Cible de Sécurité CSPN

Application e-CPS

Identification du document	
Référence Programme	/IDNUM/INECPS
Date de création	19/04/2021
Date de dernière mise à jour	24/11/2021
État	Final
Version	1.2
Classification	Public
Nombre de pages	20

Historique des versions

Version	Date	Auteur	Nature de la révision Paragraphes modifiés
0.1	19/04/2021	Red Alert Labs	Création du document
0.2	02/05/2021	Red Alert Labs	Mise à jour du contenu et version pour commentaire
0.5	03/05/2021	Red Alert Labs	Version pour commentaires
0.6	04/05/2021	IN Groupe	Mise à jour du contenu et version pour commentaire
0.7	06/05/2021	Red Alert Labs	Prise en compte des commentaires et mise à jour du contenu
0.8	17/05/2021	IN Groupe	Réponses aux remarques et commentaires
0.85	25/05/2021	Red Alert Labs	Prise en compte des réponses et commentaires
1.0	17/06/2021	IN Groupe	Version finale
1.1	24/11/2021	IN Groupe	Ajustement des numéros des versions soumises à évaluation
1.2	19/12/2022	Red Alert Labs	Séparation Android/iOS et ajustements

Table des matières

I. Introduction

I.1. OBJET DU DOCUMENT

Le présent document est une cible de sécurité réalisée dans le cadre d'une évaluation du produit e-CPS selon la méthodologie CSPN de l'ANSSI. La cible est structurée suivant la description de la section **4.2** du référentiel [ANSSI_CSPN_CER_P_02].

I.2. IDENTIFICATION DU PRODUIT EVALUE

L'évaluation concerne une application mobile de gestion d'identité numérique (e-CPS). Ce produit communique avec l'utilisateur et une Plateforme logicielle distante (nommée « Plateforme »).

Organisation éditrice	IN Groupe
Lien vers l'organisation	https://www.ingroupe.com/
Nom commercial du produit	e-CPS
Numéro des versions évaluées	Le produit est évalué dans les versions suivantes : – Android : 2.3.22
Catégorie de produit	Identification, authentification et contrôle d'accès

I.3. DOCUMENTS DE REFERENCE

Référence	Nom du document
[ANSSI_CSPN_CER_P_02]	*CRITERES POUR L'EVALUATION EN VUE D'UNE CERTIFICATION DESECURITE DE PREMIER NIVEAU* https://www.ssi.gouv.fr/uploads/2015/01/anssi-cspn-cer-p-02-criteres_pour_evaluation_en_vue_d_une_cspn_v4.0.pdf *Version: 4.0*
[ANSSI_RSR_TLS]	*Recommandations de sécurité relatives à TLS.* https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf *Version: 1.2*
[DAT]	*Dossier d'Architecture Technique (DAT)* Version 1.1 du 08/11/2021
[SAD]	*Software Architecture Document (SAD)* Version 1.0 du 25/01/2019
[SDD]	*Conception des services d'e-CPS* Version 1.2 du 10/11/2021
[HOTP]	https://tools.ietf.org/html/rfc4226
[RGS_B1]	*GUIDE DES MÉCANISMES CRYPTOGRAPHIQUES (ex RGS Annexe B1)* *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.* https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf *Version: 2.04*

Référence	Nom du document
[RGS_B2]	*Référentiel Général de Sécurité, AnnexeB2* *Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques.* https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B2.pdf *Version: 2.0*
[RGS_B3]	*Référentiel Général de Sécurité, AnnexeB3* *Règles et recommandations concernant les mécanismes d'authentification* https://www.ssi.gouv.fr/uploads/2015/01/RGS_B_3.pdf *Version: 1.0*
[SPEC_CRYPTO]	*Mécanismes cryptographiques e-CPS* *Version : 1.1*

I.4. GLOSSAIRE

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANS	Agence du Numérique en Santé
CSPN	Certification de Sécurité de Premier Niveau
CPS	Carte Professionnel de Santé
DMP	Dossier Medical Partagé
HOTP	*HMAC One Time Password*
HSM	*Hardware Security Module*
LDAP	*Lightweight Directory Access Protocol*
RPPS	Répertoire Partagé des Professionnels de Santé
TLS	*Transport Layer Security*
OS	Système d'exploitation (*Operating System*).

II. Description de la cible

II.1. DESCRIPTION GENERALE

La solution e-CPS est une solution innovante pour le monde de la santé visant à accompagner les professionnels de santé dès qu'ils souhaitent utiliser leur mobile ou leur tablette dans le cadre de leur activité. e-CPS fait partie des projets dits de "e-santé" répondant aux enjeux croisés de la médecine contemporaine : mobilité et sécurité renforcée autour des données de santé.

Qu'est-ce que le projet e-CPS ?

IN Groupe, qui réalise depuis 2012 la CPS (Carte des Professionnels de Santé) utilisée quotidiennement par les professionnels pour signer leurs actes médicaux, porte le projet e-CPS en partenariat avec l'ANS et la Caisse nationale d'assurance maladie (Cnam).

Grâce à ce projet, le praticien peut dériver sa carte CPS sur son smartphone ou sa tablette grâce à une application disponible pour les ordiphones (Android et Apple). Cette application, actuellement en production a pour ambition d'être **universelle** (c'est-à-dire pouvoir s'installer sur tous les smartphones mobiles et les tablettes) et **simple d'utilisation**.

Permettre un usage en mobilité

Aujourd'hui, l'utilisation des mobiles est devenue incontournable aussi bien dans la vie quotidienne que professionnelle. Echanger des données de santé via MSSanté, rechercher des informations dans le DMP, méritent qu'une attention particulière soit portée sur l'authentification des professionnels de santé dès qu'ils souhaitent utiliser leur mobile dans le cadre de leur activité. Il était donc essentiel que la carte CPS puisse évoluer en ce sens pour faciliter les usages en mobilité et s'adapter aux nouvelles exigences du numérique.

D'un niveau de sécurité équivalent à la carte CPS, la solution e-CPS permet aux professionnels de santé de s'authentifier directement auprès d'un service en ligne avec son mobile ou sa tablette, sans passer par un poste configuré et équipé d'un lecteur de carte. La e-CPS devient un moyen supplémentaire de s'authentifier ; la détention d'une carte CPS n'est donc plus indispensable. Elle est ainsi dématérialisée.

