PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Direction centrale de la sécurité des systèmes d'information

Paris, le 15 mai 2006

N°1083/SGDN/DCSSI/SDR
Référence : NOTE/06.1

NOTE D'APPLICATION

PRISE EN COMPTE DE CORRECTIFS DU LOGICIEL EMBARQUÉ, CHARGÉS EN EEPROM , LORS DE L'ÉVALUATION D'UNE CARTE À PUCE SELON LE PP 9911

Objet : Prise en compte de correctifs du logiciel embarqué, chargés en EEPROM , lors de l'évaluation d'une carte à puce selon le PP 9911

Application : A compter du 20 septembre 2005

Diffusion : Publique

Vérifié par	Validé par Le sous-directeur "Régulation"	Vu l'avis du comité directeur Approuvé par Le Directeur central de la sécurité des systèmes d'information
Le responsable qualité *[ORIGINAL SIGNE]* *Le chef du centre de certification* *[ORIGINAL SIGNE]*	*[ORIGINAL SIGNE]*	*[ORIGINAL SIGNE]*

Suivi des modifications

Révision	Date	Modifications
1		Création

TABLE DES MATIERES

1. Objet de la note

L'objet de cette note est de fixer un cadre pour la prise en compte du chargement de correctifs logiciels (patch) en mémoire EEPROM de carte à puce, lors de l'évaluation de cartes selon le [PP9911].

2. Références

- [PP9911] : Eurosmart protection profile : Smart Card Integrated Circuit with Embedded Software v2.0. certifié par la DCSSI sous la référence 9911.Document publié sur le site : www.ssi.gouv.fr,
- Présentation à la 5ème conférence de l'ICCC : "The effects of patch on a CC evaluation of a smart card that claims PP/9911", CESTI LETI, 29 septembre 2004.

3. Problématique

Le profil de protection [PP9911] présente le cycle de vie d'une carte à puce de la façon suivante :

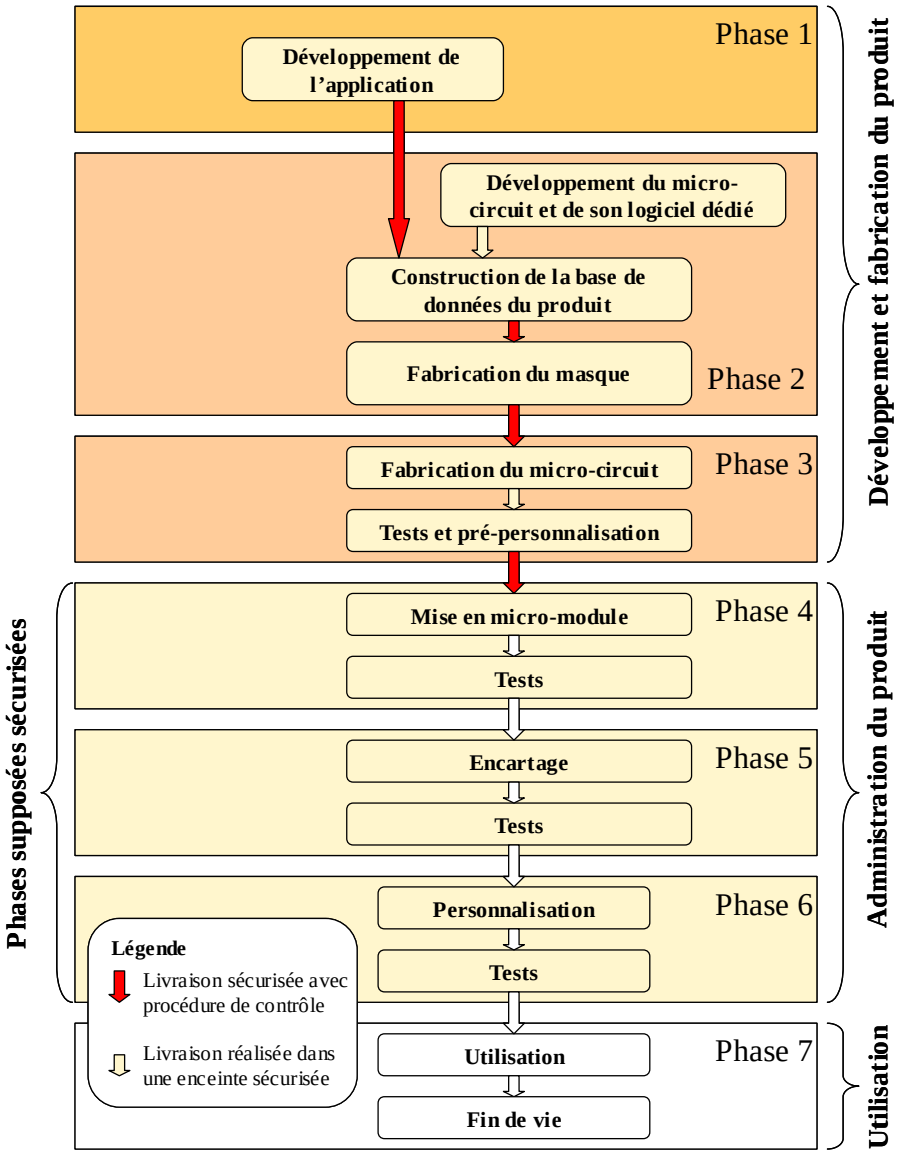

Figure 1 - Cycle de vie d'une carte à puce, selon le [PP9911]

Les hypothèses et menaces du profil de protection [PP9911] expriment tacitement que le code de l'application embarquée est développé en phase 1 et chargé dans la puce lors de sa fabrication en phase 3. L'intégrité du code une fois écrit dans la carte serait alors garantie par la technologie des mémoires ROM du

micro-circuit. Or le comportement du logiciel embarqué en ROM peut être modifié dans des phases ultérieures à celles de fabrication, par le chargement de correctifs logiciels en mémoire EEPROM (ces correctifs sont appelés « patch » ou « soft mask »). De plus, certains micro-circuits utilisent des mémoires réinscriptibles à la place de la mémoire ROM (par exemple des mémoires flash, EEPROM) permettant d'embarquer le logiciel dans des phases ultérieures à celles prévues par le [PP9911].

