fonction FS4

Cette fonction de sécurité permet d'authentifier l'autorité, dite « porteur », habilitée à intervenir durant les phases d'utilisation et d'invalidation

Il peut être demandé à l'utilisateur d'une carte de faire la preuve qu'il en a la légitime détention, à l'aide du code porteur qui lui a été attribué. Ce code lui permet de s'authentifier.

La fonction d'authentification réalisée par le masque, consiste à comparer le code présenté à la carte, au code enregistré dans la zone secrète de la mémoire utilisateur de cette carte.

Afin d'interdire la recherche de ce code par des essais exhaustifs, le nombre de présentations successives infructueuses est limité.

FS5 AUTHENTIFICATION SIMULTANEE DU PORTEUR ET DE L'EMETTEUR PRINCIPAL

Les fonctions de sécurité SF_OBS_A (Unobservability) et SF_ALEAS_A (Unpredictable Number Generation support) de la cible de sécurité composant contribuent à la fonction FS5

Cette fonction de sécurité permet d'authentifier l'autorité, dite «autorité de déblocage » habilitée à intervenir durant les phases d'utilisation et d'invalidation

Lorsque la carte est en état de blocage, seule l'opération de déblocage est autorisée. Cette opération exige la présence obligatoire du porteur et de l'émetteur principal. Ensemble, ils doivent constituer une clé globale.

La fonction d'authentification réalisée par le masque, consiste à comparer les données représentatives du code porteur et de la clé présentées à la carte, au code porteur et à la clé enregistrés dans la zone secrète de la mémoire utilisateur de cette carte.

FS6 AUTHENTIFICATION DE LA CARTE

La fonction de sécurité SF_OBS_A (Unobservability) de la cible de sécurité composant contribue à la fonction FS6

Cette fonction de sécurité permet à l'application de déterminer l'habilitation de la carte à réaliser ou non la transaction.

La fonction d'authentification de la carte est la fonction qui permet de vérifier que la carte possède effectivement le jeu secret que son émetteur lui a dédié et de s'assurer ainsi de son authenticité.

FS7 SIGNATURE DE DONNEES EXTERNES

Les items sont identiques à la fonction FS6

3.2 CONTROLE D'ACCES

FS8 INHIBITION DU MODE TESTS

Les fonctions de sécurité SF_CONFIG_A (TOE configuration switching and control) et SF_TEST_A (Test of the TOE functionality and inhibition of the Test/issuer function) de la cible de sécurité composant contribuent à la fonction de sécurité FS8

Le rôle premier de cette fonction est de verrouiller l'accès en lecture au logiciel masqué ainsi qu'aux données enregistrées dans l'Eeprom, via le logiciel de test

FS9 IRREVERSIBILITE DES PHASES

Le masque reconnaît les différentes phases de vie du composant masqué (fabrication, personnalisation, utilisation et invalidation), il garantit leur chronologie et interdit tout retour à une phase antérieure.
L'objectif premier de cette fonction est d'interdire tout retour à une phase qui permettrait la divulgation d'informations sensibles.

FS10 CLOISONNEMENT DES TYPES DE MEMOIRES

La fonction de sécurité SF_FWL_A (Storage and function access firewall) de la cible du composant contribue à la fonction de sécurité FS10

Les instructions et données stockées dans la mémoire programme du masque (ROM) ne sont pas accessibles du monde extérieur ni en lecture, ni en écriture, ni en modification, mais sont exploitées par le microcircuit.

Les données faisant l'objet de traitements par le microprocesseur, sous le contrôle du masque ou nécessaires à la réalisation de ces traitements et transitant par la mémoire de travail (RAM) ne sont pas accessibles de l'extérieur ni en lecture, ni en écriture, ni en modification.

Les données applicatives enregistrées dans la mémoire utilisateur(EEPROM) sont, accessibles par le monde extérieur, sous contrôle du masque qui vérifie que les conditions d'accès à ces données sont satisfaites. l'échange des données entre la carte et le monde extérieur se fait par l'intermédiaire du protocole T=0 conforme aux normes ISO 7816-3

FS11 CLOISONNEMENT DE LA MEMOIRE UTILISATEUR

La mémoire utilisateur est, en fonction des besoins de l'application, découpée en zones durant la phase de personnalisation. A chacune d'entre elles, sont attribuées des caractéristiques spécifiques qui prennent effet en phase d'utilisation.