Assurer une authentification renforcée pour échanger des données de santé sécurisées en toute sécurité

La solution e-CPS est un des dispositifs d'authentification que les services en ligne pourront offrir en s'adossant à Pro Santé Connect. Pro Santé Connect réalise l'authentification à la place des services numériques de santé et décharge les acteurs de cette gestion. Au-delà de ces simplifications pour les acteurs, Pro Santé Connect permet également d'homogénéiser la qualité des contrôles d'identité sur l'ensemble des services et, le cas échéant, d'y apporter des évolutions (fonctionnelles, réglementaires, technologiques) pouvant être déployées instantanément sur l'ensemble du territoire, sans impacter le fonctionnement des services numériques raccordés.

La solution e-CPS en synthèse :

- Elle permet de s'authentifier avec sa CPS ou avec son ordiphone afin d'accéder à des applications où qu'elles soient (installées sur un ordiphone/tablette, sur un poste de travail fixe ou en mode SAS)
- Elle regroupe un Fournisseur d'Identité « Pro Santé Connect » et un dispositif d'authentification sur ordiphone « e-CPS »
- Elle met en œuvre des techniques similaires à celles de France Connect
- Elle est opérationnelle pour l'ensemble des porteurs de carte CPS
- Elle libère les services utilisateurs des contraintes de l'authentification et de sa maintenance sécuritaire
- Elle garantit aux services utilisateurs la conformité réglementaire
- Elle est une solution d'authentification permettant de compléter ou de s'affranchir de la carte CPS

II.2. UTILISATION DU PRODUIT

Vu de l'utilisateur, la mise en œuvre de l'application e-CPS s'effectue en deux étapes.

II.2.1. PREMIERE ETAPE : DERIVATION

Lors de cette étape, l'utilisateur crée son identité numérique et installe l'application e-CPS sur son ordiphone.

Figure 1 - Description du processus d'inscription à l'aide de la CPS

Il existe deux possibilités afin de créer son identité numérique, avec ou sans l'utilisation de la carte CPS.

1. Activation de e-CPS à l'aide de la carte CPS

Une des deux procédures de dérivation disponibles s'appuie sur l'utilisation de la carte CPS, elle est présentée par l'utilisateur pour lui permettre de justifier de son identité. L'adresse courriel et le numéro de téléphone sont aussi récoltés durant cette étape.

Le Schéma 1 décrit de façon détaillée les échanges ayant lieu lors de l'activation de e-CPS à l'aide de la carte CPS.

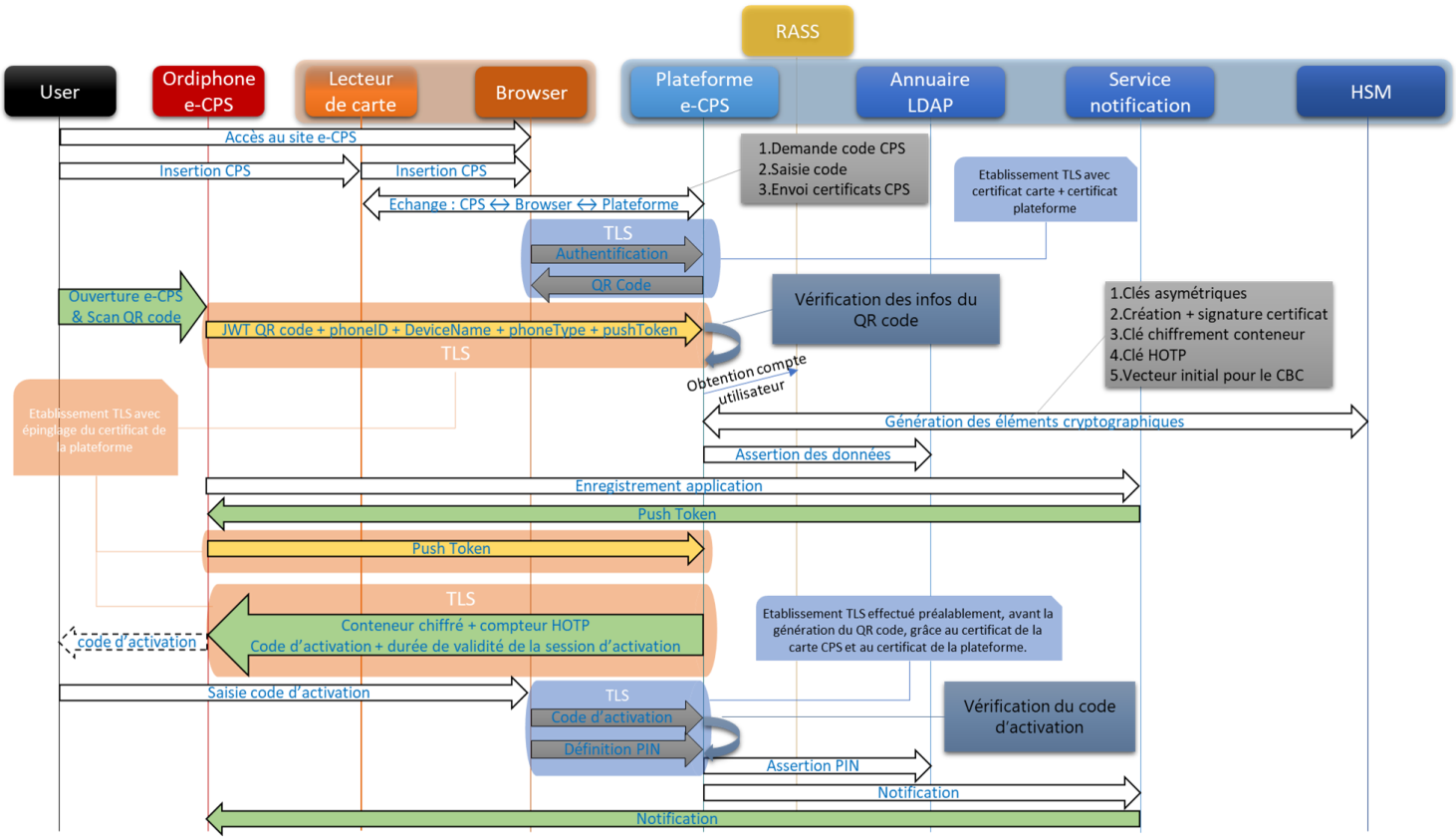

Schéma 1 - Echanges durant le processus d'activation de e-CPS à l'aide de la CPS

La génération des éléments cryptographiques évoqués dans le Schéma 1 sont explicités ci-dessous.

