MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

France Identité Numérique

France Identité

Application « France identité » iOS

Cible de sécurité

Version 2.14l

Historique des modifications

Version	Date	Modifications apportées
0.1	29/06/2021	Création du document.
0.2	30/06/2022	Relecture finale.
1.0	30/06/2022	Proposition de version finale à FIN.
1.1	16/09/2022	Prise en compte des remarques ANSSI et FIN
1.2	19/09/2022	Uniformisation du document selon le modèle FIN, mises à jour avec prise en compte des commentaires de l'ANSSI, revue globale et validation du document par MI/FIN/RSSI
1.3	24/10/2022	Ajout des données d'identité aux biens sensibles
1.4	28/10/2022	Ajout d'une menace sur les données utilisateur Correction du schéma sur l'authentification du Titre Suppression d'une référence non utilisée Ajout de l'aléa dans les biens sensibles
1.5	31/10/2022	Validation du document par le MI/FIN/RSSI
1.6	07/11/2022	Modification du nom du bien sensible B-ALEA_STOCKE Modification de l'hypothèse de délivrance du code de réinitialisation (OTP) du code PIN Ajout de la menace sur l'utilisation d'une application non légitime Ajout de la FS4 sur le contrôle de la légitimité de l'application
1.7	09/11/2022	Prise en compte des commentaires de l'ANSSI : - Modification de la cinématique de réinitialisation du code PIN et suppression de l'OTP ; - Intégration de la DeviceCheck dans le schéma du périmètre ; Retrait de la menace relative à l'usurpation de
1.8	18/11/2022	Prise en compte des remarques de l'ANSSI : - Reset PIN - QRCode
2.8	18/11/2022	Homogénéisation des numéros de version avec la cible Android
2.10	03/01/2023	- Ajout de la menace M3 et de la FS6 correspondante - Reformulation de la FS1
2.11	06/01/2023	- Complément sur FS1 - Reformulation des remarques sur les hypothèses
2.12	16/05/2023	Mise à jour suite aux prétests
2.13	01/06/2023	Mise à jour de la version de l'application mobile qui corrige des anomalies fonctionnelles 1.2.2 vers 1.2.3
2.14	05/06/2023	Mise à jour des dépendances
2.14l	07/11/2023	Mise à jour du document pour publication sur le site de l'ANSSI.

Table des matières

1 INTRODUCTION

1.1 OBJET DU DOCUMENT

Ce document décrit la cible de sécurité pour la certification de sécurité de premier niveau (CSPN) de l'application mobile France Identité sur iOS, restreinte aux fonctionnalités s'exécutant sur le terminal mobile de l'usager, par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

1.2 TERMINOLOGIE, DEFINITIONS, ACRONYMES ET ABREVIATIONS

Acronyme	Description
ANSSI	Agence nationale de sécurité des systèmes d'information
APDU	Application Protocol Data Unit
API	Application Programming Interface
CAN	Card Access Number
CNIe	Carte Nationale d'Identité électronique
COTS	Commercial of the shelf
DVK	Dynamic Virtual Keyboard (Clavier Virtuel Dynamique)
eIDAS	Electronic Identification Authentication and trust Services
eID	electronic Identity
FI	Fournisseur d'Identité
FS	Fournisseurs de Service
HSM	Hardware Security Module
ICAO	International Civil Aviation Organization
IHM	Interface Homme-Machine
MRZ	Machine-Readable Zone
NFC	Near Field Communication
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PUK	PIN Unlock Key
SDK	Software Development Kit
SGIN	Service de Garantie de l'Identité Numérique
SM	Secure Messaging
TLS	Transport Layer Security

1.3 REFERENCES

Réf.	Document
1	Machine Readable Travel Documents – doc 9303, ICAO (8th edition 2021)
2	Puce CNIe – Electronic National Identity Card Technical Specifications, v A032 – ANTS (2020)
3	The Transport Layer Security (TLS) Protocol, version 1.3, RFC 8446,
4	*DCAppAttestService, Apple Developer documentation* https://developer.apple.com/documentation/devicecheck/dcappattestservice
5	Recommandations de sécurité relatives à TLS – version 1.2 – ANSSI 2022 https://www.ssi.gouv.fr/uploads/2020/03/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf
6	Gestion sécurisée du code PIN FIN_INT_SGIN_DOC_Explications_Gestion_sécurisee_du_code_PIN_v1.2
7	Association d'une application mobile à un site web https://developer.apple.com/documentation/xcode/allowing-apps-and-websites-to-link-to-your-content?language=objc
8	OWASP Mobile Application Security Verification Standard (MASVS) • https://owasp.org/www-project-mobile-app-security/

2 IDENTIFICATION DU PRODUIT

Nom commercial du Produit	Application mobile ***France Identité*** sur iOS
Lien vers le Produit	https://france-identite.gouv.fr/
Éditeur	Ministère de l'intérieur
Version évaluée	1.2.3
Catégorie	Identification, Authentification et Contrôle d'accès

3 DESCRIPTION DU PRODUIT

3.1 DESCRIPTION GENERALE DU PRODUIT

La 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. Ce dernier est désigné dans la suite du document par le terme « *Titre* ».

Le Service de Garantie de l'Identité Numérique (SGIN) est réalisé dans ce contexte. Il 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. Le périmètre de cette cible de Certification de Sécurité de Premier Niveau concerne les composants de l'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.

Le terme « *Produit* » désigne uniquement **les composants de l'application *mobile « France Identité » impliqués dans les processus relatifs à son utilisation comme un élément d'un MIE*** dans la suite du document.

