
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 2000/05

Applications Oberthur B0' v1.0 et Routeur v1.0
conçues pour Multos v4.02

Novembre 2000

Ce document constitue le rapport de certification du produit "Applications Oberthur B0’ v1.0 et Routeur v1.0 conçues pour Multos v4.02".

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
Service Central de la Sécurité des Systèmes d’Information
51, boulevard de Latour-Maubourg
F-75700 PARIS 07 SP

mél : ssi20@calva.net



Ce document est folioté de 1 à 34 et certificat.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

# CERTIFICAT 2000/05

## Applications Oberthur B0' v1.0 et Routeur v1.0 conçues pour Multos v4.02

EAL4 Augmenté

| **Développeur :** | **Commanditaire :** |
|---|---|
| **Oberthur Card Systems** | **Crédit Mutuel** |

Le 20 novembre 2000,

Le Commanditaire :
Le Directeur du Crédit Mutuel

M. Claude BRUN

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 (conforme à la norme ISO 15408) 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 :
SGDN/SCSSI
51, boulevard de Latour-Maubourg
F-75700 PARIS 07 SP

IT Security Certified

Common Criteria

## Chapitre 1

# Introduction

1 Ce document représente le rapport de certification du produit “Applications Oberthur B0’ v1.0 et Routeur v1.0 conçues pour Multos v4.02”.

2 Ces applications sont conçues pour être chargées sur une carte à puce équipée du système d’exploitation multi-applications Multos v4.02.

3 L’application Routeur est destinée à aiguiller les commandes envoyées à la carte. L’application B0’ est destinée à être utilisée dans le système de débit/crédit “CB”.

4 Le niveau d’assurance atteint est le niveau EAL 4 augmenté des composants d’assurance AVA_VLA.3 “Résistance moyenne”, ALC_DVS.2 “Caractère suffisant des mesures de sécurité”, ADV_IMP.2 “Implémentation de la TSF” tels que décrits dans la partie 3 des Critères Communs [3].

# Chapitre 2

# Résumé

## 2.1 Contexte de l'évaluation

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

6 L'évaluation s'est déroulée de juin 1999 à septembre 2000.

7 Durant cette période, le développeur des applications, De La Rue Card Systems, est devenu Oberthur Card Systems et le site de développement a été transféré vers Puteaux.

## 2.2 Description de la cible d'évaluation

8 La cible d'évaluation est constituée des deux applications suivantes :

a) B0' : application bancaire conforme aux spécifications B4-B0' V2 du GIE Cartes Bancaires ;

b) Routeur : application permettant l'aiguillage des commandes pour les différentes applications chargées sur la carte.

9 Le circuit intégré et le système d'exploitation sur lesquels doivent être chargées ces deux applications ne font pas partie de la cible d'évaluation pour ce certificat.

## 2.3 Résumé des fonctions de sécurité évaluées

### 2.3.1 Résumé des fonctions de sécurité

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

- Contrôle d'accès aux informations stockées en mémoire,
- Irreversibilité des phases de vie de l'application B0',
- Traçabilité des opérations,
- Authentification des utilisateurs et administrateurs,
- Authentification des données utilisées,
- Réaction aux conditions anormales de fonctionnement des applications.

### 2.3.2 Niveau d'évaluation

11 Le niveau d'évaluation visé identifié dans la cible de sécurité [5] est le niveau EAL4 augmenté des composants d'assurance AVA_VLA.3 "Résistance moyenne", ALC_DVS.2 "Caractère suffisant des mesures de sécurité" et ADV_IMP.2 "Implémentation de la TSF" tels que décrits dans la partie 3 des Critères Communs [3].

12 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'attaques moyen tel qu'il est spécifié par le composant d'assurance AVA_VLA.3.

## 2.4 Acteurs dans l'évaluation

13 Le commanditaire de l'évaluation est :

Crédit Mutuel
6, rue de Ventadour
75001 PARIS
France

14 La cible d'évaluation a été développée par la société :

Oberthur Card Systems
25, rue Auguste Blanche
92800 PUTEAUX
France

15 L'évaluation a été conduite par le Centre d'Évaluation de la Sécurité des Technologies de l'Information d'Algoriel Consulting :

Algoriel Consulting
401 Avenue de la Fleuride
ZI les Paluds, BP 1018
13782 AUBAGNE
France

## 2.5 Conclusions de l'évaluation

16 Le produit soumis à évaluation satisfait aux exigences du niveau d'évaluation EAL4 augmenté des composants d'assurance AVA_VLA.3 "Résistance moyenne", ALC_DVS.2 "Caractère suffisant des mesures de sécurité" et ADV_IMP.2 "Implémentation de la TSF".

