
PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

# Rapport de certification ANSSI-CC-2018/35

# Plateforme IDMotion V2 masquée sur le composant IFX_CCI_000014h

## OS Multos V4.5.2, AMD version 0151v001

*Paris, le 30 août 2018*

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

Guillaume POUPARD
[ORIGINAL SIGNE]

# 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 termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

*Référence du rapport de certification*

# ANSSI-CC-2018/35

*Nom du produit*

## Plateforme ID Motion V2

*Référence/version du produit*

## OS version Multos V4.5.2
## AMD version 0151v001

*Conformité à un profil de protection*

## Néant

*Critères d'évaluation et version*

## Critères Communs version 3.1 révision 5

*Niveau d'évaluation*

## EAL 5 augmenté
**ALC_DVS.2, AVA_VAN.5**

*Développeurs :*

### Gemalto
**La Vigie, Avenue du jujubier, ZI Athélia IV, BP 90- 13702 La Ciotat**

### Infineon Technologies AG
**Am Campeon 1-12**
**85579 Neubiberg**

*Commanditaire*

### Gemalto
**La Vigie, Avenue du jujubier, ZI Athélia IV, BP 90- 13702 La Ciotat**

*Centre d'évaluation*

### THALES (TCS – CNES)
**290 allée du Lac, 31670 Labège, France**

*Accords de reconnaissance applicables*

**CCRA**

**SOG-IS**

**Ce certificat est reconnu au niveau EAL2.**

# 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 modifié. Ce décret indique que :

- L'agence nationale 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 rendus publics (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 sont disponibles sur le site Internet www.ssi.gouv.fr.

# Table des matières

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la « Plateforme IDMotion V2 masquée sur le composant IFX_CCI_000014h, OS version Multos V4.5.2, AMD version 0151v001 » développée par *GEMALTO* et *INFINEON TECHNOLOGIES AG*.

Le produit évalué est de type « carte à puce » avec et sans contact. Il est conçu de façon à ce que plusieurs applications puissent être chargées et exécutées de façon sécurisée sur la carte à puce. Ces applications sont écrites dans un langage, indépendant du composant sous-jacent, nommé MEL[1]. Les applications en langage MEL sont interprétées par le système d'exploitation Multos.

## 1.2. Description du produit

### *1.2.1. Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité s'inspire du profil de protection [PP/0010] certifié par l'ANSSI.

### *1.2.2. Services de sécurité*

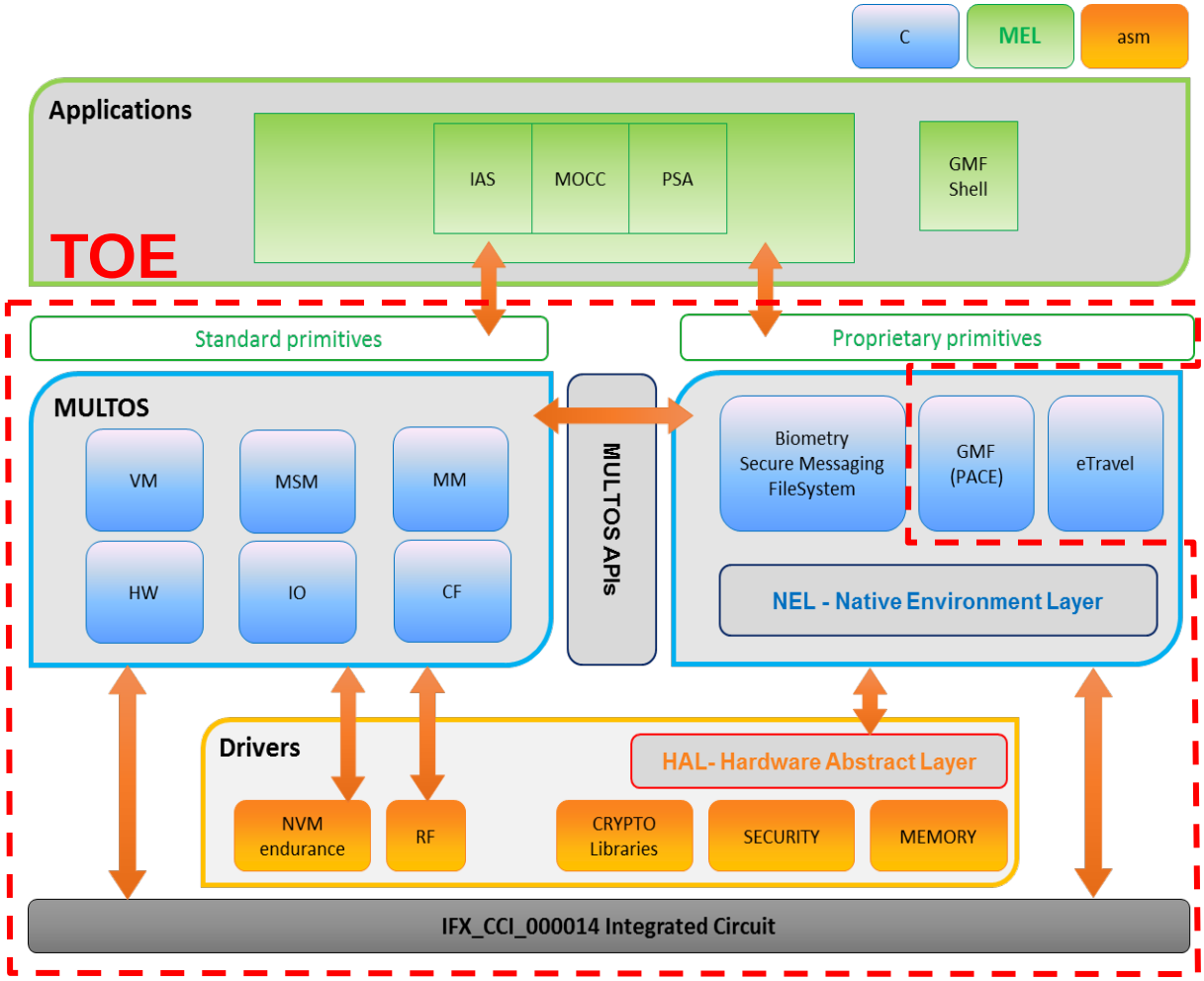
Les principaux services de sécurité fournis par le produit sont :