Des conditions d'accès particulières sont affectées à chaque zone et distinctement pour chacune des opérations de lecture d'écriture et d'effacement.
Seules les conditions d'accès aux zones de travail sont paramétrables.

Les conditions possibles sont :

- Libre: aucune authentification préalable à l'opération n'est requise,
- Protégée : une authentification préalable à l'opération est nécessaire,
- Interdit : le masque garantit l'inaccessibilité de l'extérieur aux données contenues dans cette zone.

FS12 PHASE D'INVALIDATION

En cas d'invalidation du composant masqué, le masque interdit toute écriture ou effacement dans la mémoire utilisateur.
La lecture des données en zone libre est possible.
La lecture des données en zone(s) protégée(s) est conditionnée à l'authentification préalable de l'émetteur principal ou de l'émetteur secondaire (voir FS2 et FS3).
La fonction de signature est désactivée.
carte réalisée.

3.3 FIDELITE / AUTHENTICITE

FS13 TRACABILITE DES DROITS AUX MOTS EN ZONES PROTEGEES

Le masque enregistre pour chaque donnée située dans une zone protégée de la mémoire utilisateur, une signature identifiant l'autorité qui a écrit cette donnée.

3.4 AUDIT

FS14 SUPERVISION

Les fonctions de sécurité SF_INT_A (TOE logical integrity), SF_PHT_A (Physical tampering security function) et SF_ADMNIS-A (security violation administration) de la cible du composant contribuent à la fonction de sécurité FS14

Le composant masqué exerce une surveillance et une analyse des événements concernant ses conditions d'environnement et son intégrité de fonctionnement et réagit selon la nature de l'événement détecté.

3.5 RECAPITULATIF FONCTIONS DEDIEES A LA SECURITE / MENACES

Fonctions de Sécurité

Menaces	FS1	FS2	FS3	FS4	FS5	FS6	FS7	FS8	FS9	FS10	FS11	FS12	FS13	FS14
ME1								X	X		X	X		
ME2								X	X	X				
ME3						X	X							
ME4	X													
ME5		X	X	X	X								X	
ME6										X	X	X		
ME7														X

Coté composant, seules les fonctions contribuant à une fonction de sécurité globale sont remontés au niveau de la cible composant masqué.
La cohérence de fonction de sécurité du composant seul est assuré par le certificat du composant.

4 MECANISME OBLIGATOIRE

Note : Le mécanisme sécuritaire n'est pas décrit dans la version publique de ce document.

5 COTATION ANNONCEE ET NIVEAU D'EVALUATION VISE

L'évaluation sera faite conformément au schéma d'évaluation français ITSEC.

La cotation requise pour la résistance minimum des mécanismes est moyenne.

Le niveau d'évaluation visé est le niveau E3.

6 CIBLE D'EVALUATION

6.1 CYCLE DE VIE D'UN COMPOSANT MASQUE

Les différentes phases listées ci-dessous décrivent le processus de développement, de fabrication d'un composant masqué, de la carte, et des informations concernant l'utilisation et la fin de vie.

PHASE 1 DEVELOPPEMENT DU MASQUE

Etape 1
Le masqueur choisit un microcircuit électronique pour développer son masque.
Il reçoit de la part du concepteur de microcircuits électroniques les éléments lui permettant de développer et de répondre au mieux aux exigences des spécifications générales du composant masqué.

Etape 2
Le masqueur développe le masque spécifique au microcircuit électronique.
Les tests des fonctions et les vérifications de conformité du masque sont réalisés par le masqueur sur émulateur.

Etape 3
A l'issue des tests du masque réalisés sur émulateur par le masqueur, une procédure d'échange du masque entre le masqueur et le fondeur est appliquée pour permettre la phase suivante qui est le masquage du composant.

PHASE 2 DEVELOPPEMENT DU COMPOSANT

Cette phase consiste à étudier l'ensemble microcircuit par le fondeur.

PHASE 3 MASQUAGE DU COMPOSANT

Etape 1

Une fois le masque développé, son installation dans le microcircuit électronique est faite chez le fondeur. Ceci consiste à implanter dans la ROM du composant, le programme de la carte ou masque, définissant ainsi ses spécificités fonctionnelles. A la fin de la fabrication du composant masqué, le fondeur réalise des tests via le logiciel de tests fondeur embarqué et termine cette étape en inhibant le mode test du composant.