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

# Chapitre 3

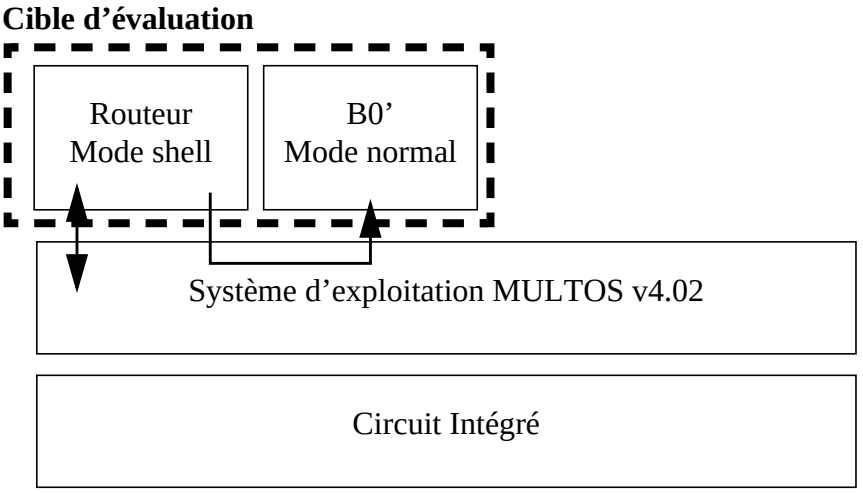
# Identification de la cible d'évaluation

## 3.1 Architecture de la cible d'évaluation

18 La cible d'évaluation est constituée des applications suivantes :

- B0' v1.0 développée par Oberthur Card Systems ;
- Routeur v1.0 développée par Oberthur Card Systems.

19 L'application Routeur est chargée en Mode shell ; cela signifie qu'elle reçoit l'intégralité des commandes envoyées à la carte. Son rôle est d'aiguiller ces commandes à travers le système d'exploitation Multos vers B0' ou vers une autre application chargée sur la carte.




## 3.2 Description du matériel

20 La cible d'évaluation n'est pas constituée de matériel.

## 3.3 Description du logiciel

21 La cible d'évaluation est constituée uniquement des applications B0' v1.0 et Routeur v1.0.

22 L'application B0' v1.0 est une application de débit-crédit conforme aux spécifications B4-B0' V2 du GIE Cartes Bancaires.

23 L'application Routeur v1.0 permet l'exécution sur une même carte multi-applications de l'application B0' et d'autres applications.

24 Le système d'exploitation Multos v4.02 ne fait pas partie de cette évaluation.

## 3.4 Description de la documentation

25 La documentation d'utilisation disponible pour les applications certifiées est la suivante :

- Contrat porteur émis par les banques à destination des porteurs de cartes bancaires "CB",
- Manuels émis par le GIE Cartes Bancaires à destination des personnalisateurs et des émetteurs de cartes.

# 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 Politique de sécurité

27 Les applications évaluées sont destinées à être chargées sur une carte à puce équipée du système d'exploitation multi-applications Multos v4.02.

28 Cette carte doit pouvoir être utilisée dans le système "CB".

## 4.3 Menaces

29 Les menaces couvertes par la cible d'évaluation ou par les mesures prises dans son environnement sont les suivantes :

- divulgation, vol ou modification d'informations ou d'éléments de la cible d'évaluation pendant son développement ;
- chargement non autorisé ou modification du code et des données de la cible d'évaluation lors de son chargement sur la plate-forme Multos ;
- personnalisation non autorisée ou divulgation, vol ou modification d'informations lors de la personnalisation ;
- utilisation non autorisée des services de la cible d'évaluation ;
- divulgation ou modification du code ou des données sensibles de la cible d'évaluation pendant son exploitation par :
  - des actions externes (commandes, I/O),
  - des actions internes (applications, système d'exploitation),
  - une utilisation dans des conditions anormales de fonctionnement ;
- répudiation des transactions ;
- répudiation de la personnalisation par un émetteur ;
- effacement non autorisé ou non-sûr de la cible d'évaluation.