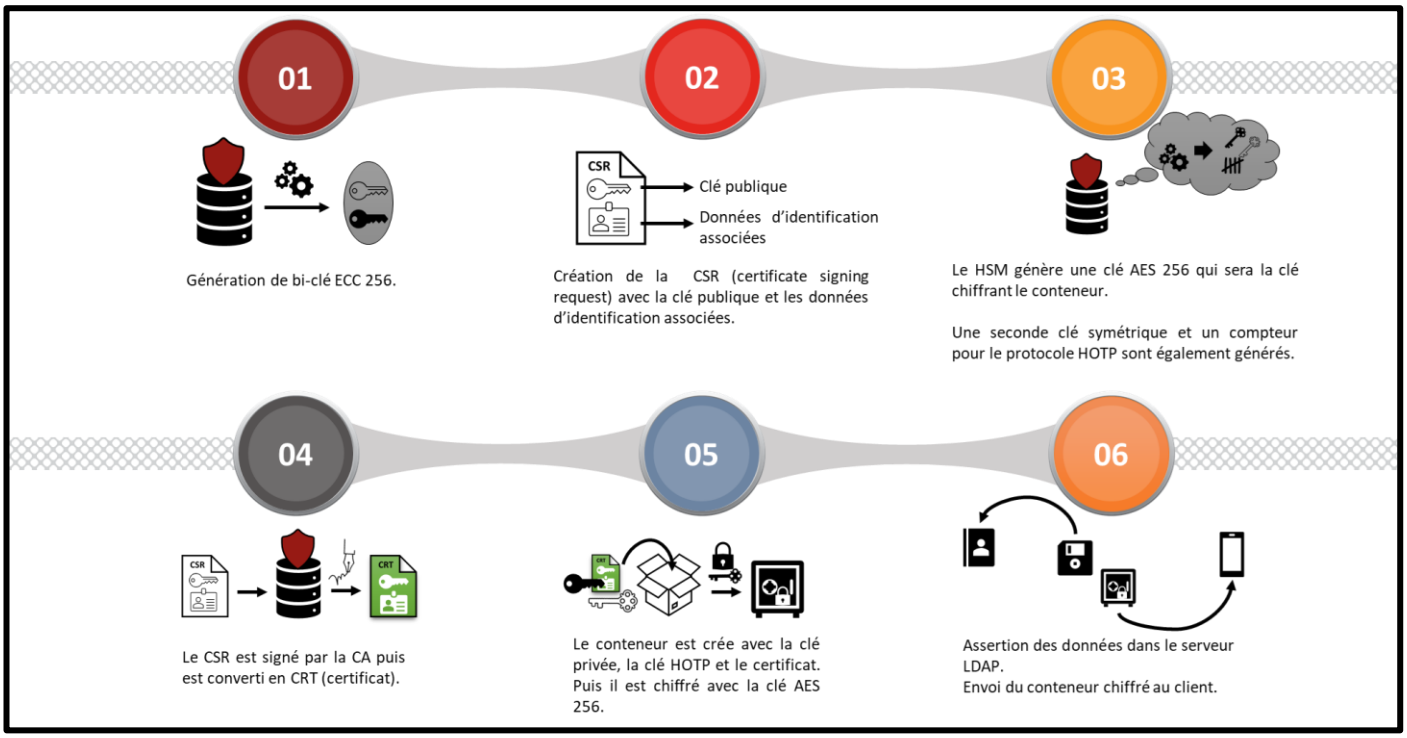

Schéma 2 - Description de la génération des éléments cryptographiques

2. *Activation de e-CPS sans la carte CPS.*

La seconde procédure de dérivation possible ne nécessite pas la carte CPS. Dans ce cas :

- L'utilisateur va s'authentifier et associer son identité avec l'application grâce à ;
  - son numéro d'identifiant national,
  - l'adresse mail et le numéro de téléphone mobile associés à celui-ci dans la base de données de l'ANS.
- Un lien d'activation et un QR code seront envoyés à l'adresse mail,
- Une fois le lien d'activation utilisé un SMS contenant un code d'activation sera envoyé au numéro de téléphone associé.
- L'utilisateur rentre ce code d'activation dans son téléphone et est authentifié.
- Une fois que l'utilisateur est authentifié à travers ces étapes il devra comme dans la méthode avec la carte CPS définir un code PIN qui lui sera par la suite demandé à chaque authentification.

II.2.2. SECONDE ETAPE : AUTHENTIFICATION LORS DE L'ACCES A UN SERVICE

L'utilisateur se connecte à un service requérant une authentification par carte CPS ou équivalent ; l'acceptation du moyen d'authentification est du ressort du service. L'utilisateur reçoit alors une notification sur son ordiphone permettant de lancer l'application mobile. Cette notification présente le service auquel il souhaite accéder, et l'utilisateur doit saisir un code d'authentification défini lors de l'inscription pour accéder au service.

La Figure 2 - Description du processus d'authentification suivante représente les grandes étapes du processus d'authentification de l'utilisateur, tandis que le Schéma 3 décrit de manière plus précise l'ensemble des échanges lors du processus.