Etape 2

Les tests des composants masqués prototypes et les vérifications de leur conformité sont réalisés par le masqueur afin d'autoriser la production en masse.

Lors de la production, avant livraison aux encarteurs, tous les composants masqués sont testés par le fondeur.

PHASE 4 ENCARTAGE

Cette phase consiste à réaliser physiquement une carte.

Etape 1

Elle consiste à partir du composant masqué, d'un circuit imprimé et de divers éléments, de constituer de façon industrielle un micromodule.

Etape 2

Cette étape réalise l'assemblage du micromodule avec un support plastique conforme aux normes 7816-1 / 2 afin d'obtenir une carte au format ISO.

PHASE 5 TEST , PREPERSONNALISATION ET PERSONNALISATION

Etape 1 (test et prépersonnalisation)

Opération comprenant d'une part le test fonctionnel du composant via le masque, et d'autre part, l'écriture dans la mémoire de la carte de son numéro de série et des informations identifiant l'encarteur.

Etape 2 (personnalisation)

Opération qui consiste à définir pour la carte : la structure de sa mémoire utilisateur, ses protections et toutes les informations physiques et logiques initiales nécessaires à son utilisation.
On distingue plusieurs personnalisations:

- Personnalisation électrique
- Définition de la partition de la mémoire utilisateur et écriture dans le composant de données spécifiques à l'application et au porteur.
- Personnalisation physique
- Estampage ou engravage sur le corps de carte.
- Personnalisation graphique
- Impression, monochrome ou en couleurs, d'images sur le corps de carte.

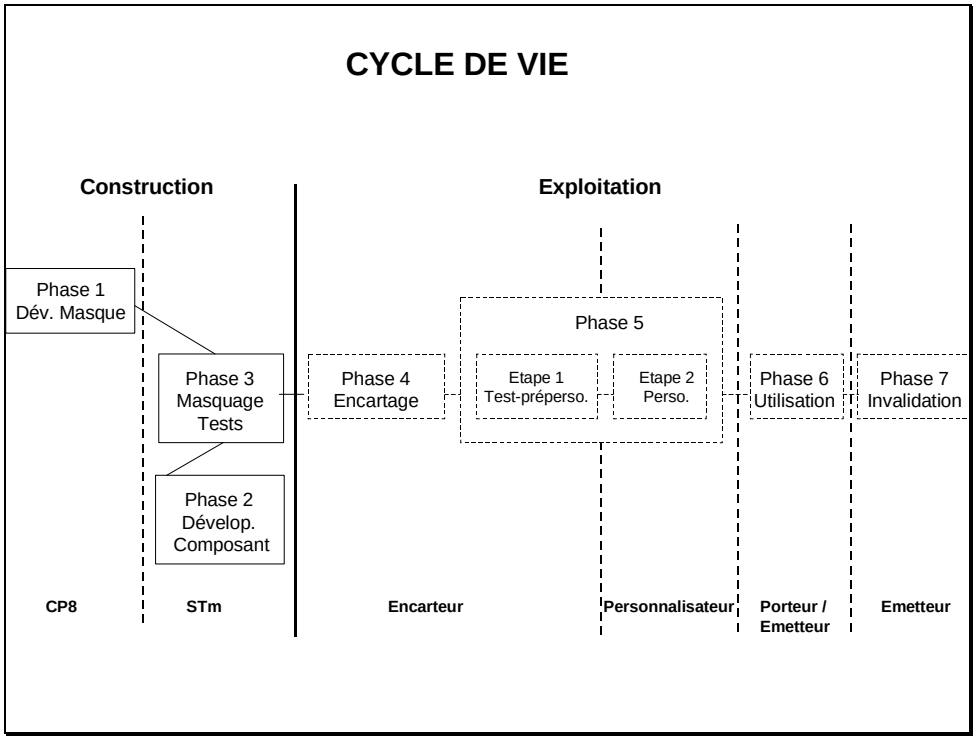
PHASE 6 UTILISATION

Phase de disponibilité de la carte pour un porteur, pour des services déterminés dans le cadre d'une application .

PHASE 7 INVALIDATION

Phase rendant la carte non évolutive et inutilisable par le porteur.

CYCLE DE VIE



6.2 COMPOSITION DE LA CIBLE D'EVALUATION

Elle est composée du ***COMPOSANT MASQUE*** IGEA 440 sur ST19XS04D, constitué du microcircuit électronique ST19XS04D sur lequel est installé le ***MASQUE*** IGEA 440, destiné à fournir la carte IGEA 440.