Le Produit offre les opérations et fonctionnalités suivantes :

- L'identification et l'authentification de l'usager auprès d'un service en ligne ;
- L'établissement d'un canal sécurisé TLS ;
- La saisie sécurisée du code PIN de la CNIe de l'usager ;
- La communication avec la CNIe de l'usager ;
- La gestion du code PIN de la CNIe de l'usager.

Un canal sécurisé TLS est établi pour l'intégralité des communications entre le Produit et le Backend. Ce canal assure une communication protégeant en authenticité, en intégrité et en confidentialité tous les messages échangés entre le Produit et le Backend.

Le Backend vérifie l'attestation d'application fournie par le Produit. La génération de l'attestation d'application est réalisée par l'OS à la demande du Produit. La demande de génération d'attestation d'application doit être conforme à la documentation de l'OS décrite dans [7] et sera aussi analysée lors de l'évaluation.

La saisie sécurisée du code PIN du Titre est réalisée sur le Produit par l'usager grâce à un clavier virtuel dynamique (DVK). Le code PIN n'est jamais transmis au Backend.

Le service de lecture et les opérations sur les Titres s'appuient sur l'application « *ICAO* » [**1**] et sur l'application « *eID* » [**2**] de la CNIe pour l'authentification du Titre, l'authentification de l'usager et la lecture des attributs d'identité. Pour réaliser ces opérations sur le Titre, le Backend établit un canal sécurisé (protocole de « *Chip Authentication* ») de bout en bout avec le Titre tel que défini dans [**1**] et [**2**]. Le Produit permet d'échanger les messages APDU avec le Titre de l'usager par NFC.

Afin d'établir le canal de communication sécurisé PACE avec l'application « *ICAO* » de la CNIe, le CAN ou la MRZ sont nécessaires (cf. [**1**]). De même, pour l'application « *eID* », le code PIN de l'usager est nécessaire (cf. [**2**]), et éventuellement le CAN s'il s'agit du dernier essai. Ces éléments sont transmis par l'usager au Produit.

Un schéma global de l'architecture du Produit est présenté dans la « Figure 1 ».

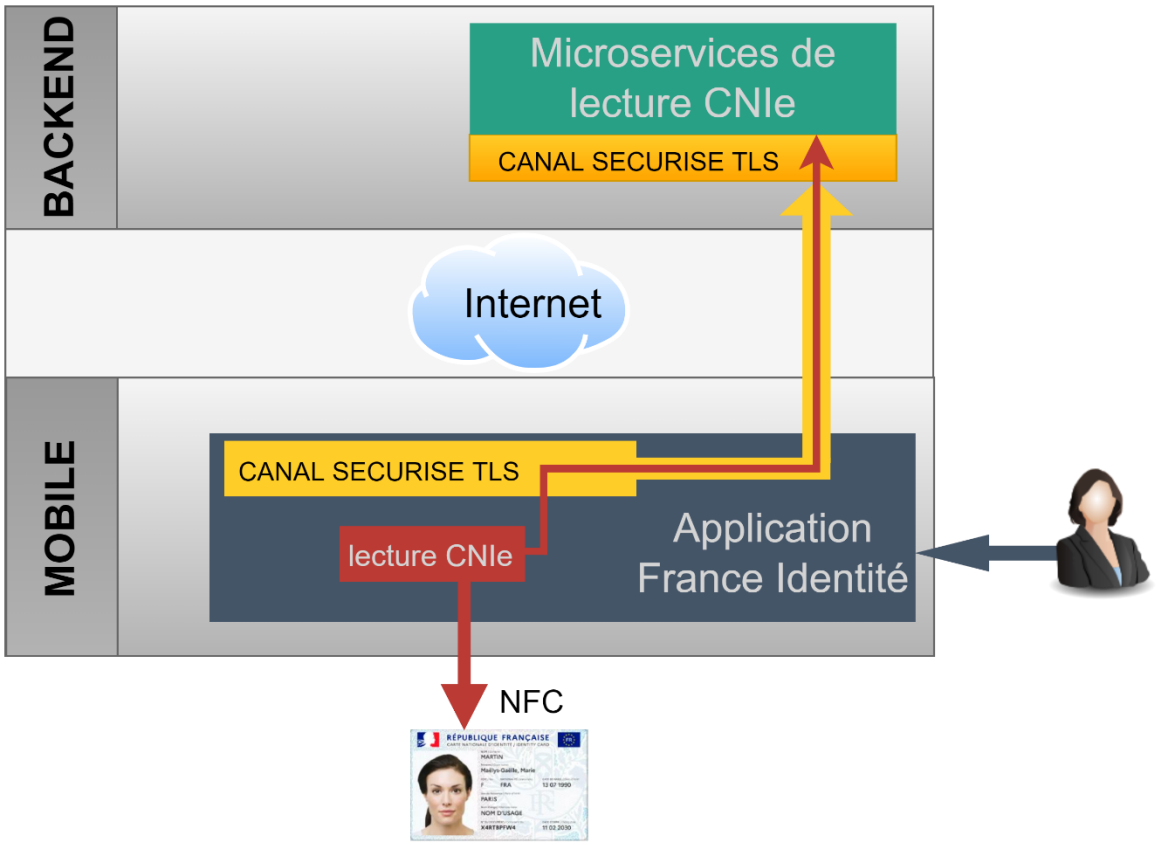

Figure 1 : Architecture globale du Produit

3.2 DESCRIPTION DE L'UTILISATION DU PRODUIT

L'objectif principal du Produit est d'être un des composants d'un moyen d'identification électronique (MIE) de niveau élevé au sens du règlement eIDAS.

