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

Paris, le 09 juillet 2013

N° 2360/ANSSI/SDE/PSS/CCN
Référence :ANSSI-CC-NOTE-16/1.0

NOTE D'APPLICATION

EXPERTISE COMPLEMENTAIRE POUR DES EVALUATIONS DE PRODUITS BANCAIRES

Application : Dès son approbation

Diffusion : Publique

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

Signé : Patrick PAILLOUX

Suivi des modifications

Version	Date	Modifications
1.0	9 juillet 2013	Création

En application du décret n° 2002-535 du 18 avril 2002 modifié, la présente note d'application a été soumise au comité directeur de la certification, qui a donné un avis favorable.

La présente note d'application est disponible en ligne sur les sites suivants :

- le site institutionnel de l'ANSSI (www.ssi.gouv.fr) ;
- le site institutionnel du SGDSN (www.sgdsn.gouv.fr) ;
- le site prévu par le décret n° 2008-1281 du 8 décembre 2008 pour la publication des instructions et circulaires (www.circulaires.gouv.fr).

TABLE DES MATIERES

1. Objet de la note

L'objet de cette note est d'exposer le processus d'expertise complémentaire des produits bancaires pouvant être mis en œuvre en parallèle d'une évaluation Critères Communs dans le cadre du schéma français.

2. Références

- 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.
- Convention d'expertise pour les évaluations de sécurité entre GIE CB, MPS, SFPMEI et ANSSI.

3. Problématique

Les entités interbancaires GIE CB[1], SFPMEI[2] et MPS[3] gèrent les autorisations de mise sur le marché (également dénommés agréments bancaires) des applications bancaires sur cartes à puce, comme suit :

- GIE CB traite les applications CB-EMV ;
- SFPMEI et MPS traitent les applications Monéo.

Le volet sécurité de cet agrément bancaire repose sur les deux types d'évaluation suivants :

- des évaluations Critères Communs (CC) menées dans le cadre du schéma français de certification ;
- des expertises complémentaires optionnelles.

Les entités interbancaires et l'ANSSI ont convenu de confier à l'ANSSI la charge de coordonner, le cas échéant, ces deux types d'évaluations afin d'assurer leur bon déroulement.

4. Présentation de la démarche d'expertise complémentaire

Les laboratoires chargés de mener les expertises complémentaires sont dénommés « laboratoires d'excellence » pour les distinguer des CESTI. Le chapitre 7 décrit les modalités de référencement de ces laboratoires d'excellence. La liste de ces laboratoires d'excellence est maintenue par l'ANSSI et les entités interbancaires. L'annexe A en dresse la liste au moment de la rédaction de la présente note. Elle est mise à jour en tant que de besoin, conformément à la convention en référence et en accord avec les signataires de la convention.

Une expertise complémentaire correspond à une évaluation en « boîte noire », c'est à dire sans mise à disposition des détails de conception de l'application bancaire considérée. Ni les méthodes de test, ni les équipements utilisés ne sont prédéterminés.

Une expertise complémentaire correspond à une charge maximale de deux hommes x mois. Cette charge est consacrée à la réalisation de tests de pénétration et à la rédaction d'un rapport d'expertise. Le rapport d'expertise décrit les tests de pénétration effectués et les vulnérabilités détectées. Ce rapport relève de la seule responsabilité du laboratoire d'excellence ayant réalisé l'expertise

[1] Groupement d'Intérêt Economique des Cartes Bancaires.

[2] Société Financière du Porte-Monnaie Electronique Interbancaire.

[3] Société MONEO PAYMENT SOLUTIONS.

complémentaire. Il est cependant revu par l'ANSSI pour confirmer les cotations des éventuelles attaques identifiées par le laboratoire d'excellence.