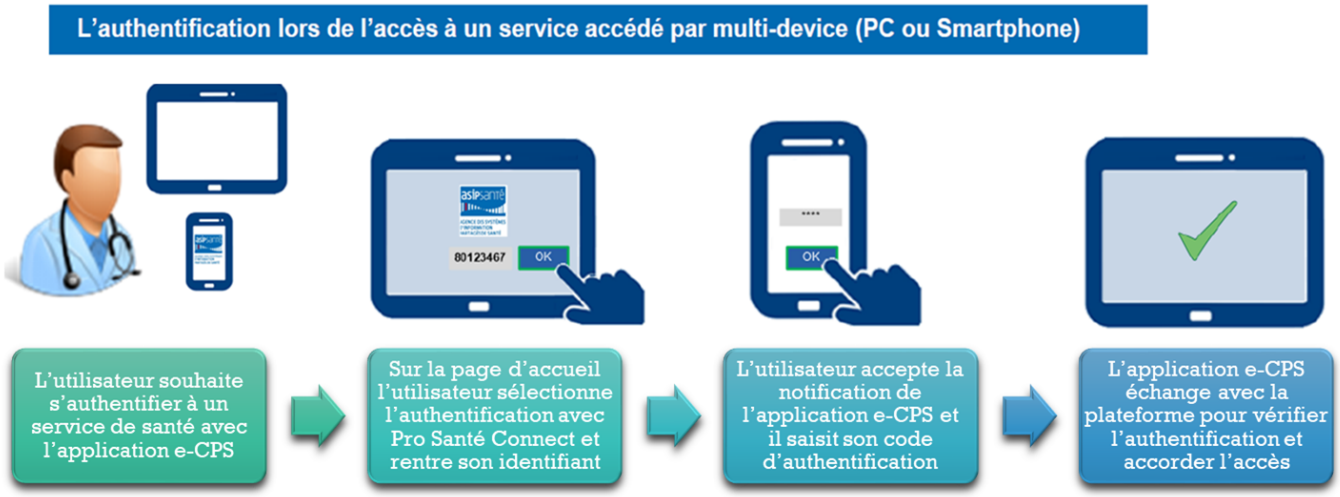

Figure 2 - Description du processus d'authentification

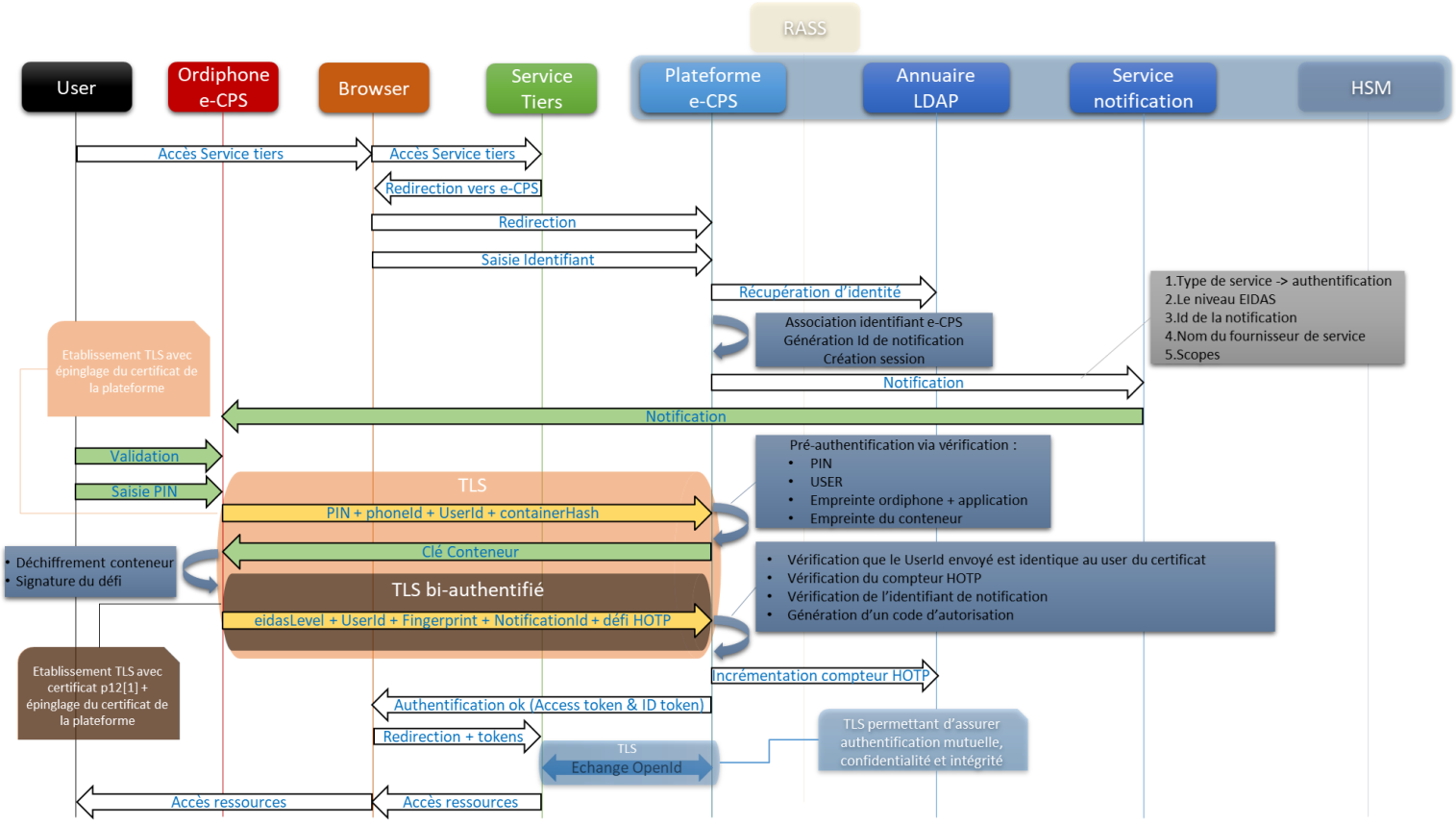

Schéma 3 - Détails des échanges lors de la procédure d'authentification

II.3. DESCRIPTION DES DEPENDANCES

L'application mobile doit être installée sur un ordiphone Android disposant d'une connexion Internet.

Il est requis que l'ordiphone fonctionne au minimum sous la version 6 d'Android pour exécuter l'application e-CPS. La protection de certains biens en lien avec l'application repose directement sur les fonctions de sécurité du système d'exploitation.

L'application e-CPS fonctionnant sur l'ordiphone ou la tablette communique avec une plateforme logicielle distante hébergée et exploitée par IN Groupe. D'un point de vue fonctionnel, l'application e-CPS n'est pas utilisable sans la plateforme associée. En effet, c'est avec celle-ci que le service tiers, sur lequel le porteur tente de s'authentifier, communique.

Pour l'inscription, l'utilisateur doit de plus disposer d'un compte sur le « *store* » correspondant à son environnement (nécessaire au téléchargement de l'application mobile), ainsi que posséder une carte CPS ou un numéro RPPS. Si l'utilisateur sélectionne la méthode d'activation avec la carte CPS, il doit également disposer d'un poste de travail possédant un lecteur de carte, un navigateur web et une connexion internet.

II.4. DESCRIPTION DE L'ENVIRONNEMENT D'EXECUTION

II.4.1. MATERIEL COMPATIBLE OU DEDIE

L'environnement technique nécessaire au fonctionnement de l'application, nécessite un appareil physique (ordiphone ou tablette) prenant en charge l'environnement d'exécution de l'application mobile et disposant d'une connectivité internet (via une carte SIM avec abonnement données mobile ou via WIFI).

L'application e-CPS fonctionnant sur l'ordiphone ou la tablette communique avec une plateforme logicielle distante hébergée et exploitée par IN Groupe.
La plateforme garantit différent rôles :

- Vérification de l'identité de l'utilisateur lors de l'inscription.
- Dérivation de son identité numérique.
- Création des éléments cryptographiques.
- Stockage des données nécessaires au fonctionnement de l'application.
- Transfert au client des données nécessaires.
- Notification du client des tentatives d'authentification.
- Vérification de l'authentification.

