



**PREMIER  
MINISTRE**

*Liberté  
Égalité  
Fraternité*

**Secrétariat général de la défense  
et de la sécurité nationale**

Agence nationale de la sécurité  
des systèmes d'information

# **Rapport de certification ANSSI-CSPN-2021/27**

## **INWallet Mobile Middleware Version 2.1.3, pour Android**

Paris, le 8 octobre 2021

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 présumées 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](mailto:certification@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	<b>ANSSI-CSPN-2021/27</b>
Nom du produit	<b>INWallet Mobile Middleware</b>
Référence/version du produit	<b>Version 2.1.3, pour Android</b>
Catégorie de produit	<b>Identification, authentification et contrôle d'accès</b>
Critère d'évaluation et version	<b>CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)</b>
Commanditaire	<b>IMPRIMERIE NATIONALE</b> 104 avenue du Président Kennedy 75016 Paris, France
Développeur	<b>IMPRIMERIE NATIONALE</b> 104 avenue du Président Kennedy 75016 Paris, France
Centre d'évaluation	<b>AMOSSYS</b> 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées	<b>Gestion du PIN utilisateur Protection en transit des clés PACE Sécurisation des échanges avec la carte CNle Sécurisation des communications avec le serveur Vérification des certificats</b>
Fonctions de sécurité non évaluées	<b>Néant</b>
Restriction(s) d'usage	<b>Non</b>

## PREFACE

### 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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 CSPN sont disponibles sur le site Internet [www.ssi.gouv.fr](http://www.ssi.gouv.fr).

## TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit évalué.....	6
1.2.1	Catégorie du produit .....	7
1.2.2	Identification du produit .....	7
1.2.3	Fonctions de sécurité.....	7
1.2.4	Configuration évaluée .....	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation.....	8
2.2	Charge de travail prévue et durée de l'évaluation.....	8
2.3	Travaux d'évaluation .....	8
2.3.1	Installation du produit.....	8
2.3.2	Analyse de la documentation.....	8
2.3.3	Revue du code source (facultative).....	8
2.3.4	Analyse de la conformité des fonctions de sécurité .....	8
2.3.5	Analyse de la résistance des mécanismes des fonctions de sécurité .....	9
2.3.6	Analyse des vulnérabilités (conception, construction, etc.) .....	9
2.3.7	Analyse de la facilité d'emploi .....	9
2.4	Analyse de la résistance des mécanismes cryptographiques .....	9
2.5	Analyse du générateur d'aléas.....	9
3	La certification .....	10
3.1	Conclusion.....	10
3.2	Recommandations et restrictions d'usage.....	10
ANNEXE A.	Références documentaires du produit évalué .....	11
ANNEXE B.	Références à la certification.....	12

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « INWallet Mobile Middleware, Version 2.1.3, pour Android » développé par IMPRIMERIE NATIONALE.

Ce produit est un *middleware* applicatif prêt à être intégré au sein d'une application mobile pour *Android*. Le *middleware* a pour unique rôle de s'interfacer avec la Carte Nationale d'Identité électronique (CNle) et les serveurs de vérification afin de réaliser une authentification du porteur de la carte. Pour cela, c'est le *middleware* qui va initier les sessions PACE avec la CNle et les tunnels TLS avec les serveurs d'authentification.

L'application mobile qui va utiliser le *middleware* est hors périmètre de l'évaluation.

La figure ci-dessous explicite l'architecture de la solution.

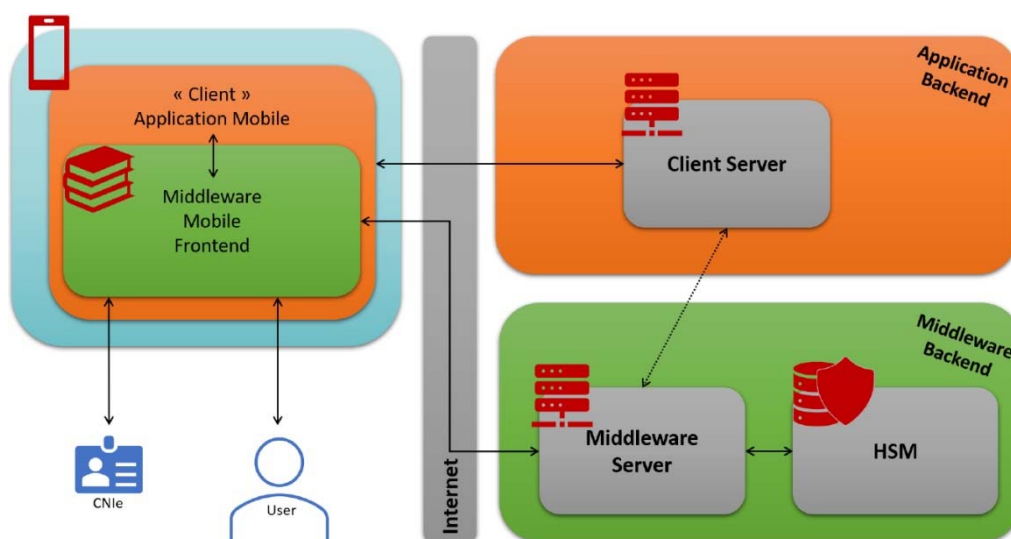


Figure 1 - Architecture Produit.