Aux fins de réalisation de l'expertise complémentaire, les entités interbancaires s'engagent contractuellement avec les laboratoires d'excellence chargés de réaliser ces expertises. Ces contrats prévoient notamment les clauses nécessaires pour la réalisation et la restitution de l'expertise complémentaire. Ils prévoient également que l'ANSSI soit informée par le laboratoire d'excellence du déroulement des travaux d'expertise et des résultats au fur et à mesure de l'avancement des travaux, pour permettre à l'ANSSI de coordonner au mieux l'expertise complémentaire et l'évaluation CC conduite en parallèle.

5. Proposition d'expertise

5.1. Proposition d'expertise complémentaire par l'ANSSI

5.1.1. Introduction

Chaque évaluation CC d'application bancaire ne peut être assortie d'une expertise complémentaire. Par conséquent, des choix doivent être faits pour identifier les produits soumis à expertise.

Il a été ainsi décidé que l'ANSSI propose aux entités interbancaires :

- les produits qui pourraient faire l'objet d'une expertise complémentaire ;
- les laboratoires d'excellence qui réaliseraient ces expertises.

Ces propositions sont faites sur la base des critères présentés ci-dessous.

5.1.2. Critères de choix du produit

L'ANSSI propose les produits éligibles à expertise complémentaire sur la base des principaux critères suivants, présentés par ordre d'importance décroissante :

- le caractère innovant du produit : la priorité est donnée aux produits les plus novateurs (par exemple : nouveau microcircuit, nouveau système d'exploitation, nouvelle application, …) afin de renforcer le savoir-faire des développeurs en matière de sécurité des produits « d'avenir » ;
- la rotation des développeurs : si deux développeurs présentent des produits éligibles qui ne pourraient faire tous les deux l'objet d'une expertise complémentaire, la priorité est donnée au développeur pour lequel la dernière expertise est la plus ancienne ;
- la sensibilité des produits à certaines attaques : la priorité est donnée aux produits pour lesquels il est pressenti que certains types d'attaques auraient une probabilité élevée de réussite et que ces attaques permettraient d'accéder aux biens bancaires les plus sensibles.

5.1.3. Critères de choix du laboratoire

L'ANSSI propose les laboratoires d'excellence sur la base des principaux critères suivants, présentés par ordre d'importance décroissante :

- les moyens techniques et la compétence du laboratoire : la priorité est donnée au laboratoire disposant des moyens techniques de tests et des compétences associées les plus adaptés au regard du produit soumis à expertise ;

- la disponibilité du laboratoire : le laboratoire retenu doit pouvoir réaliser l'expertise complémentaire dans des délais compatibles avec la fin prévue ou estimée de l'évaluation CC ;
- la rotation des laboratoires : si plusieurs laboratoires remplissent les conditions pour réaliser l'expertise, la priorité est donnée au laboratoire pour lequel la dernière expertise est la plus ancienne.

5.2. Contractualisation

Les entités interbancaires valident les propositions de l'ANSSI, sur la base de leur engagement de financement, au plus tard au moment de la réunion de lancement de l'évaluation CC du produit. Il appartient ensuite aux entités interbancaires de passer un contrat avec le laboratoire retenu dans des délais permettant de réaliser l'expertise complémentaire avant le terme prévu de l'évaluation CC.

Dès que l'ANSSI est informée de la finalisation du processus de contractualisation, elle informe le développeur de la décision de soumettre le produit à expertise complémentaire, du laboratoire qui la réalisera et de la date retenue de réalisation des travaux d'expertise.

6. Coordination de l'expertise complémentaire et de l'évaluation CC

6.1. Introduction

Pour permettre à l'ANSSI d'identifier au plus tôt les produits susceptibles d'être soumis à expertise complémentaire et ainsi de minimiser au mieux l'impact de l'expertise complémentaire sur l'évaluation CC, les développeurs doivent diffuser annuellement à l'ANSSI la liste de tous leurs produits bancaires qui seraient soumis à une évaluation CC dans l'année au sein du schéma français. Cette liste doit être assortie d'un descriptif technique, de la date prévisionnelle de demande d'évaluation CC et des dates prévisionnelles de disponibilité de chacun de ces produits. Toute modification doit être communiquée au centre de certification. Si cet engagement n'est pas respecté de la part des développeurs, l'objectif de coordination entre l'expertise complémentaire et l'évaluation CC ne pourra être tenu. Ce problème ne saurait être imputé ni aux entités interbancaires ni à l'ANSSI.