Afin d'assurer ces rôles la plateforme communique avec :

- Un serveur LDAP
- Un service de notification tiers
- Un HSM
- L'annuaire RASS de l'ANS

L'application e-CPS et la plateforme distante communique à travers un protocole sécurisé (TLS).
Tous les éléments communiquant avec la plateforme utilisent également des protocoles sécurisés (LDAPS, HTTPS)

II.4.2. PRECISIONS SUR LES SYSTEMES D'EXPLOITATIONS

Cette cible de sécurité couvre les spécificités du système d'exploitation Android.

Dans un objectif d'évaluation, l'application e-CPS sera la version 2.3

La plateforme fonctionnera sur un serveur Linux mis à jour comprenant les derniers correctifs de sécurité.

Il existe de légères distinctions entre les versions iOS et Android, celles-ci sont explicitées dans chacune des cibles.

- L'empreinte de l'ordiphone (phoneId) correspondant au SHA256 de la concaténation des éléments suivants :
  - la marque de l'ordiphone (BRAND),
  - le nom correspondant à la révision spécifique de l'appareil (DEVICE),
  - le modèle de l'ordiphone (MODEL),
  - le code de pays du fournisseur de la carte SIM (simCountryIso),
  - le code de pays + le code réseau opérateur (simOperator),
  - le nom du fournisseur de service de la carte SIM (simOperatorName),
  - empreinte de l'identifiant unique de 128 bits généré lors du premier lancement de l'application (UUID).

- Les données persistantes sont protégées par les fonctionnalités mis à disposition par le système d'exploitation, pour Android il s'agit du Keystore implémenté dans un environnement d'exécution de confiance.

II.5. PERIMETRE D'EVALUATION DU PRODUIT

Le périmètre d'évaluation comprend :

- L'application dans sa globalité incluant :
  - Le processus d'inscription ;
  - Le processus d'authentification ;
- Le stockage des biens par l'application sur l'ordiphone ;
- Les communications entre l'application e-CPS et la plateforme distante.

Les éléments suivants sont considérés comme en dehors du périmètre de cette évaluation CSPN.

- Le navigateur web interagissant avec l'utilisateur ;
- La plateforme logicielle distante.

Le périmètre d'évaluation est résumé par la Figure 3 ci-dessous.

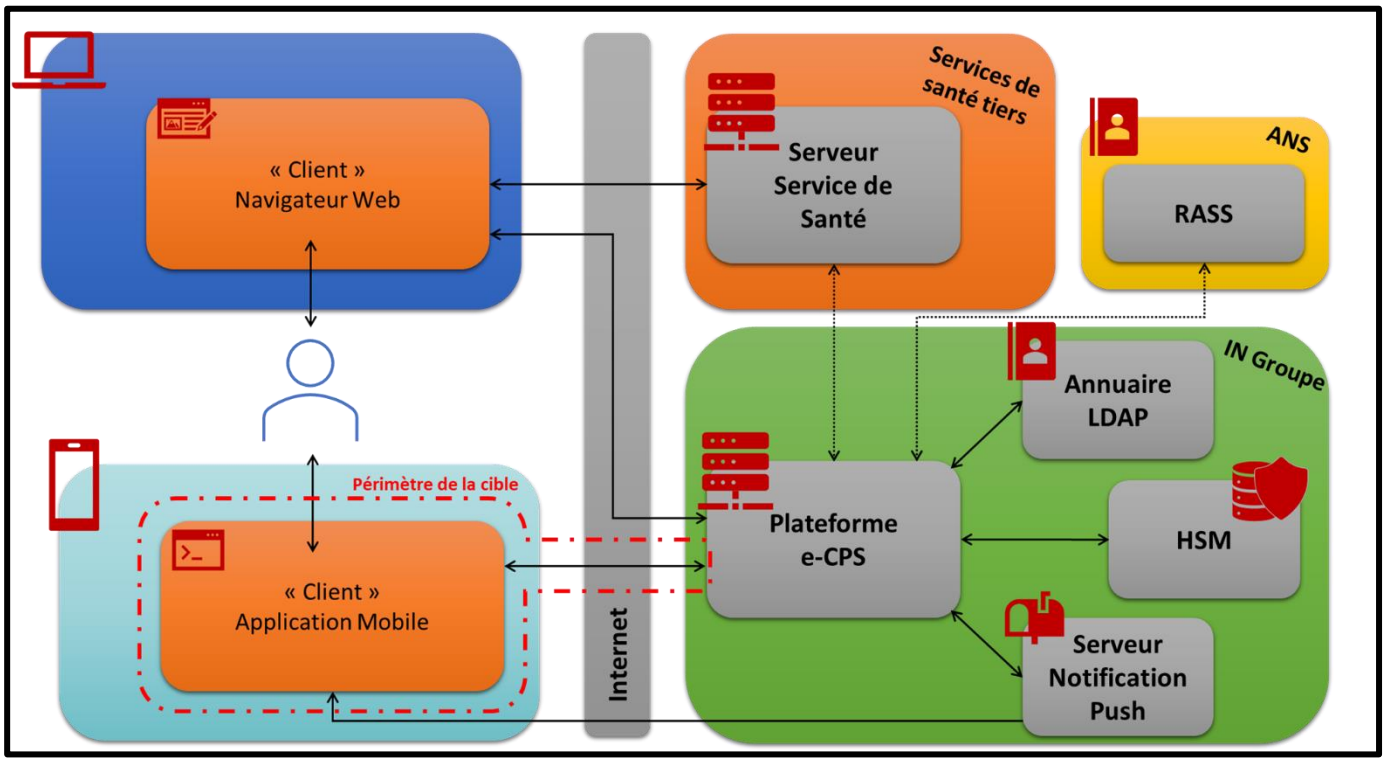

Figure 3 - Périmètre de l'évaluation

III. Problématique de sécurité

III.1. DESCRIPTION DES UTILISATEURS

- Les utilisateurs de l'application e-CPS

Les utilisateurs typiques à prendre en compte sont les utilisateurs finaux de l'application e-CPS.
Les utilisateurs finaux sont généralement des professionnels de santé qui doivent s'authentifier auprès d'un service distant.

Dans un souci de compréhension, il est important de noter que d'autres utilisateurs / acteurs indirects sont impliqués dans l'environnement de la solution :

- *Les fournisseurs de services*

Un service tiers utilisant le résultat des authentifications sur la plateforme pour authentifier les utilisateurs finaux.