30 Le détail de ces menaces est disponible dans la cible de sécurité [5].

## 4.4 Hypothèses d'utilisation et d'environnement

31 La cible d'évaluation doit être utilisée et administrée conformément aux exigences spécifiées dans la documentation d'utilisation et d'administration, et notamment dans les manuels émis par le GIE Cartes Bancaires pour le système "CB".

32 Les résultats de l'évaluation sont conditionnés par le respect des hypothèses sur l'utilisation et l'environnement d'utilisation de la cible d'évaluation suivantes :

- les procédures mises en place pour les différentes livraisons sont suffisantes pour garantir la confidentialité et l'intégrité des éléments transmis. Le personnel effectuant le transport est supposé de confiance ;
- le chargement et l'effacement des applications évaluées sont effectuées dans un environnement sûr et par des personnes de confiance ;
- la plate-forme Multos fournit des mécanismes de sécurité permettant de protéger le code et des données de la cible d'évaluation contre la modification ou la divulgation par une autre application ou par le système d'exploitation ;
- la plate-forme Multos fournit des mécanismes de sécurité garantissant le chargement et l'effacement sûr des applications.

33 Le détail de ces hypothèses est disponible dans la cible de sécurité [5].

## 4.5 Fonctions de sécurité évaluées

34 Les fonctions de sécurité évaluées sont les suivantes :

- Contrôle d'accès aux informations stockées en mémoire (en lecture, en écriture et en effacement) en fonction de la phase de vie de l'application B0', de l'utilisateur et de la zone mémoire visée ;
- Irreversibilité du cycle de vie de l'application B0',
- Traçabilité des opérations (écritures en mémoire, authentifications),
- Authentification des utilisateurs et administrateurs,
- Authentification de l'application utilisée,
- Authentification des transactions,
- Réaction aux conditions anormales de fonctionnement des applications.

## 4.6 Tests de la cible d'évaluation

35 L'évaluateur a effectué des tests fonctionnels sur le produit afin de vérifier la conformité des fonctions de sécurité à leurs spécifications en utilisant le plan de test fourni par le développeur.

36 De plus, l'évaluateur a effectué de manière indépendante un ensemble de tests de pénétration sur le produit afin d'estimer l'efficacité des fonctions de sécurité offertes par le produit. Ces tests de pénétration sont adaptés à la nature du produit soumis à évaluation ainsi qu'à son environnement d'exploitation supposé. Ils permettent de s'assurer que le produit évalué resiste aux attaques correspondant à un potentiel d'attaque moyen tel que défini par le composant AVA_VLA.3.

# Chapitre 5

# Résultats de l'évaluation

## 5.1 Rapport Technique d'Évaluation

37 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [6].

## 5.2 Résultats de l'évaluation de la cible de sécurité

38 La cible de sécurité répond aux exigences de la classe ASE, telle que définie dans la partie 3 des Critères Communs [3].

### 5.2.1 ASE_DES.1 : Description de la TOE

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

40 La cible d'évaluation (TOE) est constituée des applications Router v1.0 et B0' v1.0. La description de la cible d'évaluation est précisée au chapitre 3 du présent rapport de certification.

### 5.2.2 ASE_ENV.1 : Environnement de sécurité

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

42 Les menaces auxquelles doit faire face le produit, les hypothèses d'utilisation et d'environnement ainsi que les politiques de sécurité organisationnelles que la cible d'évaluation doit respecter sont décrites dans la cible de sécurité [5]. Ces caractéristiques sont résumées au chapitre 4 de ce rapport de certification.

### 5.2.3 ASE_INT.1 : Introduction de la ST

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

44 L'introduction de la cible de sécurité [5] précise l'identification du produit et contient une vue d'ensemble de la cible de sécurité, ainsi qu'une annonce de conformité aux Critères Communs.

### 5.2.4 ASE_OBJ.1 : Objectifs de sécurité

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

46 Les objectifs de sécurité pour la cible d'évaluation ainsi que pour l'environnement sont décrits dans la cible de sécurité [5].

### 5.2.5 ASE_PPC.1 : Annonce de conformité à un PP

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

48 Aucune conformité à un profil de protection n'est annoncée.

### 5.2.6 ASE_REQ.1 : Exigences de sécurité des TI

49 Les critères d'évaluation sont définis par les sections ASE_REQ.1.iE de la classe ASE, telle que spécifiée dans les parties 2 et 3 des Critères Communs [2] et [3].