Pour cela, le Produit met en œuvre :

- L'établissement d'un canal sécurisé TLS entre le Produit et le Backend ;
- Un clavier de saisie sécurisé du code PIN ;
- Un composant permettant une gestion locale du protocole PACE (établissement du canal et Secure Messaging) pour :
  - authentifier l'usager ;
  - définir un nouveau code PIN sur la CNIe ;
- La transmission des APDU entre le Backend et la CNIe lue en NFC pour :
  - authentifier le Titre ;
  - accéder aux données présentes dans les applications « ICAO » et « eID » du Titre.

Par ailleurs, le Produit dispose d'un mécanisme de protection des données de l'usager.

L'utilisation générale du Produit est décrite dans la « Figure 2 » :

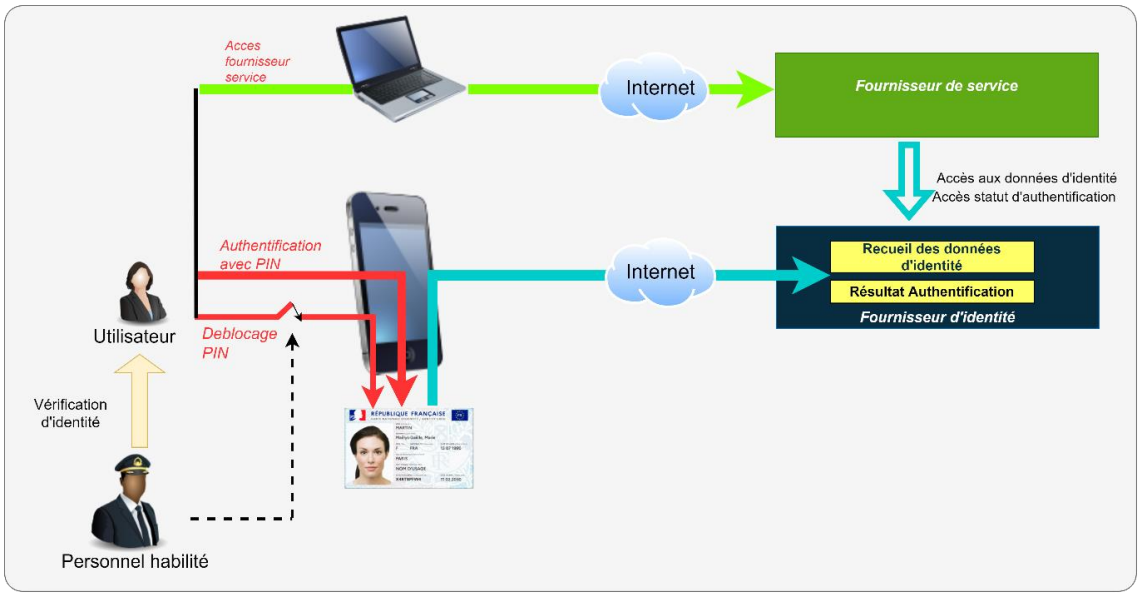

Figure 2 : cas d'usage général

Préambule :

Avant d'utiliser pour la première fois l'application « *eID* » de sa CNIe, l'usager doit la débloquer, en personnalisant un code PIN connu exclusivement de lui-même.

Mise en œuvre :

1. L'usager se connecte à un fournisseur de service. Ce dernier lui demande de s'authentifier pour recueillir ses données d'identité ;
2. L'usager, à l'aide du Produit, saisit le code PIN du Titre avant de le scanner. Si le PIN est valide, l'usager est authentifié auprès du Backend qui peut accéder aux données contenues dans le Titre présenté. En cas d'échec de lecture NFC du Titre, le code PIN est systématiquement redemandé ;
3. Le Backend vérifie l'intégrité de ces données, l'authenticité et la validité du Titre, puis transmet les données d'identité provenant du Titre au fournisseur de service.

Les schémas ci-dessous détaillent la cinématique de connexion à un fournisseur de service grâce au Produit :

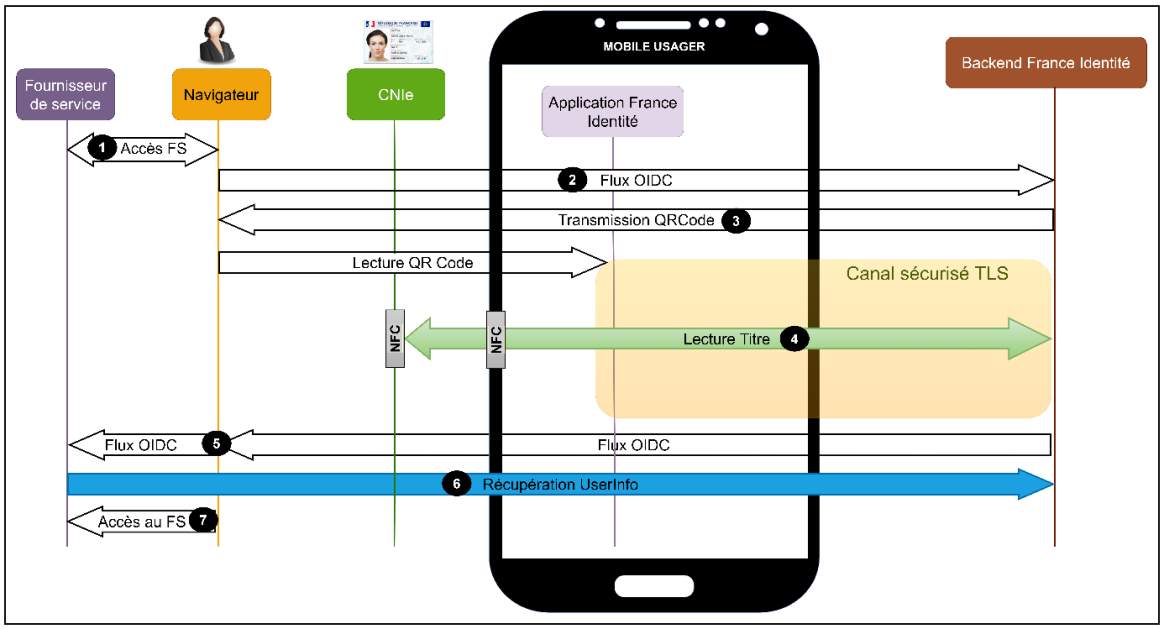

Figure 3 : connexion à un fournisseur de service avec utilisation d'un terminal externe