Dans ce contexte, la menace « T.MOD_SOFT » du PP (modification non autorisée du logiciel embarqué de la carte à puce et des données applicatives) est insuffisante car elle ne porte que sur le micro-circuit et négligent les aspects logiciels.

Cette note fournit donc un ensemble de précisions et de recommandations permettant de mener à bien l'évaluation d'un tel produit tout en restant conforme à l'approche du [PP9911].

Seul le cas du patch sera traité. Le cas plus général où la totalité du logiciel est embarquée en phase 5 doit respecter l'esprit de la présente note.

4. Impact des correctifs sur l'assurance

La présence d'un correctif chargé en phase 5 dans le produit évalué a potentiellement un impact sur chaque composant d'assurance requis pour le niveau EAL4+ visé par le [PP9911]. Cet impact est détaillé pour chaque classe d'assurance du niveau EAL4+.

4.1. ASE – Cible de sécurité

Bien que la TOE ne soit pas totalement finalisée en fin de phase 3, il est possible de maintenir une conformité de la cible de sécurité au profil de protection [PP9911] en ajoutant les éléments suivants :

- la fonctionnalité de chargement du patch doit être identifiée dans la cible de sécurité ;
- en cas d'évaluation de produit avec un patch, l'identification de la TOE doit permettre d'identifier le patch comme un composant de la TOE ;
- la menace « T.MOD_SOFT » doit être étendue pour être couvrir également le logiciel. L'ajout d'objectifs sur la TOE et/ou sur l'environnement est donc requis ;
- si des objectifs sur la TOE sont ajoutés, ils devront être couverts par les exigences fonctionnelles de sécurité adéquates et d'éventuelles fonctions de sécurité en découleront ;
- des menaces sur l'environnement peuvent être ajoutées, notamment en ce qui concerne la livraison du patch par le développeur au responsable du chargement de patch. Il est néanmoins possible de considérer que les menaces existantes « T.DIS_DEL.1 et 2 » et « T.MOD_DEL.1 et 2 » sont suffisantes pour traiter ce point.

4.2. ACM – Gestion de configuration

Le patch doit être géré en configuration par le développeur au même titre que le logiciel embarqué.

L'identification du produit doit permettre de distinguer le produit avec patch du produit sans patch (ATR, CPLC,…).

4.3. ADO – Livraison et opération

Concernant la famille ADO_IGS, l'usage dans le monde de la carte à puce est de reporter les fournitures et analyses correspondantes dans la classe relative aux guides (AGD). Ce point est donc traité au paragraphe associé (§4.5).

En ce qui concerne la famille ADO_DEL, l'existence de procédures de livraisons du patch en phase 5 doit être vérifiée et ces procédures doivent être suffisantes pour assurer l'intégrité et la confidentialité du patch. Des mesures doivent exister pour assurer que le contenu du patch n'a pas été modifié avant son chargement dans la carte.

4.4. ADV – Développement

Le patch chargé doit être évalué car il fait partie du logiciel embarqué (impact pour la famille ADV_IMP – analyse de l'implémentation, et ADV_RCR – analyse de la traçabilité). Si le patch est chargé après la certification, les procédures de continuité de l'assurance ou de ré-évaluation pourront être appliquées en fonction de l'impact du patch sur la sécurité du produit.

4.5. AGD – Guides

La TOE n'existe véritablement dans sa configuration évaluée qu'après le chargement du patch. Les procédures d'application du patch en phase 5 (donc en phase d'utilisation) devront donc être clairement décrites dans les guides.

Les moyens d'identification des états de la TOE et de la TOE elle-même (« patchée », non « patchée », version de la TOE et du patch…) doivent également être précisés.

4.6. ALC – Support au cycle de vie

Le patch doit être protégé en confidentialité et en intégrité durant son développement, au même titre que le logiciel embarqué.

4.7. ATE – Tests

Les fonctions du patch ainsi que le patch lui-même doivent être testés fonctionnellement.

4.8. AVA – Estimation des vulnérabilités

Le [PP9911] spécifie que la TOE doit savoir se protéger dès la fin de la phase 3. Par conséquent, elle doit notamment être protégée contre le chargement de patchs illégaux ce qui suppose des fonctions de sécurité spécifiques au chargement de patchs. Il faut donc s'assurer lors de l'évaluation :

- que les guides décrivent comment vérifier si un patch a été chargé dans la carte, et si c'est le cas, qu'ils donnent des indications permettant de s'assurer que le patch chargé est un patch valide (analyse MSU) ;
- que la TOE est résistante à des attaquants disposant d'un potentiel d'attaque élevé avant et après le chargement du patch (analyse VLA). Cela suppose une analyse de vulnérabilité des mécanismes de chargement de patch.