## 1.2 Description du produit évalué

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

### 1.2.1 Catégorie du produit

<input type="checkbox"/>	1	détection d'intrusions
<input type="checkbox"/>	2	anti-virus, protection contre les codes malicieux
<input type="checkbox"/>	3	pare-feu
<input type="checkbox"/>	4	effacement de données
<input type="checkbox"/>	5	administration et supervision de la sécurité
<input checked="" type="checkbox"/>	6	<b>identification, authentification et contrôle d'accès</b>
<input type="checkbox"/>	7	communication sécurisée
<input type="checkbox"/>	8	messaging sécurisée
<input type="checkbox"/>	9	stockage sécurisé
<input type="checkbox"/>	10	environnement d'exécution sécurisé
<input type="checkbox"/>	11	terminal de réception numérique ( <i>Set top box</i> , STB)
<input type="checkbox"/>	12	matériel et logiciel embarqué
<input type="checkbox"/>	13	automate programmable industriel
<input type="checkbox"/>	99	autre

### 1.2.2 Identification du produit

Produit	
Nom du produit	INWallet Mobile Middleware
Numéro de la version évaluée	Version 2.1.3, pour Android

La version certifiée du produit peut être identifiée dans le *Manifest* du SDK dans le champ *android:versionName*.

### 1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la gestion du PIN utilisateur ;
- la protection en transit des clés PACE ;
- la sécurisation des échanges avec la carte CNle ;
- la sécurisation des communications avec le serveur ;
- la vérification des certificats.

### 1.2.4 Configuration évaluée

La configuration évaluée correspond à la TOE en version 2.1.3 intégrée à l'application mobile de test Mesange.

La plateforme de test est constituée des éléments suivants :

- un *Pixel5* sous Android 11 ;
- deux serveurs distants :
  - o le serveur *Backend* du *Middleware* qui communique directement avec la TOE ;
  - o le serveur applicatif distant qui communique avec l'application mobile.
- de plusieurs CNle.

## 2 L'évaluation

### 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en ANNEXE B.

### 2.2 Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

### 2.3 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

#### 2.3.1 Installation du produit

##### 2.3.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

##### 2.3.1.2 Description de l'installation et des non-conformités éventuelles

Sans objet.

##### 2.3.1.3 Durée de l'installation

Sans objet

##### 2.3.1.4 Notes et remarques diverses

Néant.

#### 2.3.2 Analyse de la documentation

Les guides du produit permettent d'intégrer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

#### 2.3.3 Revue du code source (facultative)

L'évaluateur a revu le code source de l'intégralité du produit. Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

#### 2.3.4 Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].



### 2.3.5 Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

### 2.3.6 Analyse des vulnérabilités (conception, construction, etc.)

#### 2.3.6.1 Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

#### 2.3.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

### 2.3.7 Analyse de la facilité d'emploi

#### 2.3.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

#### 2.3.7.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté.

#### 2.3.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

## 2.4 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

## 2.5 Analyse du générateur d'aléa

Les générateurs d'aléa mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

### **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.

Ce certificat atteste que le produit « INWallet Mobile Middleware, Version 2.1.3, pour Android » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

#### **3.2 Recommandations et restrictions d'usage**

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

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

## ANNEXE A. Références documentaires du produit évalué

[CDS]	<i>CSPN Security Target INWallet Mobile Middleware</i> Référence : TOE-INWMDW ; Version : 1.6 ; Date : 23 septembre 2021.
[RTE]	Rapport Technique d'Évaluation CSPN Produit INWallet Mobile Middleware Référence : CSPN-RTE-MESANGE-1.01 ; Version : 1.01 ; Date : 20 septembre 2021.  Expertise des mécanismes cryptographiques Produit INWallet Mobile Middleware Référence : CSPN-CRY-INWallet Mobile Middleware-1.01 ; Version : 1.01 ; Date : 14 septembre 2021.
[GUIDES]	Manuel d'intégration Référence : MDW-MAN-01-INWallet Mobile Middleware SDK ; Version : 0.15 .

## ANNEXE B. Références 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.	
[CSPN]	<p>Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020.</p> <p>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019.</p> <p>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018.</p> <p>Documents disponibles sur <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p>
[RGS]	<p>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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p>