- le chargement d'applications ;
- la suppression d'applications ;
- la vérification de la signature des applications ;
- le déchiffrement des applications ;
- le chargement des données de contrôle MSM[2] ;
- l'écrasement des données critiques ;
- la gestion de l'exécution des applications ;
- la protection de la réinitialisation ;
- le contrôle d'intégrité des données sensibles de la plateforme (applications, clés internes…) ;
- l'autotest au démarrage et pendant l'initialisation ;
- la gestion des réactions aux tentatives de pénétration ;
- l'authentification de la carte ;
- la protection du chargement d'applications *post-issuance* ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

[1] *Multos Executable Language* - langage exécutable Multos.
[2] *Multos Security Manager* - gestionnaire de sécurité Multos.

### *1.2.3. Architecture*

L'architecture du produit est illustrée par la figure suivante :




***VM:*** *Virtual Machine*
***MSM:*** *Multos Security Manager*
***MM:*** *Application Memory Manager Subsystem*
***CF:*** *Cryptographic Functions subsystem*
***IO:*** *I/O Communications subsystem*
***HW:*** *Hardware Services subsystem*
***NVM:*** *Non Volatile Memory*

**Figure 1 : Architecture du produit**

Le produit est constitué des éléments suivants :

- du circuit intégré IFX_CCI_000014 développé et fabriqué par *INFINEON TECHNOLOGIES AG ;*
- du sous-système *hardware-dependent*, appelé « *drivers* » ;
- de la plateforme Multos avec sa machine virtuelle et ses API ;
- des primitives propriétaires incluant :
    - le module *Biometry Secure Messaging fileSystem* (inclus dans la TOE, mais hors TSF) ;
    - l'application ETravel EAC/PACE/BAC v2.4 chargée en Flash (hors TOE, mais faisant partie de l'image de la TOE) ;
    - l'application native GMF v1.0 (hors TOE),

- des applications Multos chargées en NVM et exécutées par la machine virtuelle Multos (hors TOE) :
    - Pin Server Application (PSA) v0.2 ;
    - IAS Classic v4.4.1C ;
    - MOC client (MOCC) v1.0.2A.

Bien que ces applications ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN].

### *1.2.4. Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 2 « introduction ».

| Configuration de la TOE | Données lues | Origine |
|---|---|---|
| OS version Multos V4.5.2 | 000452 | GEMALTO |
| Version du code correctif (AMD) IDMotion V2 | 0151001 | |
| Build number 1.1.42 | 00010001002A | |
| Identifiant de la plateforme | 16 | |
| Donnée d'identification du circuit intégré IFX_CCI_000014 | 00 00 14 | *INFINEON TECHNOLOGIES AG* |

**Tableau 1 : Identification du produit**

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET CONFIGURATION DATA. La procédure d'identification du produit est décrite dans le guide [MDRM].