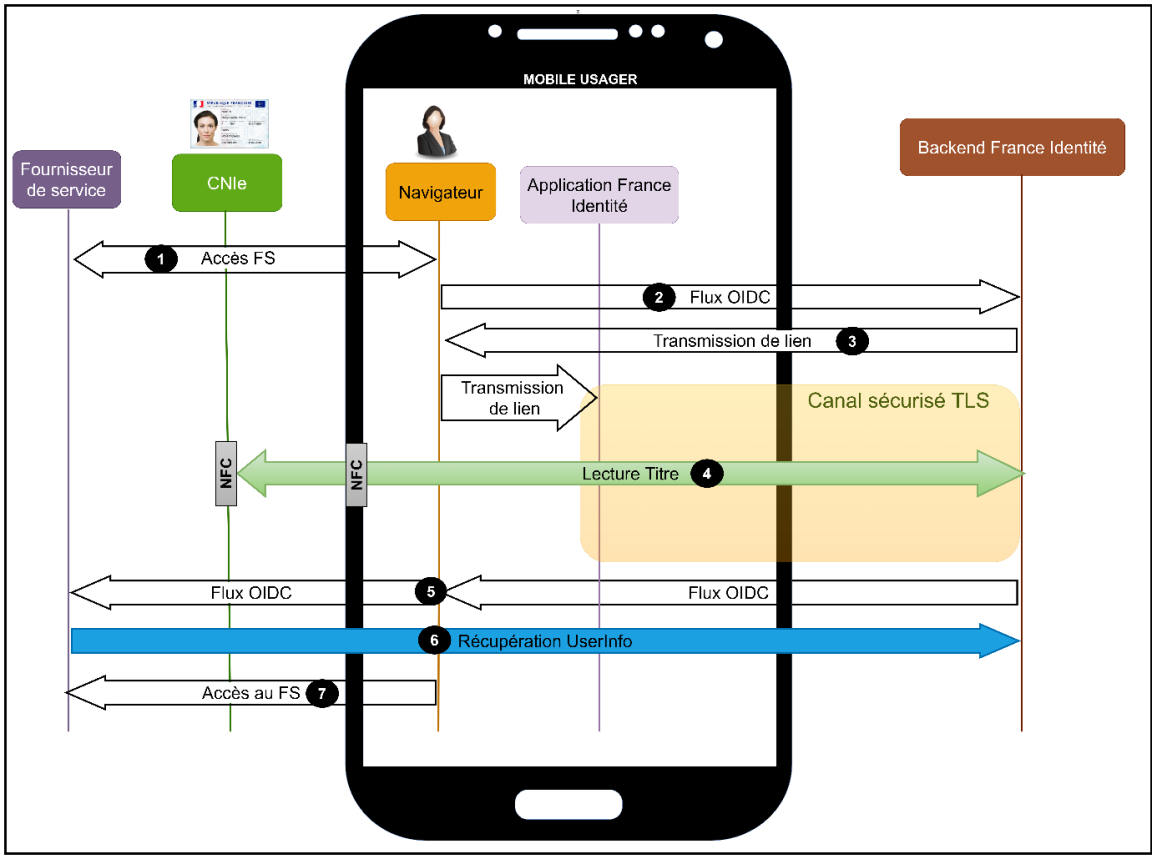

Figure 4 : connexion à un fournisseur de service sans utilisation d'un terminal externe

Les échanges entre le Backend en tant que fournisseur d'identité et le fournisseur de service, sont réalisés en utilisant le protocole OpenID Connect. Ils sont hors du périmètre de cette cible de sécurité.

Dans la cinématique de connexion, deux cas de figure sont possibles. Le premier consiste à ce que l'usager se connecte à son fournisseur de service depuis un ordinateur (mais il s'authentifie avec le Produit) tel que précisé dans la « Figure 3 » et le second consiste à ce que l'usager réalise l'ensemble des opérations depuis son terminal mobile tel que précisé dans la « Figure 4 ».

Ainsi les différentes étapes à partir du navigateur de l'usager sont les suivantes :

1. L'usager se connecte à son fournisseur de service qui le redirige vers le site de France Identité via un flux OpenID Connect pour s'authentifier ;
2. Le site de France Identité affiche auprès de l'usager un QR code ou transmet une URL ;
3. Selon le cas de figure :
   a. Premier cas, « Figure 3 », le navigateur se trouve sur un terminal externe au mobile. L'usager ouvre le Produit et scanne le QR code affiché ;
   b. Second cas, « Figure 4 », le navigateur se trouve sur le mobile de l'usager. Il est redirigé localement sur son terminal mobile vers le Produit ;
4. Le Produit présente un écran à l'usager précisant l'origine de la requête d'authentification, le niveau d'authentification souhaité et les attributs d'identité demandées ;
5. S'il y consent, le Produit déclenche une lecture du Titre de l'usager en l'authentifiant par la saisie du code PIN de sa CNIe ;
6. Le fournisseur de service récupère auprès du Backend les informations relatives à l'usager authentifié grâce à la cinématique « Authorization code flow » d'OpenID Connect;
7. Identifié et authentifié, l'usager accède au fournisseur de service.

