



**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-2020/40

Fonctions de vérification du SDK Photometrix Photometrix Verifier Core v1.2.3

Paris le 9 décembre 2020

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

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

Référence du rapport de certification	ANSSI-CSPN-2020/40
Nom du produit	Fonctions de vérification du SDK Photometrix
Référence/version du produit	Photometrix Verifier Core v1.2.3
Catégorie de produit	Identification, authentification et contrôle d'accès
Critère d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire	SURYS Parc d'activité Gustave Eiffel 22 avenue de l'Europe, Bussy-St-Georges 77607 Marne-La-Vallée Cedex 3
Développeur	SURYS Parc d'activité Gustave Eiffel 22 avenue de l'Europe, Bussy-St-Georges 77607 Marne-La-Vallée Cedex 3
Centre d'évaluation	OPPIDA 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées	Vérification d'intégrité de la clé publique Photometrix Vérification de la signature des fichiers Photometrix
Fonctions de sécurité non évaluées	Sans objet
Restriction(s) d'usage	Non

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.

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	6
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	Accès aux développeurs.....	9
2.3.8	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 présent certificat porte sur les « Fonctions de vérification du SDK Photometrix, Photometrix Verifier Core v1.2.3 » développé par SURYS.

Photometrix est un SDK permettant la construction d'applications mobiles d'authentification décentralisée de photographie. Cette méthode d'authentification repose sur la présentation simultanée de la photographie et de sa signature numérique, présentée sous forme d'un code-barre 2D.

Afin de permettre cette authentification, le SDK Photometrix fournit à l'application utilisateur la fonction de vérification d'une clé publique SURYS. Cette clé permet ensuite d'utiliser une seconde fonction : la vérification de la signature du fichier image. Seules ces deux fonctions sont évaluées dans le cadre du présent certificat, qui ne se prononce pas sur l'ensemble du mécanisme d'authentification de la solution Photometrix.

La figure ci-dessous explicite le périmètre de l'évaluation.