La principale différence entre le produit et la TOE correspond aux applications chargées pré-émission sur ce produit. Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après.

| Nom, version de l'application | Identification | Nom du *codelet* |
|---|---|---|
| IAS classic v4.4.1C | 0x00B8 | IASClassic.app,Codelet |
| MOC client v1.0.2A | 0x00B9 | MOCClient.app,Codelet |
| PSA v0.2 | 0x00B7 | PSACodelet.app,Codelet |

**Tableau 2 : Applications chargées sur le produit**

La commande GET CONFIGURATION DATA (Codelets) permet à l'utilisateur du produit de vérifier quelles applications sont installées dans le produit à sa disposition.

### *1.2.5. Cycle de vie*

Le cycle de vie du produit, détaillé au chapitre « *2.5.4 Smartcard Product Life Cycle* » de la cible de sécurité [ST], est celui d'une carte à puce (voir Figure 2), à l'exception du point de livraison qui s'effectue à la fin de la phase 5.

Les phases 1 à 5 correspondent à la construction de la TOE. Elles ont été prises en compte dans la présente évaluation, avec, pour les phases 2 et 3, une réutilisation des résultats de l'évaluation du composant, voir [CR_IC]. Aucune procédure de patching n'est possible après la phase 5.

La phase 6 correspond à la personnalisation du produit. La phase 7 correspond quant à elle à la phase opérationnelle du produit. Ces phases sont couvertes par des recommandations sécuritaires (voir [GUIDES]).

Les sites de développement et de fabrication du circuit intégré sont détaillés dans le rapport de certification [CR-IC]. Les sites de développement et de fabrication du produit sont indiqués dans la Figure 2, ci-après.

| | Phase | Description / comments | | Who | Where |
|---|---|---|---|---|---|
| ALC | 1 | IDMotion V2 platform development | Platform development, Primitives integration & tests | **Gemalto** MULTOS R&D team secure environment | **Gemalto Sydney** **Gemalto Fareham UK** |
| | | | | **Gemalto** SL Crypto team secure environment | **Gemalto Meudon (Fr)** **Gemalto La Ciotat (Fr)** |
| | | | | **Gemalto** GBU R&D team secure environment | **Gemalto Meudon** **Gemalto Singapore** |
| | 2 | IC development | IC development | **IC developer** secure environment | IC development site(s) Refer to [CR-IC] |
| | 3 | IC manufacturing | Manufacturing of virgin integrated circuits embedding a flash loader protected by a dedicated transport key. | **IC manufacturer** secure environment | IC manufacturing site(s) Refer to [CR-IC] |
| | 4 | SC manufacturing: IC packaging, also called "assembly" | IC packaging & testing | **Gemalto or IFX (for contactless only)** Production teams secure environment | **Gemalto Gémenos** **Gemalto Singapore** **Gemalto Vantaa** |
| | 5 | SC manufacturing & pre-personalization | ▪ Module embedding (ICC, smartcard, inlays/booklets, modules, or chips)<br>▪ Loading of the Gemalto software (platform and applications)<br>▪ SC initialization (profile building, loading of data needed for card pre-personalization…) | **Gemalto** Production teams secure environment | **Gemalto Gémenos** **Gemalto Singapore** **Gemalto Vantaa** **Gemalto Tczew** **Gemalto Curitiba** **Gemalto Montgomery** |
| Point de Livraison | | | | | |
| AGD | 6 | SC Personalization | Creation of files and loading of end-user data | **SC Personalizer:** Gemalto or another accredited company secure environment | SC Personalizer site |
| | 7 | End-usage | End-usage for SC issuer | **SC Issuer** | Field |
| | | | End-usage for cardholder | **Cardholder** | Field |

**Figure 2 : Cycle de vie du produit**

Le guide [GALU] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs, les guides [SEC_GUID] et [MDRM] décrivent les règles de développement des applications destinées à être chargées sur cette carte.

### *1.2.6. Configuration évaluée*

Le certificat porte sur la configuration telle que présentée par le Tableau 1 : Identification du produit.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.
Toutes les applications identifiées dans le Tableau 2 ont été vérifiées conformément aux contraintes décrites dans [GUIDES].

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].
Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

## 2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « IFX_CCI_000014h » au niveau EAL6 augmenté du composant ALC_FLR.1, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le *10 juillet* 2017 sous la référence BSI-DSZ-CC-0945-2017, voir [CR-IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 5 juillet 2018, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

## 2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

## 2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CR-IC]).
Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

# 3. La certification

## 3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Plateforme IDMotion V2 masquée sur le composant IFX_CCI_000014h, OS version Multos V4.5.2, AMD version 0151v001 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

## 3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doivent respecter les contraintes de développement de la plateforme ([SEC_GUID] et [MDRM]) ;
- pour le chargement de futures applications sur le produit, ces dernières devront appliquer la procédure de vérification evaluée de Gemalto ([SEC_GUID], [GALU] et [VP]) ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doit être activée conformément aux indications de [GDLA] ;
- la protection du chargement de toutes les applications chargées *pre-issuance* doit être activée conformément aux indications de [GDLA].

