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-CSPN-2023/21

Application France Identité iOS

Version 1.2.3

Paris, le 17 Novembre 2023

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

Emmanuel NAEGELEN

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-CSPN-2023/21**
Nom du produit **Application France Identité iOS**
Référence/version du produit **Version 1.2.3**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Ministère de l'Intérieur** Tour Olympie, 101 rue de Tolbiac 75013 Paris, France
Développeur **Atos France** 80, quai Voltaire 95870 Bezons, France
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées Gestion sécurisée du code PIN Communication sécurisée avec le *Backend* Communication sécurisée avec le titre Génération de la preuve de légitimité de l'application Protection des données d'identité de l'usager Autorisation de l'application mobile par le *Backend*
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 7
1.2.1 Catégorie du produit 7
1.2.2 Identification du produit 7
1.2.3 Fonctions de sécurité 8
1.2.4 Configuration évaluée 9
2 L'évaluation 10
2.1 Référentiels d'évaluation 10
2.2 Travaux d'évaluation 10
2.2.1 Installation du produit 10
2.2.2 Analyse de la documentation 10
2.2.3 Revue du code source (facultative) 10
2.2.4 Analyse de la conformité des fonctions de sécurité 10
2.2.5 Analyse de la résistance des mécanismes des fonctions de sécurité 10
2.2.6 Analyse des vulnérabilités (conception, construction, etc.) 11
2.2.7 Analyse de la facilité d'emploi 11
2.3 Analyse de la résistance des mécanismes cryptographiques 11
2.4 Analyse du générateur d'aléa 11
3 La certification 12
3.1 Conclusion 12
3.2 Recommandations et restrictions d'usage 12
ANNEXE A. Références documentaires du produit évalué 13
ANNEXE B. Références liées à la certification 14

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Application France Identité iOS, Version 1.2.3 » développé par Atos France.

La Carte Nationale d'Identité Électronique (CNIe) permet la mise en place d'une solution d'identité numérique dans laquelle l'identité régalienne de l'usager est prouvée à des services distants de manière sécurisée, à l'aide de son smartphone et de son titre d'identité.

Dans ce contexte, le Service de Garantie de l'Identité Numérique (SGIN) se compose d'une application centrale regroupant des composants réseaux et des micro-services applicatifs, désignée par le terme « Backend » ainsi que de d'une application mobile, désignée par le terme « France Identité » installée sur le terminal mobile de l'usager et objet du présent certificat.

Le présent certificat porte sur les composants de cette application mobile « France Identité » impliqués dans les processus relatifs à son utilisation comme élément d'un Moyen d'Identité Électronique (MIE) de niveau élevé au sens du règlement eIDAS.

La figure ci-dessous explicite l'architecture globale du produit.