3.2.1 Canal sécurisé TLS

Afin de protéger en authenticité, en confidentialité et en intégrité les communications entre le Produit et le Backend, un canal sécurisé TLS est monté de bout en bout entre le Produit et le Backend.

L'établissement du canal sécurisé TLS entre le Produit et le Backend permet :

- L'authentification du Backend à l'aide de son certificat électronique au format x509 ;
- L'établissement d'un canal de communications protégé en intégrité et confidentialité.

Une fois le canal sécurisé TLS établi, les données échangées sont protégées en intégrité, en confidentialité et en authenticité. Seule la version TLS 1.3 est supportée et autorisée par le Produit.

Ce canal sécurisé TLS est directement intégré et utilisé par le Produit lors des échanges sécurisés avec le Backend en charge de l'authentification du Titre, du changement et de la réinitialisation du code PIN. Pour authentifier ces services, le Produit embarque le certificat électronique du Backend permettant de s'assurer que les communications sont réellement établies avec celui-ci ; il s'agit d'un mécanisme de *« certificate pinning »*.

Comme décrit dans la RFC 8446 [3], pour la mise en œuvre du canal sécurisé TLS, le Backend choisit la *« cipher suite »* à utiliser parmi la liste des suites supportées par le Produit. Le Produit restreint les suites TLS à celles recommandées dans [5] pour la version 1.3.

3.2.2 Génération de l'attestation d'application

Le Backend vérifie les données du DeviceCheck fournies par le Produit. La génération des données du DeviceCheck est réalisée par l'OS à la demande du Produit. La demande de génération des données du DeviceCheck doit être conforme à la documentation de l'OS décrite dans [4] et est également analysée lors de l'évaluation.

3.2.3 Saisie sécurisée du code PIN

Pour réaliser certaines cinématiques telles que l'authentification de l'usager avec sa CNIe, le déblocage ou le changement du code PIN de la CNIe, la saisie de l'ancien et/ou du nouveau code PIN par l'usager est nécessaire. Il est donc invité à saisir son code PIN sur son terminal mobile.

Les mécanismes mis en place permettent d'atténuer les risques liés aux enregistreurs de frappe, aux captures d'écran, aux attaques par overlay (superposition d'application) et aux attaques par-dessus l'épaule.

3.2.4 Lecture et opérations sur le Titre d'identité

3.2.4.1 Lecture et Authentification du Titre (application ICAO)

Cette fonctionnalité permet au Backend d'authentifier le Titre et de lire les données d'identité stockées dans le composant électronique du Titre. Elle s'appuie sur la transmission de commandes APDU à destination du Titre depuis le Backend en fonction de différents scénarios d'échanges à l'initiative du Produit.

3.2.4.2 Enrôlement de l'usager

Lors de la première exécution du Produit, un enrôlement est réalisé. Cet enrôlement débute par une lecture et une authentification du Titre telle que définie dans le paragraphe § 3.2.4.1. Les données d'identité de l'usager sont stockées localement de manière sécurisée à des fins de personnalisation de l'interface graphique du Produit. Ces données stockées ne sont pas utilisées à des fins d'authentification.

3.2.4.3 Lecture du Titre et authentification de l'usager et de sa CNIe

Cette fonctionnalité permet au Backend d'authentifier l'usager à l'aide de son code PIN, d'authentifier le Titre, de lire les données de l'application « *eID* » du Titre.

3.2.4.4 Le changement du code PIN de la CNIe

Cette fonctionnalité permet au Produit d'effectuer le changement du code PIN de la CNIe, choisi par l'usager.

3.2.4.5 Le Reset du code PIN

Remarque : En cas d'oubli du code PIN, l'usager peut demander à le réinitialiser. Dans ce cas, le MIE perd son niveau élevé.

L'objectif de ce cas d'usage est de permettre au Backend de pouvoir réinitialiser le code PIN de l'usager lors de la première utilisation de l'application « eID » ou de la perte du code PIN du Titre.

3.2.5 Authentification du Produit

L'authentification du Produit auprès du Backend repose sur le mécanisme de « DeviceCheck ». Ce mécanisme de défense en profondeur permet d'obtenir une forte présomption du fait que la connexion établie par l'usager vers le Backend est réalisée avec un Produit authentique et intègre.

3.3 DESCRIPTION DE L'ENVIRONNEMENT PREVU DU PRODUIT

Le produit est une application « grand public » qui s'exécute sur un smartphone type iOS qui nécessite une CNIe. Il n'y a pas de mesure de sécurité physique particulière lors de l'utilisation du Produit en dehors des précautions élémentaires qui sont fournies dans le guide d'utilisation du Produit.

3.4 DEFINITION DU PERIMETRE D'EVALUATION

Le périmètre regroupe :

- Le canal sécurisé TLS ;
- Le dispositif de saisie sécurisée du code PIN ;
- L'établissement du canal PACE-PIN authentifiant l'usager ;
- La transmission de commandes APDU entre le Titre et le Backend.

Le Produit utilise les dépendances externes suivantes qui sont en dehors du périmètre de l'évaluation :

- L'API et COTS fournis par le système d'exploitation iOS pour réaliser :
  - Les communications NFC avec le Titre de l'usager ;
  - Les interactions entre le Produit et l'OS du mobile de l'usager ;
- La puce NFC du mobile ;
- La zone sécurisée de confiance du terminal mobile (Secure Enclave), compatible avec l'API du système d'exploitation, protégée par des composants matériels.