50 Les exigences de sécurité des TI fonctionnelles ou d'assurance sont décrites dans la cible de sécurité [5].

51 Le niveau d'assurance visé est le niveau EAL4 augmenté des composants AVA_VLA.3 "Résistance moyenne", ALC_DVS.2 "Caractère suffisant des mesures de sécurité", ADV_IMP.2 "Implémentation de la TSF".

### 5.2.7 ASE_SRE.1 : Exigences de sécurité des TI explicitement énoncées

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

53 La cible de sécurité [5] ne contient pas d'exigences de sécurité des TI explicitement énoncées.

### 5.2.8 ASE_TSS.1 : Spécifications globales de la TOE

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

55 La cible de sécurité [5] contient un résumé des spécifications des fonctions de sécurité du produit ainsi que les mesures d'assurance prises pour satisfaire les exigences d'assurance.

56 L'évaluateur s'est assuré que ces fonctions de sécurité sont une représentation correcte des exigences fonctionnelles de sécurité et que les mesures d'assurance prises couvrent les exigences du niveau EAL4 augmenté.

## 5.3 Résultats de l'évaluation du produit

57 Le produit répond aux exigences des Critères Communs pour le niveau EAL4 augmenté des composants AVA_VLA.3 "Résistance moyenne", ALC_DVS.2 "Caractère suffisant des mesures de sécurité", ADV_IMP.2 "Implémentation de la TSF" tels que décrits dans la partie 3 des Critères Communs [3].

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

58 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].

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

60 L'évaluateur a examiné ces spécifications et montré pour le niveau considéré qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du produit.

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

61 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].

62 Le développeur a fourni un modèle informel de la politique de sécurité de la TOE.

63 L'évaluateur a examiné ce modèle et montré que toutes les fonctions de sécurité décrites dans les spécifications fonctionnelles constituent une représentation complète et homogène de ce modèle.

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

64 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].

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

66 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 TOE.

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

67 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].

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

69 Cette conception décrit les modules constitituant le produit et l'ensemble de leurs interfaces. L'évaluateur s'est assuré que cette conception de bas niveau est une instantiation correcte et complète des exigences fonctionnelles de sécurité de la TOE.

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

70 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].

71 Le développeur a fourni l'intégralité du code source des applications.

72 Une analyse détaillée du code source a été effectuée par les évaluateurs afin, d'une part, de vérifier que ces éléments de réalisation constituent une représentation correcte et complète des exigences fonctionnelles de sécurité de la TOE, et d'autre part, de rechercher des vulnérabilités potentielles.

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

73 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].

74 Le développeur a fourni une documentation qui indique les correspondances entre les différents niveaux de représentation des fonctions de sécurité de la TOE.

75 L'évaluateur a donc pu s'assurer de la conformité des spécifications fonctionnelles de sécurité à travers la conception de haut niveau, la conception de bas niveau ainsi que son implémentation.

### 5.3.7 ACM_AUT.1 : Automatisation partielle de la CM

76 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].

77 Le développeur a fourni la documentation du système de gestion de configuration utilisé pour le développement des applications chez De La Rue Card Systems puis Oberthur Card Systems.

78 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.

79 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.

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

80 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].

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

82 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). Des procédures gèrent également les révisions majeures et mineures de la cible d'évaluation.

83 Le système de gestion de configuration énumère ainsi tous les modules élémentaires à partir desquels la cible d'évaluation a été construite.

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

84 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].

85 Le système de gestion de configuration appliqué par le développeur couvre le produit ainsi que l'ensemble de sa documentation ; il couvre également toute erreur de sécurité qui pourrait être découverte ; il contrôle donc la documentation de conception du produit, la documentation de test du produit, les éléments de réalisation du produit (code source).

86 La documentation d'utilisation et la documentation d'administration est quant à elle gérée par le GIE Cartes Bancaires.

### 5.3.10 ADO_DEL.2 : Détection de modification

87 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].

88 Le développeur a fourni les procédures de livraison des applications au responsable du chargement. Leur application a été vérifiée au cours d'une visite sur le site de développement.

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

89 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].

90 Les procédures d'installation, de génération et de démarrage du produit concernent le formatage des applications en format ALU, la demande de certificat à MAOSCO et leurs chargement sur les cartes Multos.

91 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation.

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

92 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].

93 Le développeur a fourni la documentation d'administration des fonctions de sécurité du produit. Ces guides d'administration sont à usage :

- des personnalisateurs des applications,
- des émetteurs et délégataires des émetteurs.

94 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.

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

95 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].

