



*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

**Rapport de maintenance**  
**ANSSI-CC-2016/66-M01**

**IDEal Citiz v2.1.1 Open platform**  
**Version 2.1.1-M01**

**Certificat de référence : ANSSI-CC-2016/66**

*Paris, le 14 mars 2017*

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

Guillaume POUPARD  
[ORIGINAL SIGNE]



## 1. Références

[CER]	IDEal Citiz v2.1.1 Open platform on M7892 B11, certificat ANSSI-CC-2016/66 du 21 octobre 2016.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	Rapport d'analyse d'impact « EAGLE-R-M Ideal Citiz V2.1.1-M01 », référence 2016_2000022397, version 2.0 du 12/01/2017.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.

## 2. Identification du produit maintenu

Le produit « IDEal Citiz v2.1.1 Open platform on M7892 B11 », version 2.1.1, a été initialement certifié sous la référence ANSSI-CC-2016/66 (référence [CER]).

Le produit objet de la présente maintenance est « IDEal Citiz v2.1.1 Open platform Version 2.1.1-M01 », version 2.1.1 développé par la société *SAFRAN IDENTITY & SECURITY (ex-MORPHO)*.

La version maintenue du produit est identifiable par les éléments suivants :

- les *Card Production and Life Cycle (CPLC) Data* indiquent les valeurs suivantes :

Donnée	Valeur
IC Fabricator	0x8100
IC Type <sup>1</sup>	0x7805 pour SLE78CLFX4000PM
	0x7801 pour SLE78CLFX4000P
	0x7813 pour SLE78CFX4000P
Operating System Identifier	0x4921
Operating System Release Date	0x <b>6335</b>
Operating System Release Level	0x2111

- et la valeur de la donnée *Hardware security integrity* est 0x448C448C48C6.

Cette nouvelle version contenant le patch version 7.0, apparait au travers de la réponse précédente, paramètre « Operating System Release Date » égal à **6335** au lieu de 6141 dans le produit initialement certifié.

<sup>1</sup> SLE78CLFX4000P, SLE78CLFX4000PM et SLE78CFX4000P désignent les trois configurations commerciales du composant M7892 B11.

### 3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications fonctionnelles suivantes ont été opérées :

- modification dans la gestion de la longueur du codage TLV (*Tag, Length, Value*) afin de prendre en compte l'encodage *Basic Encoding Rule* (BER) pour une taille jusqu'à 5 octets ;
- modification de la fonction « *unwrap* » afin de supporter la longueur de codage du BER pour le MAC ;
- la liste et le nombre d'applets chargés dans la plate-forme a changé. Cette liste est vérifiable avec la fonction `f_osj_MM_SER_v_PreparePreloadedAppletsContent'`.

#### 4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables, du produit évalué et sont applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	<p>Liste des guides du produit :</p> <ul style="list-style-type: none"> <li>- Ideal Citiz v2.1.1 – Basic Applet Development Recommendations, référence 2015_2000013511, version 1.0, 19 janvier 2016, Morpho ;</li> <li>- Ideal Citiz v2.1.1 – Secure Applet Development Recommendations, référence 2015_2000013510, version 1.1, 20 avril 2016, Morpho ;</li> <li>- Ideal Citiz v2.1.1 – Verification Authority Rules, référence 2015_2000013512, version 1.0, 22 janvier 2016, Morpho ;</li> <li>- IDEalcitiz_v2.1.1 – Operational user guidance, référence 2015_2000011705, version 6, 14 septembre 2016, Morpho ;</li> <li>- IDEalcitiz_v2.1.1 – Global Platform and JavaCard API, référence 2015_2000012154, version 2.0, 8 octobre 2015, Morpho ;</li> </ul>	[CER]
	<ul style="list-style-type: none"> <li>- Ideal Citiz v2.1.1 – Preparative procedure, référence 2015_2000011704, version 06, 20 décembre 2016, Morpho.</li> </ul>	[R-M01]
[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- Maintenance Security Target – IDEal Citiz v2.1.1-M01 Open Platform, référence 2016_2000022486, version 5.5, 7 février 2017, Morpho.</li> </ul> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> <li>- Maintenance Security target Lite IDEal Citiz v2.1.1-M01 Open Platform, version 1.2, référence 2016_2000023886, 7 février 2017, Morpho.</li> </ul>	[R-M01]
[CONF]	<p>Liste de configuration du produit :</p> <p>Software release sheet for Ideal Citiz V2.1.1 400K, référence 2016_2000017236, version 9, 21 décembre 2016, Morpho.</p>	[R-M01]

## 5. Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact mineur. Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée.

Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

## 6. Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

## 7. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ». Reconnaissance européenne (SOG-IS)

Le certificat initial a été 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<sup>1</sup>, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



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

Le certificat initial a été émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires<sup>2</sup>, 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 :



---

<sup>1</sup> Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

<sup>2</sup> Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.