4 DESCRIPTION DU PROBLEME DE SECURITE

4.1 USAGERS DU PRODUIT

U1 : Usager mobile : utilise les capacités du Produit pour s'authentifier dans un contexte donné auprès du Backend.

4.2 DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

4.2.1 Hypothèses sur la mise à disposition du Produit et de la délivrance du Titre

HD1 : Le processus d'installation du Produit sur le terminal usager est considéré comme étant de confiance (utilisation de l'« App Store » officiel d'Apple garantissant l'installation de composants logiciels signés par leur fournisseur / une autorité de confiance).

HD2 : Les processus de délivrance du Titre, du code d'activation et du code de réinitialisation sont considérés comme étant de confiance et assurent l'authentification du porteur.

HD3 : L'usage de la « Secure Enclave » pour la sécurisation de clés cryptographiques est considéré comme étant de confiance.

4.2.2 Hypothèses concernant le terminal mobile de l'usager

HM1 : L'usager gère son terminal mobile de façon à minimiser les risques de sécurité :

- Le système d'exploitation est à jour et les derniers correctifs de sécurité publiés pour sa version sont appliqués ;
- L'usager ne stocke ni ne communique à quiconque un secret utilisé par le Produit tel que le code PIN du Titre. Il n'est considéré ni malveillant, ni négligeant ;
- Le terminal mobile de l'usager est protégé par un code personnel (mot de passe, PIN, modèle ou biométrie) permettant d'en limiter l'accès en cas de vol.

HM2 : Le terminal mobile assure un premier niveau de protection :

- Les zones sécurisées de la « Secure Enclave » iOS sont considérées comme étant de confiance ;
- L'intégrité de l'application est assurée au moment de son installation et de sa mise à jour sur le terminal mobile ;
- L'OS du terminal mobile restreint les modifications de l'application à la seule suppression ou mise à jour officielle de celle-ci.

4.2.3 Hypothèses concernant le Titre de l'usager

HT1 : L'usager gère son Titre de façon à minimiser les risques :

- L'usager suit les recommandations d'utilisation de son Titre ;
- En cas de perte ou de vol de son Titre, l'usager informe les autorités[1].

HT2 : Le Titre dispose d'une qualification renforcée en cours de validité lorsqu'il est émis.

4.2.4 Hypothèses concernant le Backend

HS1 : Les services du Backend ainsi que l'infrastructure l'hébergeant sont considérés de confiance et audités sur la robustesse des fonctions de sécurité qu'ils mettent en œuvre selon les exigences relatives à la mise en œuvre d'un MIE de niveau élevé.

[1] Le Backend est en mesure de vérifier le statut des Titres (valide, perdu, volé).

HS2 : Les administrateurs du Backend et de l'infrastructure l'hébergeant sont compétents, formés à l'utilisation du Produit et sont considérés comme étant de confiance.

HS3 : Le Backend est configuré selon les guides d'utilisation de la solution.

4.3 BIENS SENSIBLES

B-PIN		Code PIN connu de l'usager
	Stockage	Donnée volatile au niveau du Produit ; En transit entre le Produit et le Titre lors du changement ou reset du code PIN.
	Protection	Confidentialité, Intégrité.
	Durée de vie	10 ans (durée de validité de la CNIe).

B-CAN		CAN du Titre saisi sur le terminal mobile de l'usager
	Stockage	Volatile ; En transit entre le Produit et le Backend.
	Protection	Confidentialité, Intégrité.
	Durée de vie	10 ans (durée de validité de la CNIe).

B-MRZ		MRZ du Titre reconnu à partir de l'appareil photo du terminal mobile de l'usager
	Stockage	Volatile ; En transit entre le Produit et le Backend.
	Protection	Confidentialité, Intégrité.
	Durée de vie	10 ans (durée de validité de la CNIe).

B-TLS_AUTH_SRV_CRT		Le certificat TLS de confiance du Backend est utilisé pour l'authentifier lors de l'établissement des communications sécurisées avec le Produit.
	Stockage	Dans le code du Produit qui a au moins un certificat de la chaine de certification permettant de valider le certificat TLS du Backend.
	Protection	Intégrité : Un attaquant ne devrait pas pouvoir remplacer le certificat contenu dans le Produit qui permet de vérifier la chaine de certification.
	Durée de vie	Durée de vie du Produit.

B-EXCHANGED_DATA		Les données échangées entre le Produit et le Backend
	Stockage	Les données échangées dans le cadre du MIE de niveau élevé entre le Produit et le Backend ne sont jamais conservées. Ces données sont considérées seulement en transit.
	Protection	Confidentialité, Authenticité, Intégrité.
	Durée de vie	Durée de vie de la session applicative.

B-EXCHANGED_DATA_CNIE		Les données échangées entre le Produit et le Titre
	Stockage	Le Produit ne conserve jamais les données échangées avec le Titre. Ces données sont considérées seulement en transit.
	Protection	Confidentialité, Authenticité, Intégrité.
	Durée de vie	Durée de vie de la session avec le Titre.

B-USER_DATA		Les données de l'utilisateur stockées par le Produit
	Stockage	Le Produit conserve les données d'identité de l'usager pour afficher une maquette de la CNIe. Ces données ne sont pas utilisées dans le cadre du MIE de niveau élevé.
	Protection	Confidentialité, Authenticité, Intégrité.
	Durée de vie	Durée de vie du Produit.

