PREMIÈRE
MINISTRE
*Liberté*
*Égalité*
*Fraternité*

Agence nationale de la sécurité
des systèmes d'information

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

# Rapport de certification
# ANSSI-CC-PP-2023/02

## ETSI TS 103 732-1 Consumer Mobile Device ; part 1 : Base Protection Profile (version 2.1.2)

Paris, le 28 Décembre 2023

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

Vincent STRUBEL

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

# AVERTISSEMENT

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.

Un profil de protection est un document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

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<br>**ANSSI-CC-PP-2023/02** |
| Nom du profil de protection<br>**ETSI TS 103 732-1 Consumer Mobile Device ; part 1 : Base Protection Profile** |
| Référence/version du profil de protection<br>**version 2.1.2** |
| Conformité à un profil de protection<br>Néant |
| PP-Base certifiée<br>***ETSI TS 103 732-1 Consumer Mobile Device ; part 1 : Base Protection Profile*, v2.1.2, 16 novembre 2023** |
| PP-Modules associés aux PP-Configurations certifiées<br>***ETSI TS 103 732-2 Consumer Mobile Device ; part 2 : Biometric Authentication Protection Profile Module*, v1.1.2, 16 novembre 2023** |
| Critère d'évaluation et version<br>**Critères Communs version 3.1 révision 5** |
| Niveau d'évaluation imposé par le PP<br>**EAL2 augmenté**<br>ALC_DVS_EXT.1, ALC_FLR.3 |
| Rédacteur<br>**ETSI Technical Committee Cyber Security (TC CYBER)**<br>650 route des Lucioles<br>F-06921 Sophia Antipolis Cedex, France |
| Commanditaire<br>**ETSI Technical Committee Cyber Security (TC CYBER)**<br>650 route des Lucioles<br>F-06921 Sophia Antipolis Cedex, France |
| Centre d'évaluation<br>**THALES / CNES**<br>290 allée du Lac,<br>31670 Labège, France |
| Accords de reconnaissance applicables<br>**CCRA** **SOG-IS** |

# PREFACE

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 sont disponibles sur le site Internet www.cyber.gouv.fr.

# TABLE DES MATIERES

1 Le profil de protection ..... 6
1.1 Identification du profil de protection ..... 6
1.2 Rédacteur ..... 6
1.3 Description du profil de protection ..... 6
1.4 Exigences fonctionnelles ..... 7
1.5 Exigences d'assurance ..... 7
1.6 Configurations évaluées ..... 7
2 L'évaluation ..... 8
2.1 Référentiels d'évaluation ..... 8
2.2 Travaux d'évaluation ..... 8
3 La certification ..... 9
3.1 Conclusion ..... 9
3.2 Reconnaissance du certificat ..... 9
3.2.1 Reconnaissance européenne (SOG-IS) ..... 9
3.2.2 Reconnaissance internationale critères communs (CCRA) ..... 9
ANNEXE A. Références ..... 10
ANNEXE B. Références liées à la certification ..... 11

# 1 Le profil de protection

## 1.1 Identification du profil de protection

Titre : « *Consumer Mobile Device ; part 1 : Base Protection Profile* »

Référence, version : TS 103 732-1, 2.1.2

Date : 16 novembre 2023

## 1.2 Rédacteur

Ce profil de protection a été rédigé par :

**ETSI Technical Committee Cyber Security (TC CYBER)**
650 route des Lucioles, 06921 Sophia Antipolis Cedex, France

## 1.3 Description du profil de protection

Le profil de protection « *Consumer Mobile Device Protection Profile* » [PP] décrit un smartphone, une tablette ou un autre matériel qui a les mêmes fonctionnalités, qui offre aux utilisateurs la possibilité d'effectuer différents types d'actions : appels téléphoniques, appels vidéo, jeux, écoute de musique, accès internet, etc.

Ce profil de protection autorise plusieurs configurations. En effet, il contient une partie « de base » qui consiste à définir des exigences de sécurités minimales, puis un PP-module optionnel. Les configurations évaluées sont définies dans le chapitre 1.6.

Ce PP correspond ainsi à :

- un profil de protection de base [PP_Base] qui inclut un *hardware*, un *operating system*, et des applications ;
- un PP-module optionnel [PP_mod] qui correspond aux mécanismes biométriques pour s'authentifier et la vérification biométrique permettant à l'utilisateur de gérer ses modèles d'enrôlement.