6.3 CONTEXTE DU DEVELOPPEMENT

Le masque IGEA 440 est développé par AXALTO Schlumberger (Ex. CP8).
Le composant ST19XS04D est développé par STmicroelectronics,
Le composant masqué est réalisé par STmicroelectronics.

Commanditaire : AXALTO Schlumberger (Ex. CP8)
Centre d'évaluation : LETI
Centre de Certification : DCSSI
Développeurs : AXALTO (Ex. CP8) et STmicroelectronics

6.4 CONTEXTE DE L'EVALUATION

L'évaluation sécuritaire du composant masqué sera consécutive à la qualification du microcircuit électronique, au développement et à la qualification du masque, ainsi qu'à la qualification du composant masqué.

6.6 PARAMETRES DE L'EVALUATION

6.6.1 Type de la cible d'évaluation

La cible d'évaluation est un produit.

6.6.2 Mode d'évaluation

Le mode d'évaluation est consécutif au développement et à la qualification du composant masqué.

6.6.3 Règles de confidentialité

Les règles de confidentialité à respecter lors de l'évaluation sont définies de manière contractuelle dans la convention d'évaluation.

6.6.4 Justification du choix du produit

Les éléments qui ont justifié le choix de ce produit sont essentiellement :

- la capacité mémoire de données,
- les performances des fonctions intrinsèques au composant dédiées à la sécurité,
- son encombrement limité qui facilite son encartage et augmente sa résistance aux sollicitations mécaniques.

6.7 LIMITES DE LA CIBLE D'EVALUATION

6.7.1 Eléments internes à la cible

Les procédures de sécurité garantissant la confidentialité et l'intégrité du composant masqué réalisées lors des phases 1 à 3 font partie de la cible d'évaluation.

Ces procédures sont les suivantes :

- les procédures propres au concepteur de microcircuits électroniques chargée de protéger le microcircuit électronique lors de son développement,
- les procédures propres au masqueur chargée de protéger le masque lors de son développement,
- les procédures communes au masqueur et au fondeur chargée de protéger le masque lors de sa livraison par le masqueur au fondeur,
- les procédures propres au fondeur chargée de protéger le masque lors de son stockage et de son installation dans le microcircuit électronique,
- les procédures propres au fondeur concernant la livraison des composants masqués aux encarteurs.

6.7.2 Eléments externes à la cible

La fonctionnalité de changement de PIN ne fait pas partie de la cible, ainsi que les phases 4,5,6,7 décrites dans le chapitre cycle de vie d'un composant masqué.

7 GLOSSAIRE

Bouton Circuit imprimé sur une carte, servant d'interface de contact entre le microcircuit inclus dans la carte et le ***connecteur*** de l'appareil dans lequel la carte est introduite.

Carte à microcalculateur
Carte à microcircuit dont les fonctions sont déterminées par la programmation du microcalculateur de la carte: S.P.O.M

Commanditaire(s) : Organisme(s) maître(s) d'ouvrage de l'évaluation.

Concepteur de microcircuits électroniques :
Industriel proposant un microcircuit électronique standard sur le marché.

Connecteur Appareil assurant la connexion physique et le contact électrique de la carte.

Encartage Opération qui consiste à insérer un micromodule sur un support plastique.

Encarteur Industriel chargé de l'encartage

Masque : Ensemble des programmes inscrit dans la ROM du microcalculateur constituant le "système d'exploitation de base" de la carte.

Micromodule Bouton et composant assemblés

SPOM Abréviation de **S**elf **P**rogrammable **O**ne Chip **M**icroprocesseur microprocesseur autoprogrammable monolithique.

Personnalisateur Industriel chargé de la personnalisation

Personnalisation Opération qui consiste à définir pour la carte : la structure de sa mémoire utilisateur, ses protections et toutes les informations physiques et logiques initiales nécessaires à son utilisation.

Phase de fabrication Réalisation à partir du masque et du microcircuit électronique du composant masqué

Prépersonnalisation Opération comprenant d'une part le test fonctionnel du composant, et d'autre part, l'écriture dans la mémoire de la carte de son numéro de série et des informations identifiant l'encarteur.

Porteur Titulaire final de la **carte à microcalculateur** personnalisée.

Utilisation Période de disponibilité de la carte pour un usager, pour des services déterminés dans le cadre d'une application.