## 3.3. Reconnaissance du certificat

### *3.3.1. Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

### *3.3.2. Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

# Annexe 1. Niveau d'évaluation du produit

| Classe | Famille | Composants par niveau d'assurance | | | | | | | Niveau d'assurance retenu pour le produit | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 5+ | Intitulé du composant |
| **ADV Développement** | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Security architecture description |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 | **5** | Complete semi-formal functional specification with additional error information |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 | **1** | Implementation representation of the TSF |
| | ADV_INT | | | | | 2 | 3 | 3 | **2** | Well-structured internals |
| | ADV_SPM | | | | | | 1 | 1 | | |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 | **4** | Semiformal modular design |
| **AGD Guides d'utilisation** | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Operational user guidance |
| | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Preparative procedures |
| **ALC Support au cycle de vie** | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 | **4** | Production support, acceptance procedures and automation |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 | **5** | Development tools CM coverage |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Delivery procedures |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 | **2** | Sufficiency of security measures |
| | ALC_FLR | | | | | | | | | |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 | **1** | Developer defined life-cycle model |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 | **2** | Compliance with implementation standards |
| **ASE Evaluation de la cible de sécurité** | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Conformance claims |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Extended components definition |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | ST introduction |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | **2** | Security objectives |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | **2** | Derived security requirements |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Security problem definition |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | TOE summary specification |
| **ATE Tests** | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 | **2** | Analysis of coverage |
| | ATE_DPT | | | 1 | 1 | 3 | 3 | 4 | **3** | Testing: modular design |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 | **1** | Functional testing |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 | **2** | Independent testing: sample |
| **AVA Estimation des vulnérabilités** | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 | **5** | Advanced methodical vulnerability analysis |

# Annexe 2. Références documentaires du produit évalué

| | |
|---|---|
| [ST] | Cible de sécurité de référence pour l'évaluation :<br>- IDMotion V2 Platform Security target, référence ST_D1172991, version 1.94, 27 juin 2018, Gemalto.<br><br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>- IDMotion V2 Platform Security target public version, reference ST_D1172991_P, version 1.2, Gemalto. |
| [RTE] | Rapport technique d'évaluation :<br>- Evaluation technical report project Bolero_A, référence BOLA_ETR, version 2.0, 5 juillet 2018.<br><br>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :<br>- Evaluation Technical Report for composite evaluation Project: Bolero_A, référence BOLA_ETRLite, version 1.0, 28 août 2018. |
| [CONF] | Liste de configuration du produit :<br>- LIS__ceryneia.CC-delivery_004 / 004, 28 février 2018 ;<br>- LIS__cceryneia.Ccdoc-Labo-delivery_001 / 001, 28 juin 2018. |
| [GUIDES] | - Multos Enablement, référence MAO-DOC-TEC-101, version 1.2 ;<br>- [GALU] Multos GALU, Guide to Generating Application Load Units, référence MAO-DOC-TEC-009, version 2.9 ;<br>- [GLDA] Multos GLDA, Guide to Loading and Deleting, reference MAO-DOC-TEC-008, version 2.28 ;<br>- [MDRM] Multos MDRM, Multos Developer's Reference Manual, référence MAO-DOC-TEC-006, version 1.54 ;<br>- Card Initialization Specification Multos ID Motion V2, référence CIS_Multos_ID_Motion_V2, version A01.10 ;<br>- [SEC_GUID] Security Guidance for MULTOS Application Developers, référence MI-MA-0031, version 1.6 ;<br>- [VP] Mask Verification Procedure, référence MI-PR-0012, version 1.1. |
| [CR-IC] | Certification Report BSI-DSZ-CC-0945-2017 for IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch and IFX_CCI_00001Dh design step H13 including optional software libraries and dedicated firmware from Infineon Technologies AG. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 10 juillet 2017.* |
| [PP/0010] | Protection Profile Smart Card Integrated Circuit With Multi-Application Secure Platform, version 2.0, novembre 2000. *Certifié par l'ANSSI sous la référence PP/0010.* |
| [PP0084] | Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.* |

# Annexe 3. Références liées à la certification

| | |
|---|---|
| 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. | |
| [CER/P/01] | Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation :<br>- Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;<br>- Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;<br>- Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004. |
| [JIWG IC] * | Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009. |
| [JIWG AP] * | Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013. |
| [COMP] * | Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.4, août 2015. |
| [OPEN] | Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013. |
| [CC RA] | Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014. |
| [SOG-IS] | Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee. |
| [REF] | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr. |

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.