96 Le développeur a fourni la documentation d'utilisation des fonctions de sécurité du produit. Ces guides d'utilisation sont à usage :

- des porteurs de cartes de paiement "CB",
- des développeurs de Terminaux de Paiement Électronique,
- des développeurs de Distributeurs Automatiques de Billets.

97 L'évaluateur s'est assuré que cette documentation permet une utilisation sûre du produit.

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

98 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].

99 L'évaluateur a analysé la sécurité de l'environnement de développement des applications sur le site de Gentilly (De La Rue Card Systems) puis s'est assuré, suite au changement de locaux, du stockage sûr des archives du projet sur le site de Puteaux (Oberthur Card Systems).

100 Des procédures physiques, organisationnelles, techniques et liées au personnel assurent un niveau de protection suffisant de la cible d'évaluation, de ses constituants ainsi que de sa documentation. Des visites sur chacun des sites ont permis de vérifier l'application de ces procédures.

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

101 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].

102 Le développeur a fourni le modèle de cycle de vie des applications.

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

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

104 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].

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

106 L'évaluateur a examiné cette documentation et s'est assuré de l'absence d'incohérences dans cette documentation. L'analyse de l'implémentation du produit (ADV_IMP.2) a également permis à l'évaluateur de confirmer la complétude de cette documentation.

### 5.3.17 ATE_FUN.1 : Tests fonctionnels

107 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].

108 Le développeur a fourni la documentation de tests du produit. Les tests fournis par le développeur correspondent à un ensemble de tests logiciels des fonctions de sécurité des applications.

109 Une documentation détaillée de tests a été fournie pour chacun des tests ; ces documentations décrivent le plan des tests, l'objectif des tests, les procédures de tests à réaliser ainsi que les résultats des tests.

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

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

111 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].

112 Le développeur a fourni une analyse de la documentation de tests justifiant la couverture des fonctions de sécurité par les tests.

113 L'évaluateur a confirmé cette analyse.

### 5.3.19 ATE_DPT.1 : Tests : conception de haut-niveau

114 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].

115 Le développeur a fourni une analyse de la documentation de tests justifiant la réalisation de tests fonctionnels pour les sous-systèmes identifiés dans la conception de haut niveau des applications.

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

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

117 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].

118 Une partie des tests fonctionnels du développeur a été réexécuté et des tests complémentaires développés par l'évaluateur ont été effectués pour démontrer que les fonctions de sécurité fonctionnent conformément à leurs spécifications.

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

119 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].

120 Le développeur a fourni une analyse des guides d'installation, de génération, de démarrage, d'utilisation et d'administration de la cible d'évaluation. L'objectif de cette analyse est de garantir que des éléments trompeurs, déraisonables ou contradictoires sont absents de ces guides et que les procédures sûres pour tous les modes d'exploitation ont été prises en compte.

121 L'évaluateur s'est assuré de la complétude de cette analyse et a appliqué de nouveau ces procédures afin de confirmer que le cible d'évaluation peut être configurée et utilisée de manière sûre en n'utilisant que les guides fournis.

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

122 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].

123 Le développeur a fourni une analyse de la résistance des fonctions de sécurité du produit. L'évaluateur a analysé cette documentation et mené des analyses complémentaires. La cotation indépendante des mécanismes faite par les évaluateurs est en accord avec les analyses des développeurs.

124 La résistance des fonctions de sécurité est considérée comme moyenne (SOF-medium).

### 5.3.23 AVA_VLA.3 : Résistance moyenne

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

126 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 de manière indépendante.

127 L'évaluateur a réalisé des tests de pénétration, basés sur son analyse de vulnérabilités afin de pouvoir vérifier que le produit résiste aux attaques

correspondant à un potentiel de l'attaquant tel que défini par le composant AVA_VLA.3 "Résistance moyenne".

128 Les tests réalisés ont porté uniquement sur les applications Routeur et B0'.

### 5.3.24 Verdicts

129 Pour tous les aspects des Critères Communs identifiés ci-dessus, un avis "réussite" a été émis.

# Chapitre 6

# Recommandations d'utilisation

130 La cible d'évaluation "Applications Oberthur B0' v1.0 et Routeur v1.0 conçues pour Multos v4.02" est soumise aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

131 Le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [5].

## 6.1 Chargement et effacement

132 Le chargement et l'effacement des applications évaluées doivent être impérativement effectués dans un environnement sûr et par des personnes autorisées et de confiance.

133 La plate-forme Multos sur laquelle sont chargées les applications doit impérativement fournir des fonctionnalités de chargement et d'effacements sécurisés.