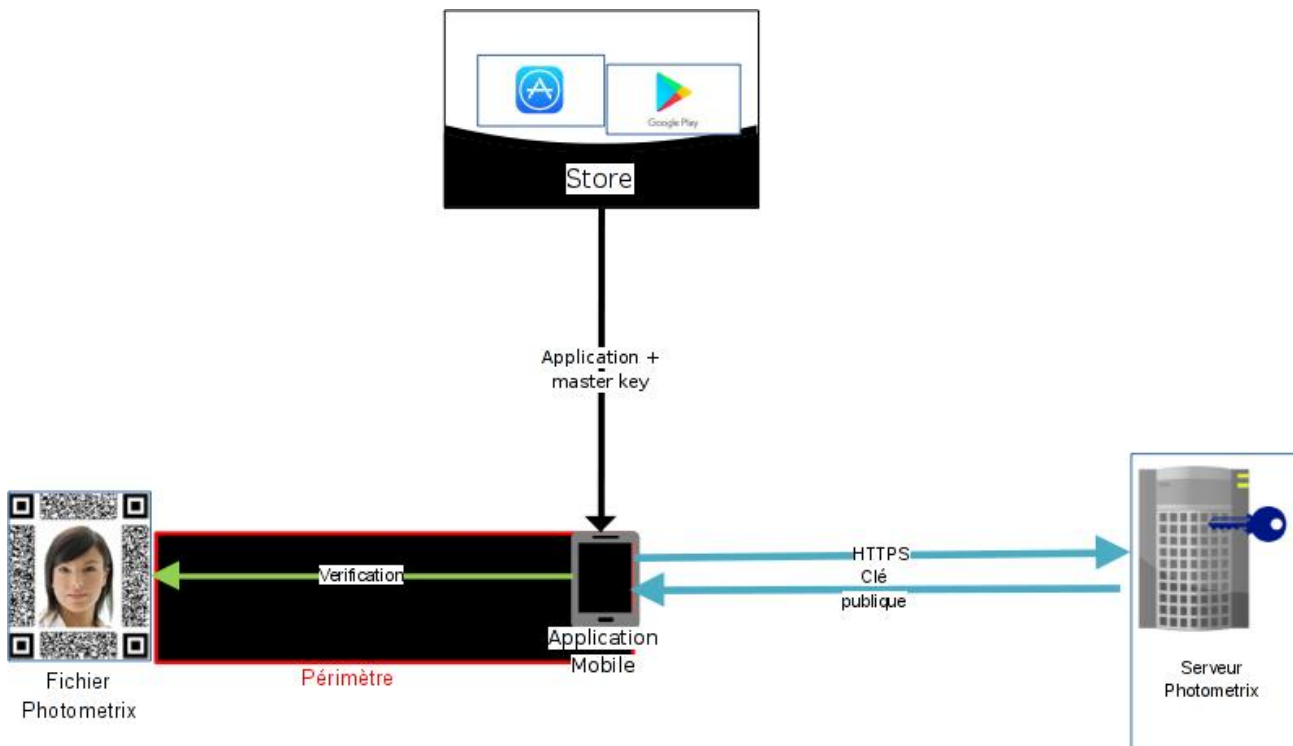


Figure 1 – Périmètre de l'évaluation.

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	identification, authentification et contrôle d'accès
<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	Fonctions de vérification du SDK Photometrix
Numéro de la version évaluée	Photometrix Verifier Core v1.2.3

La version certifiée du produit peut être identifiée dans le code source, au niveau de la fonction `Java_com_surys_photometrixchecker_PhotometrixCheckerAPI_getSdkVersionNumberNative` :

```
JNIEXPORT jstring JNICALL Java_com_surys_photometrixchecker_PhotometrixCheckerAPI_getSdkVersionNumberNative(JNIEnv* env_, jobject this_)  
{  
    std::string sdk_version = PhotometrixBridge::Instance()->_sdkVersion;  
    return env->NewStringUTF(sdk_version.c_str());  
}
```

Cette version pointe vers l'attribut `_sdkVersion` de la classe `PhotometrixBridge`, qui contient bien le numéro de version, comme indiqué ci-dessous :

```
std::string _sdkVersion = "1.2.3";
```

Figure 2 : affichage de la version du produit

1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la fonction de vérification de la clé publique SURYS, récupérée depuis le serveur Photometrix ;
- la fonction de vérification des fichiers Photometrix, à l'aide de cette clé publique.

1.2.4 Configuration évaluée

La configuration évaluée correspond à l'utilisation du SDK Photometrix à travers une application mobile générique fournie par SURYS, déployée sur un Samsung Galaxy S7 possédant Android 9.

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 2.

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: l'application générique s'installe comme n'importe quelle application Android. Le produit soumis à évaluation est un SDK, c'est-à-dire du code source, qui ne requiert pas particulièrement d'installation.

2.3.1.3 Durée de l'installation

Sans objet.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 Analyse de la documentation

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer 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. L'analyse a été effectuée à l'aide de l'outil CppCheck.

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

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitable dans le contexte défini par la cible de sécurité [CDS].

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 Accès aux développeurs

Sans objet.

2.3.8 Analyse de la facilité d'emploi

2.3.8.1 Cas où la sécurité est remise en cause

Sans objet.

2.3.8.2 Avis d'expert sur la facilité d'emploi

Afin de simplifier l'utilisation du SDK, SURYS fournit un guide et une application générique à l'attention des développeurs.

2.3.8.3 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 vulnérabilité exploitable.

2.5 Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléas.

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 « Fonctions de vérification du SDK Photometrix, version Photometrix Verifier Core v1.2.3 » 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.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations et restrictions suivantes.

Aucune recommandation particulière n'est formulée par l'évaluateur.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent impérativement se conformer aux recommandation du document [GUIDE].

ANNEXE A. Références documentaires du produit évalué

[CDS]	<i>File verification functions of Photometrix SDK version 1.2.3 – CSPN Security Target</i> Référence : sans ; Version : 1.7 ; Date : 10 novembre 2020.
[RTE]	<i>Rapport Technique d'Évaluation CSPN Photometrix</i> Référence : OPPIDA/CESTI/FAZER/RTE ; Version : 2.0 ; Date : 14 octobre 2020.
[GUIDE]	<i>Photometrix Server documentation</i> Référence : sans ; Version : 2.02 ; Date : 12 mars 2018 ; <i>Photometrix SDK Android</i> Référence : sans ; Version : 1.1 ; Date : 25 mai 2020.

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]

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 ;

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 ;

Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018.

Documents disponibles sur www.ssi.gouv.fr.