B-MASTER_KEY		**La clé protégeant les clés cryptographiques utilisées dans le Produit**
	Stockage	Secure Enclave
	Protection	Confidentialité, Authenticité, Intégrité
	Durée de vie	Durée de vie du Produit

B-USER_DATA_KEY		La clé **protégeant les données d'identité de l'usager**
	Stockage	Géré par l'OS
	Protection	Confidentialité, Authenticité, Intégrité.
	Durée de vie	Durée de vie du Produit.

B-ALEA_STOCKE		Aléa généré par le Backend et utilisé pour alimenter le générateur aléatoire sur le dispositif mobile
	Stockage	En transit entre l'application hôte et le Backend au travers du SDK Stocké sur le dispositif mobile
	Protection	Confidentialité, Authenticité, Intégrité

4.4 AGENTS MENAÇANTS

Les agents menaçants sont les suivants :

- Les attaquants, capables d'intercepter et de modifier les flux de communications entre le Produit et le Backend ;
- Les attaquants, capables d'intercepter et de modifier les flux de communications entre l'application et le Titre ;
- Les attaquants disposant d'un accès physique au terminal mobile de l'usager ;
- Les attaquants disposant d'un accès logique au terminal ou aux données de l'application, via par exemple l'installation d'une porte dérobée ou d'une application malveillante ;
- Les attaquants capables de tromper l'usager par hameçonnage par exemple.

4.5 MENACES

Les scénarios de menaces suivants ont été identifiés :

- Menaces génériques contre le Produit :

  M0 – Altération du Produit : un attaquant parvient à corrompre le Produit.

  M1 – Utilisation d'une version d'application qui n'est pas ou plus légitime

M2 – **Divulgation des données de l'usager** : un attaquant parvient à accéder aux données de l'utilisateur stockées par le Produit.

M3 – **Contrefaçon du Produit ou d'un fournisseur de service** : Un attaquant s'authentifie à la place de l'utilisateur. Par exemple au travers d'une application mobile ou d'un fournisseur de service sous son contrôle, un attaquant demande à un usager de s'authentifier et utilise cette session pour s'authentifier sur un service tiers

- Menaces génériques sur le Titre :

M4 – **Utilisation consécutive à un vol d'un Titre et du terminal associé (utilisé par l'usager durant l'enrôlement de son Titre).**

M5 – **Corruption d'un Titre** : un attaquant parvient à corrompre un Titre usager.

- Menaces sur les secrets :

M6 – Compromission du code PIN : un attaquant parvient à accéder ou modifier le code PIN, via par exemple :

- L'enregistrement de l'écran ;
- L'utilisation d'un overlay (application transparente) ;
- La compromission du clavier utilisé pour la saisie du code PIN.

- Menaces sur la communication entre le Produit et le Backend :

M7 – **Compromission des communications avec le Backend** : un attaquant parvient à intercepter et à modifier les communications entre le Produit et le Backend.

- Menaces sur la communication entre le Produit et le Titre :

M8 – **Compromission des communications CNIe** : un attaquant parvient à intercepter et modifier les communications entre le Produit et le Titre.

5 FONCTIONS DE SECURITE

5.1 FS1 : GESTION SECURISEE DU CODE PIN

5.1.1 Saisie sécurisée du code PIN

Le Produit fournit un clavier virtuel dynamique (DVK) qui assure la sécurité de la saisie du code PIN. Le DVK met en œuvre des mécanismes, décrit dans [6], permettant d'atténuer les risques liés aux attaques par-dessus l'épaule. aux enregistreurs de frappe et aux captures d'écran.

Le code PIN est supprimé dès le démarrage de la lecture du Titre. En cas de non-présentation du Titre (démarrage lecture NFC), le code PIN est supprimé au bout de 10 secondes.

La cryptographie et la génération d'aléa utilisées pour la communication avec le Titre est maitrisée et importée dans le Produit. Le retraitement algorithmique est alimenté par une source entropie gérée par le Produit faisant intervenir un aléa externe provenant du Backend.

Les opérations cryptographiques utilisées sont à l'état de l'art.

5.1.2 Blocage du code PIN

Dans le cas où le code PIN est bloqué par le Titre, le Produit remonte une erreur.

5.1.3 Changement de code PIN

L'usager peut changer le code PIN de son Titre à l'aide de son ancien code PIN (et du CAN si c'est le dernier essai du code PIN).

Le changement de code PIN est réalisé avec l'aide du Backend grâce au code PUK. Le code PUK n'est jamais présent sur le dispositif mobile de l'utilisateur. Le code PUK est calculé coté Backend à partir du CAN transmis par le Produit, saisi par l'utilisateur et du numéro de Titre (fourni par le Titre) durant la cinématique.

5.1.4 Reset du code PIN

La réinitialisation du PIN est réalisée à partir du Backend à l'aide du code PUK. Le code PUK n'est jamais présent sur le terminal mobile de l'usager.

5.2 FS2 : COMMUNICATION SECURISEE AVEC LE BACKEND

Canal sécurisé TLS entre le Produit et le Backend
Les communications entre le Produit et le Backend sont protégées en confidentialité, intégrité et authenticité grâce à un canal sécurisé TLS v1.3 avec authentification du Backend.

Comme décrit dans [3], pour la réalisation du canal sécurisé, le Backend choisit la suite TLS à utiliser parmi la liste des suites supportées du terminal mobile. Le Produit restreint les suites TLS supportées à celles recommandées (cf. [5]). Le Backend doit également suivre les exigences sécuritaires (cf. [5]).

Le certificat TLS du Backend est embarqué dans le Produit**.** Il permet de réaliser une authentification du Backend auprès du Produit lors de l'établissement du canal TLS (*certificate pinning*).