## 1.4 Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies par le profil de protection[1] , au chapitre 7 du [PP], sont les suivantes :

- FCS_RNG_EXT.1 *Random numbers generation*
- FCS_CKH_EXT.1 *Cryptographic Key Hierarchy*
- FCS_UPF_EXT.1 *Update Check Frequency*
- FPT_ITC_EXT *Inter-TSF Trusted Channel*

De plus, le profil de protection reprend les exigences fonctionnelles de sécurité suivantes définies dans la partie 2 des Critères Communs [CC] :

- *Cryptographic key generation* (FCS_CKM.1) ;
- *Cryptographic key destruction* (FCS_CKM.4) ;
- *Cryptographic operation* (FCS_COP.1) ;
- *Subset access control* (FDP_ACC.1) ;
- *Complete access control* (FDP_ACC.2) ;
- *Security attribute based access control* (FDP_ACF.1) ;
- *Timing of authentication* (FIA_UAU.1) ;
- *Timing of identification* (FIA_UID.1) ;
- *Multiple authentication mechanisms* (FIA_UAU.5) ;
- *Re-authenticating* (FIA_UAU.5) ;
- *Protected authentication feedback* (FIA_UAU.7) ;
- *Verification of secrets* (FIA_SOS.1) ;
- *Authentication failure handling (*FIA_AFL.1) ;
- *Management of security attributes* (FMT_MSA.1) ;
- *Static attribute initialisation* (FMT_MSA.3) ;
- *Specification of Management Function* (FMT_SMF.1) ;
- *Pseudonymity* (FPR_PSE.1) ;
- Inter-TSF trusted channel (FTP_ITC.1) ;
- *Failure with preservation of secure state* (FPT_FLS.1) ;
  *TSF testing* (FPT_TST.1) ;
- *Automated recovery* (FPT_RCV.2) ;

## 1.5 Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL2 augmenté des composants d'assurance suivants ALC_DVS_EXT.1, ALC_FLR.3**.

En dehors du composant d'assurance étendu ALC_DVS_EXT.1, toutes les exigences d'assurance imposées par le profil de protection sont extraites de la partie 3 des Critères Communs [CC].

Les reconnaissances SOG-IS et CCRA des produits évalués selon ce profil de protection seront limitées à EAL2 augmenté du composant ALC_FLR.3.

## 1.6 Configurations évaluées

Deux PP-configurations ont été évaluées et sont certifiées :

1. [PP_Base] Profil de protection de base ;
2. [PP_Base+mod] Profil de protection de base [PP_Base] avec le PP-module [PP_mod], telle que définie dans PP-Configuration.

[1] Exigences fonctionnelles étendues non issues de la partie 2 des [CC].

# 2 L'évaluation

## 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 5** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

## 2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives aux composants d'assurance ci-dessous sont à « **réussite** ».

Pour la configuration 1 [PP_Base], les composants évalués (définis dans [CC]) sont les suivants :

| Composants | Descriptions |
|---|---|
| APE_CCL.1 | *Conformance claims* |
| APE_ECD.1 | *Extended components definition* |
| APE_INT.1 | *Protection profile introduction* |
| APE_OBJ.2 | *Security objectives* |
| APE_REQ.2 | *Derived security requirements* |
| APE_SPD.1 | *Security problem definition* |

**Tableau 1 - Evaluation du PP pour la configuration 1**

Pour la configuration 2 [PP_Base+mod], les composants évalués sont les suivants :

| Composants | Descriptions |
|---|---|
| ACE_CCL.1 | *PP-module conformance claims* |
| ACE_ECD.1 | *PP-module Extended components definition* |
| ACE_INT.1 | *PP-module introduction* |
| ACE_OBJ.1 | *PP-module objectives* |
| ACE_REQ.1 | *PP-module security functional requirements* |
| ACE_SPD.1 | *PP-module Security problem definition* |
| ACE_MCO.1 | *PP-module consistency* |
| ACE_CCO.1 | *PP-module configuration consistency* |

**Tableau 2 - Evaluation du PP pour la configuration 2**

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

# 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.

## 3.2 Reconnaissance du certificat

### 3.2.1 *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[2], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour classes d'assurance APE et ACE. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

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

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[3], des certificats Critères Communs. La reconnaissance s'applique pour les classes d'assurance APE et ACE. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

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

[3] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

# ANNEXE A. Références

| | |
|---|---|
| [PP] | - [PP_Base] *Consumer Mobile Device ; part 1 : Base Protection Profile, référence ETSI TS 103 732-1, version 2.1.2, novembre 2023 ;*<br>- [PP_mod] *Consumer Mobile Device ; part 2 : Biometric Authentication Protection Profile Module*, référence ETSI TS 103 732-2, version 1.1.2, 16 novembre 2023 ;<br>- [PP_Base+mod] *Consumer Mobile Device Base PP-Configuration ; part 1 : CMD and Biometric Verification*, référence ETSI TS 103 932-1, version 1.1.2, 16 novembre 2023. |
| [RTE] | Rapport technique d'évaluation :<br>- *Protection Profile Evaluation Technical Report CFG_CMD_BIO, référence CFG_CMD_BIO_APE*, version 1.1, 9 août 2023. |

# ANNEXE B. 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] | Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0. |
| [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. |
| [CCRA] | *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. |