L'expertise complémentaire se déroule indépendamment de l'évaluation CC. Si des échanges entre le laboratoire d'excellence et le CESTI s'avèrent nécessaires, ils seront sous le contrôle de l'ANSSI.

6.2. Fournitures

Le développeur livre au laboratoire d'excellence les échantillons du produit et les profils correspondants.

Le développeur est garant de la cohérence entre les échantillons du produit livrés au laboratoire réalisant l'expertise complémentaire et ceux livrés au CESTI dans le cadre de l'évaluation CC. Lorsque les échantillons livrés au laboratoire d'excellence et au CESTI correspondent à des versions différentes du produit, le développeur doit fournir une analyse d'impact détaillée entre les deux versions du produit, et s'engage quoi qu'il en soit à conserver des échantillons de chaque version en quantité suffisante pour permettre au CESTI d'effectuer les vérifications que celui-ci jugerait utiles.

6.3. Diffusion des rapports d'expertise complémentaire

Les entités interbancaires, le développeur et l'ANSSI sont destinataires du rapport d'expertise. Les informations du rapport d'expertise ne sont divulguées ni par les entités interbancaires, ni par le développeur au laboratoire en charge de l'évaluation CC.

6.4. Résultats de l'expertise complémentaire

Lorsque l'ANSSI juge que certaines vulnérabilités mises en évidence lors de l'expertise complémentaire peuvent avoir un impact sur le niveau de sécurité visé par l'évaluation CC, elle demande au développeur de corriger son produit (comme pour n'importe quelle vulnérabilité découverte lors d'une évaluation CC) et le CESTI se prononcera sur l'efficacité de la contre-mesure dans le cadre de l'évaluation CC.

7. Référencement des laboratoires d'excellence

Les entités interbancaires et l'ANSSI référencent les laboratoires candidats sur la base des critères suivants :

- excellente réputation sur le plan éthique ;
- compétence technique garantissant la pertinence des résultats des tests de pénétration réalisés en boîte noire. Concernant les CESTI, cette compétence est vérifiée, dans le cadre des procédures prévues par le schéma français de certification, qui informe les entités interbancaires des domaines d'excellence des CESTI. Concernant les autres laboratoires, une compétence équivalente à celle des CESTI, dans leur domaine d'expertise spécifique, devra être reconnue ;
- capacité à maintenir la confidentialité et l'indépendance de leurs travaux, y compris vis-à-vis de leurs actionnaires ou de leur structure de contrôle. Des accords de confidentialité globaux (représentant légal du laboratoire) et individuels (experts réalisant les tests de pénétration) pourront être exigés. Pour les CESTI, cette capacité est attestée par l'ANSSI dans le cadre des procédures prévues par le schéma national de certification. Pour les autres laboratoires, cette capacité est attestée par les entités interbancaires qui informent l'ANSSI des accords de confidentialité signés ;
- aptitude à travailler avec l'ANSSI dans le cadre du présent processus d'expertise.

Annexe A Liste des laboratoires d'excellence référencés

CEA/LETI
MINATEC – 17, rue des Martyrs, 38054 Grenoble Cedex 8, France

EDSI
1, rue de Paris, 35510 Cesson-Sévigné, France

SERMA Technologies
30, avenue Gustave Eiffel, 33608 Pessac Cedex, France

THALES (TCS/CNES)
BPI1414 – 18, avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Annexe B Foire aux questions

1 Quelle est la charge maximale allouée au laboratoire d'excellence pour ces tests ?

La charge maximale des travaux d'expertise est fixée par les entités interbancaires et est de 2 hommes x mois (voir le chapitre 4).