## 6.2 Personnalisation

134 Le processus de personnalisation est une étape critique destinée à configurer le produit de manière sûre.

135 La personnalisation doit être strictement définie et contrôlée ; des mesures de sécurité doivent être appliquées au cours de la personnalisation afin de pouvoir garantir l'intégrité et la confidentialité des données secrètes introduites dans le produit.

## 6.3 Fonctionnalités de sécurité offertes par la plate-forme Multos

136 Pour cette évaluation, la plate-forme Multos est supposée fournir les fonctionnalités de sécurité suivantes :

- protection du code et des données de la cible d'évaluation contre la modification ou la divulgation par une autre application ou par le système d'exploitation,
- chargement et effacement sécurisé des applets.

137 L'émetteur de la carte doit donc s'assurer que la plate-forme utilisée fournit bien ces fonctions. Pour cela, il peut s'appuyer sur une évaluation ou sur un certificat, à un niveau suffisant, émis pour cette plate-forme.

## 6.4 Porteurs

138 Le porteur doit utiliser sa carte conformément aux recommandations fournies par l’émetteur, sa banque. Il est notamment le seul responsable de la protection du code PIN qui lui est fourni avec sa carte.

# Chapitre 7

# Certification

## 7.1 Objet

139 Le produit dont les caractéristiques de sécurité sont définies dans la cible de sécurité [5], satisfait aux exigences du niveau d'évaluation EAL4 augmenté des composants d'assurance suivants décrits dans la partie 3 des Critères Communs [3] :

- AVA_VLA.3 "Résistance moyenne",
- ALC_DVS.2 "Caractère suffisant des mesures de sécurité",
- ADV_IMP.2 "Implémentation de la TSF".

140 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 moyen tel qu'il est spécifié par le composant d'assurance AVA_VLA.3.

## 7.2 Portée de la certification

141 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.

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

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

# Annexe A

# Glossaire

## A.1 Abréviations

| | |
|---|---|
| **CC** | (Common Criteria) - Critères Communs, l'intitulé utilisé historiquement pour la présente norme à la place de l'intitulé officiel de l'ISO 15408 : "Critères d'évaluation de la sécurité des technologies de l'information" |
| **EAL** | (Evaluation Assurance Level) - Niveau d'assurance de l'évaluation |
| **PP** | (Protection Profile) - Profil de protection |
| **SF** | (Security Function) - Fonction de sécurité |
| **ST** | (Security Target) - Cible de sécurité |
| **TI** | (IT : Information Technology) - Technologie de l'Information |
| **TOE** | (Target of Evaluation) - Cible d'évaluation |
| **TSF** | (TOE Security Functions) - Ensemble des fonctions de sécurité de la TOE |

## A.2 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 à un EAL ou à un paquet d'assurance. |
| **Chargeur** | Industriel responsable du chargement des applets sur une plate-forme multi-applications. |
| **Cible d'évaluation (TOE)** | Un produit ou un système TI et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation. |
| **Cible de sécurité (ST)** | Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée. |
| **Classe** | Un groupement de familles qui partagent un thème commun. |
| **Emetteur** | Banque ou organisme émetteur de la carte de débit/crédit. |
| **Encarteur** | Industriel insérant un composant masqué dans un support plastique au format d'une carte. |
| **Evaluation** | Estimation d'un PP, d'une ST ou d'une TOE par rapport à des critères définis. |
| **Fonction de sécurité** | Une partie ou des parties de la TOE sur lesquelles on s'appuie pour appliquer un sous-ensemble étroitement imbriqué de règles tirées de la TSP. |
| **Informel** | Qui est exprimé à l'aide d'un langage naturel. |
| **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 CC. |
| **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 d'un carte de débit/crédit. |
| **Produit** | Un ensemble de logiciels, microprogrammes ou matériels TI 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 TOE, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs. |
| **Utilisateur** | Toute entité (utilisateur humain ou entité TI externe) hors de la TOE qui interagit avec elle. |

## 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] Common Methodology for Information Technology Security Evaluation CEM-99/045, version 1.0 August 1999.

[5] Cible de sécurité "B0' on Multos Security Target", issue 2-AA, septembre 2000 (diffusion limitée).

[6] Rapport technique d'évaluation RAP/BLD/SG/00.05.1677 version 1, août 2000 + Mémorandum MEM/BLD/SG/00.10.1873 (diffusion limitée).