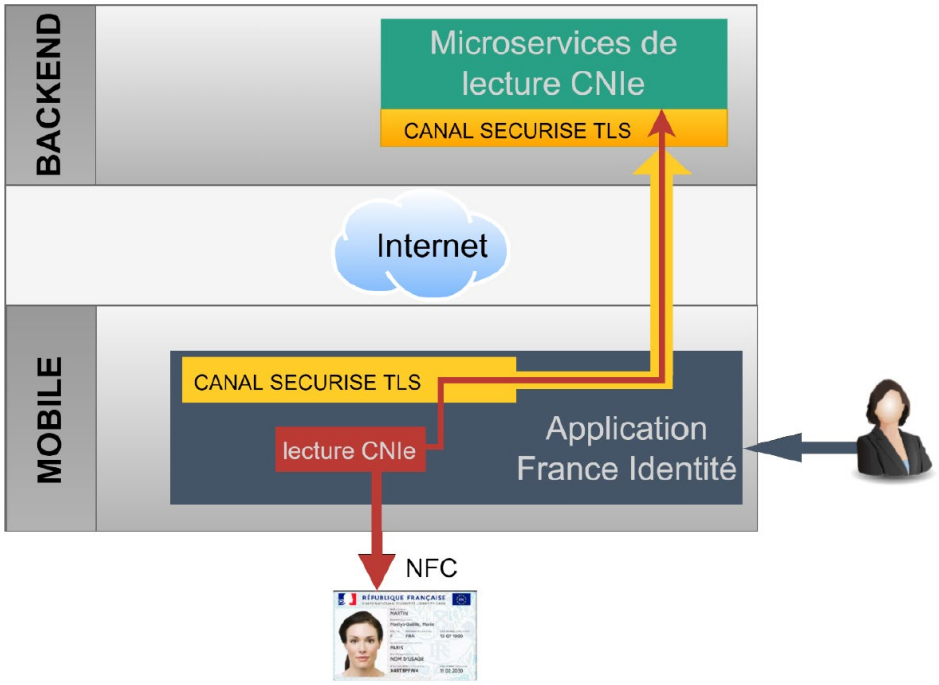


Figure 1 - Architecture globale du produit.

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*

☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☒	**6**	**identification, authentification et contrôle d'accès**
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

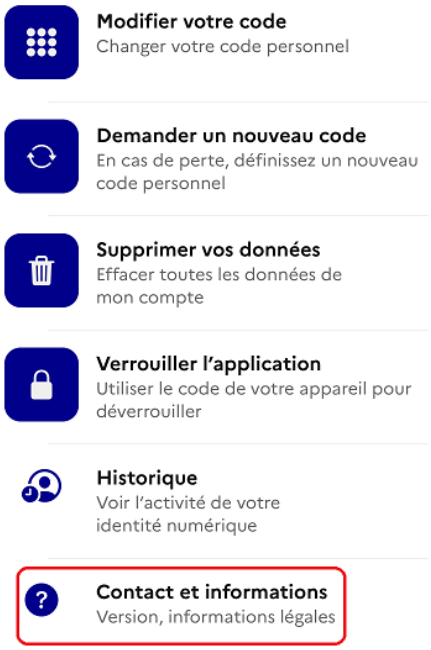
1.2.2 *Identification du produit*

Produit	
Nom du produit	Application France Identité iOS
Numéro de la version évaluée	Version 1.2.3

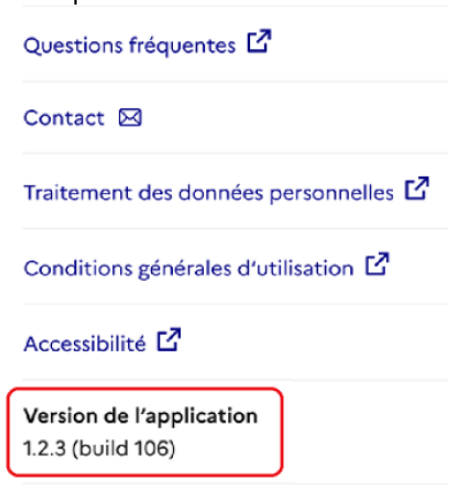
La version certifiée du produit peut être identifiée de la manière suivante (après avoir enregistré au préalable une carte d'identité) ;

- dans le menu principal affichant la carte d'identité, cliquer sur le logo en haut à droite :

- puis cliquer sur « Contact et informations » :



- puis lire le numéro de version du produit affiché :



1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la gestion sécurisée du code PIN ;
- la communication sécurisée avec le *Backend* ;
- la communication sécurisée avec le titre ;
- la génération de la preuve de légitimité de l'application ;
- la protection des données d'identité de l'usager ;
- l'autorisation de l'application mobile par le *Backend*.

1.2.4 *Configuration évaluée*

La configuration évaluée est décrite dans la cible de sécurité [CDS].

La plateforme d'évaluation est présentée sur la figure ci-dessous.