- *Administrateurs de la plateforme*

Le gestionnaire de la plate-forme.

III.2. BIENS SENSIBLES

Les biens sensibles à protéger sont ceux impliqués dans le bon fonctionnement de l'application. Cette liste couvre à la fois le processus d'inscription et le processus d'authentification.
Chacun de ces actifs est lié à au moins un critère de sécurité (également appelé besoin de sécurité) : intégrité, authenticité et confidentialité.

Conteneur :
Durant la phase d'inscription un conteneur contenant des éléments sensibles est transmis par la plateforme à l'application mobile. Ce conteneur est stocké dans la mémoire de l'ordiphone et est transmis chiffré. La clé de déchiffrement est enregistrée sur la plateforme et transmise à l'ordiphone au moment de chaque authentification.

Le conteneur contient les biens sensibles suivant :

- B1. Clé privée (p12[0]) :
Le conteneur protège une clé privée utilisée dans le mécanisme d'authentification entre l'application et la plateforme. La clé privée est générée par la plateforme. Elle est associée aux données d'identification et à la clé publique avec un certificat X509v3 puis stockée dans un conteneur chiffré. Ce dernier est stocké temporairement puis fourni à la cible pendant le processus de dérivation.
Besoins de sécurité : Confidentialité, Intégrité, Authenticité.

- B2. Clé publique – Certificat (p12[1]) :
Le conteneur protège un certificat X509v3. Ce certificat contient la clé publique associée à la clé privée p12[0], ainsi que des données d'identification propre à l'utilisateur et est signé par une autorité de certification hébergée et exploitée par IN Groupe.
Besoins de sécurité : Intégrité, Authenticité.

- B3. Clé HOTP (« secret ») :

Le conteneur protège une clé secrète utilisée comme graine dans l'algorithme HOTP durant le processus d'authentification. La clé secrète est générée par la plateforme durant le processus d'inscription. La clé est stockée dans la plateforme ainsi que dans le conteneur. Elle est par la suite utilisée à chaque authentification de l'utilisateur.

Besoins de sécurité : Confidentialité, Intégrité.

Les biens décrit ci-dessous ne sont pas stockés dans le conteneur.

- B4. Clé chiffrement conteneur :

Le conteneur est chiffré par une clé AES qui est stockée par la plateforme et fournit à l'application lors de la phase de pré-authentification. Elle est stockée en dehors du périmètre de la cible.

Besoins de sécurité : Confidentialité.

- B5. Données persistantes :

D'autres éléments sont stockés dans l'ordiphone et utilisés par l'application :

1. **Compteur HOTP (HOTP_COUNTER)**
   Un compteur est utilisé dans l'algorithme HOTP durant le processus d'authentification. Ce dernier est généré par la plateforme durant le processus d'inscription, puis est stocké par cette dernière ainsi que dans l'ordiphone. Il est stocké dans le périmètre de la cible.
2. **UUID**
   Identifiant unique de 128 bits généré lors du premier lancement de l'application. Cet identifiant est stocké de manière chiffrée dans les données persistantes. La clé de chiffrement de l'UUID est créée, hébergée et gérée par le *Keystore* de l'ordiphone et se trouve donc en dehors du périmètre de cette évaluation.
3. **L'identifiant utilisateur (NAT_ID = UserID)**
   Identifiant unique correspondant au numéro d'identification du professionnel de santé.
4. **Autres :**
   - FIRST_LAUNCH_AFTER_ACTIVATION
   - activationTimeoutDuration
   - CURRENT_PUSH_TOKEN_HASH_ID_KEY
   - PAIRING_CODE_ID_KEY
   - WALLET_STATE_KEY
   - EXPIRATION_CARD_TIME_KEY
   - EXPIRATION_ECPS_TIME_KEY
   - EXPIRATION_ECPS_TIME_OMB_KEY
   - SAFETY_NET_TIME
   - EXPIRATION_CARD_TIME_OMB_KEY
   - SAFETY_NET_NONCE

Besoins de sécurité : Confidentialité, Intégrité.

- B6. Données nécessaires à l'authentification :

Certaines données propres à l'ordiphone ou à l'utilisateur, permettant l'authentification, sont générées de manière dynamique, récupérées ou traitées de façon temporaire et ne sont pas stockées dans le périmètre de cette cible.

- phoneId
  - Il s'agit d'une empreinte du téléphone, correspondant au SHA256 de la concaténation des éléments suivants :
    - la marque de l'ordiphone (BRAND),
    - le nom correspondant à la révision spécifique de l'appareil (DEVICE),
    - le modèle de l'ordiphone (MODEL),
    - le code de pays du fournisseur de la carte SIM (simCountryIso),
    - le code de pays + le code réseau opérateur (simOperator),
    - le nom du fournisseur de service de la carte SIM (simOperatorName),
    - empreinte de l'identifiant unique de 128 bits généré lors du premier lancement de l'application (UUID).

- Empreinte du conteneur.
- Identifiant utilisateur
- NotificationID

Besoins de sécurité : Intégrité.

- B7. Données personnelles :

Des données personnelles peuvent être récupérées par l'application.

- commonName : l'identifiant nationale de la personne
- surname : le nom de la personne
- given name : le prénom de la personne
- personal title : l'intitule du poste de la personne
- personal title code : le code de l'intitule du poste
- exercises : Les exercises liés au professionnel de santé.

Besoins de sécurité : Confidentialité.

- B8. Empreintes des certificats TLS épinglés de la plateforme :

Empreinte du certificat épinglé de la plateforme, pour l'authentification TLS.
Besoins de sécurité : Intégrité.

- B9. PIN :

Le processus d'authentification nécessite un PIN (code à 4 chiffres) connu uniquement de l'utilisateur. Le PIN est choisi par l'utilisateur lors de la phase d'inscription et est envoyé au serveur, où il est stocké chiffré avec BCRYPT10. Il est par la suite demandé à l'utilisateur à chaque authentification, il est transmis au serveur et vérifié par ce dernier.
Besoins de sécurité : Confidentialité, Intégrité.