La cryptographie et la génération d'aléa utilisées pour la communication avec le Titre sont maitrisées et importées dans le Produit. Le retraitement algorithmique est alimenté par une source entropie gérée par le Produit faisant intervenir un aléa externe provenant du Backend.

Les opérations cryptographiques utilisées sont à l'état de l'art.

5.3 FS3 : COMMUNICATION SECURISEE AVEC LE TITRE

5.3.1 Établissement du canal PACE-PIN

Le Produit crée des canaux sécurisés avec le Titre à l'aide du protocole PACE (cf. [**1**][**2**]) et du code PIN associé au Titre.

Le PACE-PIN est réalisé par le Produit dans les cinématiques suivantes :

- Lecture du Titre, authentification de l'usager et de la CNIe ;
- Le changement du code PIN.

5.3.2 Établissement du canal PACE-CAN

Le Produit crée des canaux sécurisés avec le Titre à l'aide du protocole PACE (cf. [**1**][**2**]) et du CAN associé au Titre.

Le PACE-CAN est réalisé par le Produit dans les cinématiques suivantes :

- Lecture du Titre
- Le changement du code PIN ;
- La réinitialisation du PIN ;
- Le dernier essai de saisie du PIN.

5.3.3 Canal sécurisé avec le Titre

Des canaux sécurisés avec le Titre sont réalisés par le Produit dans trois cas :

- Lors d'une authentification de la CNIe et de l'usager ;
- Lors du changement du code PIN ;
- Lors de la réinitialisation du code PIN de l'usager.

Le Produit protège les APDU du Titre, authentifie et déchiffre les réponses associées (cf. [**1**][**2**]) à partir des clés de session calculées par le protocole PACE-CAN ou PACE-PIN.

Pour la réinitialisation du code PIN du Titre, le Produit protège en confidentialité et en intégrité l'APDU contenant le code PIN (cf. [**1**][**2**]) à partir des clés de session calculées par le protocole PACE-PUK qui sont fournies par le Backend.

La spécification décrivant la protection des échanges avec le Titre est présentée dans les standards (cf. [**1**][**2**]).

Cryptographie et Génération d'aléa
La cryptographie et la génération d'aléa utilisées pour la communication avec le Titre sont maitrisées et importées dans le Produit. Le retraitement algorithmique est alimenté par une source entropie gérée par le Produit faisant intervenir un aléa externe provenant du Backend.

5.4 FS4 : GENERATION DE LA PREUVE DE LEGITIMITE DE L'APPLICATION

Afin de garantir au service applicatif backend que la connexion est établie avec l'application légitime, le SDK génère une preuve de légitimité s'appuyant sur les mécanismes et API du système d'exploitation prévus à cet effet : les mécanismes d'attestation de clé décrit dans [4].

La preuve de légitimité de l'application comprend l'attestation de la clé et la preuve de possession de la clé privée associée.

La mise en œuvre de l'utilisation des API offertes par le système d'exploitation permettant la génération de la preuve de légitimité de l'application est correctement réalisée et est conforme aux guides d'utilisation décrit dans [4].

5.5 FS5 : PROTECTION DES DONNEES D'IDENTITE DE L'USAGER

Le stockage des données d'identité de l'usager repose sur un mécanisme de chiffrement offert par l'OS.

5.6 FS6 : AUTORISATION DE L'APPLICATION MOBILE PAR LE BACKEND

Afin de s'assurer que seul le Produit est autorisé à ouvrir les liens (deeplink) gérés et proposés par le Backend, le Produit implémente les mécanismes dits « Universal Links » offerts par le système d'exploitation et décrit dans [7].

6 COUVERTURE DES MENACES

6.1 MENACES ET BIENS SENSIBLES

	B-PIN	B-CAN	B-MRZ	B-TLS_AUTH_SRV_ CRT	B-EXCHANGED_DATA	B-EXCHANGED_DATA_CNIE	B-USER_DATA	B-MASTERKEY	B-USER_DATA_KEY	B-ALEA_STOCKE
M0 – Altération du Produit	x	x	x	x	x	x				x
M1 – Utilisation d'une version d'application qui n'est pas ou plus légitime	x	x	x	x	x	x				x
M2 – Divulgation des données de l'usager							x			
M3 – Contrefaçon du Produit ou d'un fournisseur de service	x	x	x	x	x	x				
M4 – Utilisation consécutive à un vol d'un Titre et du terminal associé	x	x	x	x			x	x	x	
M5 – Corruption d'un Titre	x	x	x		x	x				
M6 – Compromission du code PIN	x									
M7 – Compromission des communications avec le Backend		x	x		x					x
M8 – Compromission des communications CNIe	x		x			x				

6.2 MENACES, FONCTIONS DE SECURITE ET HYPOTHESES

	M0 – Altération du Produit	M1 – Utilisation d'une version d'application qui n'est pas ou plus légitime	M2 – Divulgation des données de l'usager	M3 – Contrefaçon du Produit ou d'un fournisseur de service	M4 – Utilisation consécutive à un vol d'un Titre et du terminal associé	M5 – Corruption d'un Titre	M6 – Compromission du code PIN	M7 – Compromission des communications Backend	M8 – Compromission des communications CNIe
		Fonctions de sécurité							
FS1					x		x		
FS2							x	x	
FS3						x			x
FS4		x							
FS5			x		x				
FS6				x					
		Hypothèses							
HD1	x	x							
HD2					x		x		
HD3		x	x						
HM1	x		x					x	x
HM2	x	x	x					x	x
HT1					x		x		
HT2						x	x		x
HS1								x	
HS2								x	
HS3								x	