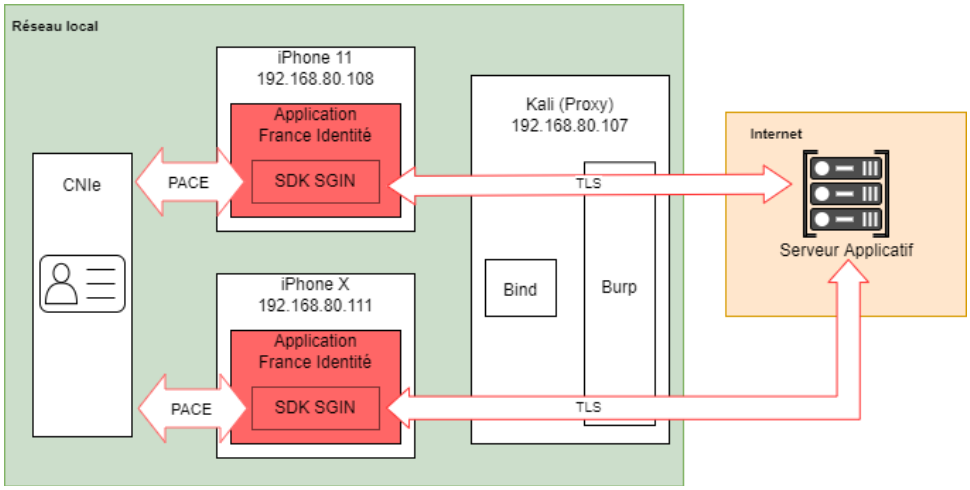


Figure 2 – Plateforme d'évaluation.

Cette plateforme est constituée des éléments suivants :

- une carte nationale d'identité électronique (CNIe) ;
- deux terminaux mobiles client iOS :
  - un iPhone 11 sous iOS 16 ;
  - un iPhone X « jailbreaké » sous iOS 16.
- une machine Kali Linux, servant de proxy, incluant :
  - un serveur DNS Bind ;
  - le logiciel Burp agissant en tant que proxy transparent.
- le Backend distant France Identité.

L'application est installée sur les deux téléphones, dont l'iPhone X dit « jailbreaké » qui permet d'analyser en détail le fonctionnement et l'impact de l'application sur le téléphone. Pour celui-ci, le développeur a fourni une version *France Identité-1.2.3-NOPIN* de l'application.

L'application intègre le SDK SGIN, composé de deux SDK (ascp & idmobile) développés spécifiquement pour l'application.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-08].

2.2 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].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

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

2.2.1.2 Description de l'installation et des non-conformités éventuelles

Après mise en place de l'environnement d'évaluation, l'installation de l'application France Identité iOS consiste à utiliser le lien d'invitation *Firebase* reçu par email (en échange des UDID des iPhones sur lesquels l'application doit être installée) pour télécharger l'IPA de l'application, puis à l'installer en cliquant sur l'IPA.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *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.

2.2.3 *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.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

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

2.2.5 *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.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

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

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 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.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

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

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant 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.

Ce certificat atteste que le produit « Application France Identité iOS, Version 1.2.3 » 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 suivre les recommandations se trouvant dans les guides fournis [GUIDES].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Application « France Identité » iOS – Cible de sécurité, version 2.14, 5 juin 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Application « France Identité » iOS, version 2.14I, 7 novembre 2023.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN - Application mobile France Identité sur iOS – version 1.2.3, référence CSPN-RTE-QUETZAL-1.02, version 1.02, 9 octobre 2023.
[ANA_CRY]	Rapport d'expertise cryptographique : - Expertise des mécanismes cryptographiques - Application mobile France Identité sur iOS – version 1.2.3, référence CSPN-CRY-QUETZAL-1.01, version 1.01, 27 septembre 2023.
[GUIDES]	Guides du produit : - *Electronic National Identity Card technical specifications* , version A032, 13 novembre 2020 ; - Application « France identité » - Gestion du cycle de vie du MIE, version 1.0, 16 mai 2023 ; - Application « France identité » - Gestion sécurisée du code PIN, version 1.2, 11 mai 2023 ; - Application « France identité » - Interactions avec *FranceConnect*, version 1.0, 16 mai 2023 ; - Application « France identité » - Politique de signature et de publication, version 1.0, 16 mai 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.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 4.0, 3 mars 2022. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[NOTE-08]	Note d'application - Méthodologie pour l'évaluation d'applications mobiles, référence ANSSI-CSPN-NOTE-08, version 1.0, 23 juillet 2021.