		Intégrité	Authenticité	Confidentialité
B1	Clé privée (p12[0])	✓	✓	✓
B2	Clé publique – Certificat (p12[1])	✓	✓	
B3	Clé HOTP (« secret »)	✓		✓
B4	Clé chiffrement conteneur			✓
B5	Données persistantes	✓		✓
B6	Données nécessaires à l'authentification	✓		
B7	Données personnelles			✓
B8	Empreintes des certificats TLS épinglés de la plateforme	✓		
B9	PIN	✓		✓

Tableau 1- Matrice des biens en fonction des besoins de sécurité

III.3. HYPOTHESES D'ENVIRONNEMENT

1. Utilisateur et Ordiphone

- **H1. L'utilisateur gère son équipement mobile de manière à minimiser les risques de sécurité. Plus précisément:**
  a. Le système d'exploitation de l'équipement mobile est toujours à jour et les derniers correctifs de sécurité disponibles sont régulièrement appliqués.
  b. Le chiffrement du système de fichiers est activé chaque fois qu'il est disponible.
  c. Une authentification est nécessaire pour déverrouiller l'équipement (ex: mot de passe, biométrique).
  d. L'utilisateur n'enregistre pas son code PIN à l'intérieur de l'équipement mobile et ne le transmet pas à un tiers. Le code PIN n'est utilisé pour aucune autre utilisation que l'authentification dans le cadre du produit.
  e. Lors de l'installation de l'application et lors de la première connexion par l'utilisateur (activation de e-CPS), le téléphone n'est pas rooté.
- **H2. Keystore et TEE / SE**
  Le terminal possède un keystore basé sur un Trusted Execution Environment (TEE) ou un Secure Element (SE).

2. Plateformes distante et communications liées

- **H3. Plateforme et dépendances opérationnelles**
  Il est considéré que la plateforme et ses dépendances (matériels et logiciels) sont renforcées et non corrompues (seuls les administrateurs et utilisateur autorisés peuvent y accéder). De plus les communications ayant lieu entre ces entités sont gérées de manière à assurer la confidentialité, l'intégrité et l'authenticité des échanges.
- **H4. Protection des données**
  Les données utilisateurs et les données relatives au fonctionnement de la cible, stockées sur les serveurs distants sont protégées contre toute perte de confidentialité et d'intégrité.
- **H5. Cryptographie fiable**
  Les ressources informatiques et cryptographiques utilisées par la plateforme sont fiables et de confiance.
  Le générateur de nombres aléatoires de la solution a une qualité suffisante pour être utilisé comme source d'entropie, conformément aux règlement [RGS_B1]. De même la création et la gestion des clés utilisées suivent les règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques du RGS.
  .

III.4. DESCRIPTIONS DES MENACES

Cette section décrit les menaces à éviter par la cible. Ces menaces découlent des biens protégés par la cible et de la méthode d'utilisation de la cible dans l'environnement opérationnel.
Par définition, une menace est une action ou un événement susceptible de porter atteinte à la sécurité de l'application e-CPS.

Les menaces suivantes ont été identifiées :

- **M1. VOL_PIN : Vol du code PIN durant la saisie**
  Capture du code PIN durant la saisie de celui-ci sur le clavier de l'application par un utilisateur.

  Biens impactés : PIN.
- **M2. VOL_LOCAL : Vol des données stockées localement**

Un attaquant pourrait collecter les données liées à l'application enregistrées sur l'ordiphone afin de récupérer des informations sensibles ou de réussir une authentification illégitime.

Biens impactés : Clé privée (p12[0]), Clé HOTP (« secret »), Données persistantes.

- M3. MODIF_LOCAL : Modification des données stockées localement
Un attaquant pourrait modifier les données liées à l'application enregistrées sur l'ordiphone.

Biens impactés : Clé privée (p12[0]), Clé publique – Certificat (p12[1]), Clé HOTP (« secret »), Données persistantes, Empreintes des certificats TLS épinglés de la plateforme.

- M4. VOL_TRANSIT : Vol des données en transit
Un attaquant pourrait collecter les données sensibles lors des échanges entre la plateforme et l'application afin de récupérer des informations sensibles ou de réussir une authentification illégitime.

Biens impactés : Tous sauf - B2 et - B8.

- M5. MODIF_TRANSIT : Modification des données en transit
Un attaquant pourrait modifier les données lors des échanges entre la plateforme et l'application.

Biens impactés : Tous sauf - B7 et - B8.

- M6. BYPASS_AUTH : Contournement du processus d'authentification
Un utilisateur malveillant pourrait tenter de contourner le processus d'authentification en rejouant des requêtes interceptées afin d'obtenir des données sensibles ou une authentification illégitime.

Biens impactés : Données personnelles.

- M7. CLONE : Clonage
Un utilisateur malveillant pourrait cloner l'application et les biens protégés enregistrés sur l'ordiphone afin de les utiliser dans un autre équipement (ordiphone, émulateur …). L'utilisateur malveillant pourrait alors usurper l'identité de l'utilisateur légitime obtenir des accès non autorisés chez des fournisseurs de service.

Biens impactés : Données personnelles.

La table ci-dessous décrits les impacts en Confidentialité (C), Intégrité (I) et Authenticité (A) des menaces sur les bien

		VOL_PIN	VOL_LOCAL	MODIF_LOCAL	VOL_TRANSIT	MODIF_TRANSIT	BYPASS_AUTH	CLONE
		-M1	**-M2**	**-M3**	**-M4**	**-M5**	**-M6**	**-M7**
B1	Clé privée (p12[0])		**C A**	**I A**	**C A**	**I A**		**C A**
B2	Clé publique – Certificat (p12[1])			**I A**		**I A**		**A**
B3	Clé HOTP (« secret »)		**C**	**I**	**C**	**I**		**C**
B4	Clé chiffrement conteneur				**C**			
B5	Données persistantes		**C**	**I**	**C**	**I**		**C**
B6	Données nécessaires à l'authentification					**I**		
B7	Données personnelles				**C**		**C**	**C**
B8	Empreintes des certificats TLS épinglés de la plateforme			**I**				

B9	PIN	**C**			**C**	**I**		

Tableau 2 - Matrice des biens en fonction des menaces

III.5. FONCTIONS DE SECURITE

- FS1. Protection des communications

- Implémentation du protocole TLS

  Les données échangées entre la plateforme et l'application sont protégées en authenticité, confidentialité et en intégrité via l'emploi du protocole HTTPs utilisant TLS suivant le guide de recommandation de l'ANSSI [ANSSI_RSR_TLS]. Pour le détails des suites de chiffrement utilisées, des algorithmes impliqués dans l'échange des clés, le chiffrement et la signature des données ainsi que la taille des clés mises en œuvre se référer au document [SPEC_CRYPTO].