2 Cette charge est-elle indépendante du nombre d'applications embarquées sur la carte ?

Oui, la charge maximale est de 2 hommes x mois indépendamment du nombre d'applications embarquées sur la carte.

3 Qui définit les profils (personnalisation) à fournir pour ces tests?

Si les profils de personnalisation ont un impact sur l'évaluation, les entités interbancaires valident le choix des profils sélectionnés.

4 Comment se déroule le suivi des travaux du laboratoire d'excellence au cours de l'expertise ?

Aucune interaction entre l'ANSSI et le laboratoire d'excellence n'est spécialement planifiée en dehors des cas suivants :

- difficulté administrative durant le déroulement des travaux ;
- découverte d'une vulnérabilité. Le laboratoire d'excellence alerte alors l'ANSSI qui en informe elle-même le développeur.

5 *Quelles sont les conséquences sur l'évaluation CC si le laboratoire d'excellence est en retard ?*

La mise en œuvre de la présente procédure a justement pour but d'assurer la synchronisation entre les deux évaluations (c'est-à-dire que l'expertise doit être terminée avant la fin de l'évaluation CC).

Si toutefois le laboratoire d'excellence ne peut pas livrer à temps ses résultats, seuls les résultats d'expertise disponibles avant la certification sont pris en compte.

6 Comment et par qui serait géré un éventuel retard de livraison des échantillons (suite au retard du projet, par exemple) vis-à-vis du créneau réservé au laboratoire d'excellence ?

L'ANSSI en réfère aux entités interbancaires qui identifient les suites à donner. Une des suites pouvant être de bloquer le processus de certification CC jusqu'à l'obtention des résultats d'expertise.

7 Quelles sont les conséquences sur l'évaluation CC si les règles décrites dans le paragraphe 6.1 ne sont pas respectées ?

L'ANSSI en réfère aux entités interbancaires qui identifient les suites à donner. Une des suites pouvant être de forcer la réalisation d'une expertise quitte à imposer des délais dans l'évaluation CC.

8 En cas de vulnérabilité détectée par le CESTI, puis corrigée par le développeur, le produit corrigé doit-il repasser les tests du laboratoire d'excellence ?

Non.

9 Concernant les échantillons, dans quel cadre le développeur peut-il contractualiser un engagement de confidentialité avec le laboratoire d'excellence ?

Le laboratoire d'excellence contractualise avec les entités interbancaires qui financent son expertise, et signe la convention d'expertise qui le lie aux autres acteurs de cette évaluation. La confidentialité des travaux du laboratoire d'excellence est couverte par ces contrats.

Toutefois, si le développeur le souhaite, il peut mettre en place un contrat de livraison et restitution sécurisées des échantillons avec le laboratoire d'excellence (qui est par ailleurs déjà tenu à la confidentialité par les clauses du contrat des entités interbancaires). Ce contrat, s'il a été jugé nécessaire, doit être limité à ces seuls aspects et ne doit pas interférer avec le déroulement de l'expertise.

10 En cas de vulnérabilité détectée par le laboratoire d'excellence, quel est le processus?

Dès qu'un problème impactant les résultats de l'évaluation CC est validé par le centre de certification, le développeur en est informé afin qu'il puisse déterminer au plus vite les évolutions nécessaires de ce produit (voir le chapitre 6.4).

La correction des problèmes identifiés par le laboratoire d'excellence est validée par le CESTI en charge de l'évaluation CC (voir chapitre 6.4).

11 Quel est l'impact sur l'évaluation en cours par le CESTI ?

L'impact est le même que si la vulnérabilité avait été trouvée pendant l'évaluation CC, par le CESTI ou par quelqu'un d'autre.

12 Après son expertise, le laboratoire d'excellence conserve-t-il les échantillons ?

Non, il s'engage à restituer ou à détruire l'ensemble des échantillons dès la fin de l'expertise.