- Epinglage du certificat TLS de la plateforme

  L'application e-CPS embarque l'empreinte SHA256 du certificat serveur de la plateforme et la vérifie dans le cadre de l'établissement du canal TLS (*certificate pinning*). Cela permet d'authentifier la plateforme avec laquelle elle communique.

- Seconde session TLS avec authentification mutuelle

  Une fois la phase de pré-authentification réussie, la clé de chiffrement du conteneur récupérée et le conteneur déchiffré, une seconde session TLS avec authentification mutuelle est établit entre l'application et la plateforme. Le serveur est authentifié par l'empreinte de son certificat stockée sur l'ordiphone, tandis que l'ordiphone est authentifié avec sa bi-clé stockée dans le conteneur (p12 : clé privée et certificat).

  L'authentification de l'utilisateur via son certificat est effectuée par la plateforme et non par la cible.

- FS2. Protection des données du conteneur

- Confidentialité

  Le conteneur est chiffré, avec l'algorithme AES-256-CBC, afin d'assurer la confidentialité des données s'y trouvant. Le conteneur et les éléments qu'il contient sont générés par la plateforme. Le chiffrement du conteneur est également effectué par la plateforme, il est transmis chiffré à l'application.

- Intégrité

  L'intégrité du conteneur, et donc des éléments qu'il contient, est garantie par une empreinte SHA256. L'empreinte n'est pas stockée sur l'ordiphone de l'utilisateur, mais calculée dynamiquement puis envoyée au serveur lors de la vérification du code PIN. Le serveur vérifie que l'empreinte correspond à celle qu'il a calculé et sauvegardé lors de la création du conteneur pendant le processus d'inscription. Si l'empreinte envoyée au serveur ne correspond pas à celle attendue, les données de l'utilisateur sont supprimées du téléphone.

- FS3. Protection des données persistantes (empreinte du certificat de la plateforme compris)

- Confidentialité et intégrité

  Afin de réussir une authentification, l'application à besoin de certaines données. Ces données sont stockées sur l'ordiphone et sont protégées en confidentialité et en intégrité. L'application nécessite pour son fonctionnement la présence d'un *Keystore*. C'est le *Keystore* de l'ordiphone qui se chargera de protéger en intégrité et en confidentialité les données persistantes. L'application interagit directement avec les fonctionnalités de sécurité propre au système d'exploitation, pour générer les clés de chiffrement et stocker de manière sécurisée ces informations.

- Obfuscation de code

  - Sous Android, la majorité du code de l'application est obfusqué. Seules certaines des bibliothèques externes (Retrofit, Glide, EventBus) et les chaines de caractères "utilisées à l'extérieur" (constantes nécessaires aux requêtes HTTP telles que les URL et les noms des paramètres) ne sont pas obfusquées.

  Cela permet de minimiser les attaques s'appuyant sur la rétro-ingénierie logicielle.

- FS4. Mécanisme d'authentification robuste

- Anti-clonage

  La protection contre le clonage s'appuie sur la vérification d'une empreinte liée à l'ordiphone et à l'instance de l'application (phoneId). Elle reste inchangée durant toute la durée de vie de l'application. Lors de l'inscription, l'empreinte est transmise au serveur, qui l'associe au compte utilisateur.

  A chaque authentification, le serveur va comparer cette empreinte avec l'empreinte reçue durant l'envoi du code PIN pour vérification. Si une différence est détectée, toutes les informations de l'utilisateur sont détruites, et son application est remise à zéro à la prochaine ouverture.

  De plus, lorsqu'un téléphone est associé à une identité, il n'est pas possible d'en associer un autre, il faut désactiver l'association précédente pour associer un nouveau téléphone. La désactivation de l'association entraîne la suppression du conteneur par l'application du téléphone dissocié.

  Également, si le conteneur et les données persistantes sont copiées sur un autre téléphone, l'application ne reconnait pas le conteneur.

- Pré-authentification

  Durant le processus d'authentification, une pré-authentification est réalisée avant que la clé du conteneur ne soit transmise et que l'utilisateur soit authentifié grâce à son certificat. Cette pré-authentification correspond à la vérification par le serveur, des éléments listés ci-dessous et transmis par l'application.

  - Le PIN, connu uniquement de l'utilisateur ;
  - l'identifiant de l'utilisateur ;
  - l'empreinte du conteneur, propre au conteneur ;
  - l'empreinte de l'ordiphone, propre à l'ordiphone et à l'instance de l'application (phoneId).

  Si un seul de ces éléments n'est pas correct la requête échoue.

- Authentification par mot de passe à usage unique (HOTP)

  Durant la phase d'authentification un défi est réalisé, il s'agit d'une authentification par HOTP. Un compteur partagé par l'application et la plateforme est synchronisé lors de la phase d'inscription, il est échangé en même temps que la clé HOTP utilisée elle aussi dans cet algorithme. Le compteur est incrémenté à chaque appel d'authentification lorsque l'algorithme est utilisé. Si le compteur est désynchronisé, toutes les données de l'application sont supprimées. La fenêtre de validation du serveur est nulle.

  De plus, l'empreinte de l'ordiphone (phoneId) et l'identifiant de notification sont comparés aux données possédées par le serveur. L'identifiant utilisateur est également comparé aux données d'identification présentes dans le certificat du conteneur, transmis préalablement pour l'établissement du TLS avec authentification mutuelle.

  Tous ces éléments doivent être corrects pour que l'authentification de l'utilisateur soit validée.

- FS5. Gestion du PIN

- Clavier PIN sécurisé

  Le clavier PIN sécurisé assure la sécurité des entrées de données. Les mécanismes en place permettent d'atténuer les risques liés aux enregistreurs de frappe, aux captures d'écran et aux attaques par-dessus l'épaule (*shoulder surfing*).

- Echecs limités

  Un compteur limite le nombre de tentatives infructueuses d'authentification afin de se protéger contre les attaques par force brute. Le code PIN est associé à un compteur de tentatives défini à 3 qui est décrémenté à chaque échec d'authentification.

III.6. MATRICE DE COUVERTURE.

	VOL_PIN **-M1**	VOL_LOCAL **-M2**	MODIF_LOCAL **-M3**	VOL_TRANSIT **-M4**	MODIF_TRANSIT **-M5**	BYPASS_AUTH **-M6**	CLONE **-M7**
- FS1 Protection des communications	✓			✓	✓		
- FS2 Protection des données du conteneur		✓	✓				✓
- FS3 Protection des données persistantes		✓	✓				✓
- FS4 Mécanisme d'authentification robuste			✓		✓	✓	✓
- FS5 Gestion du PIN	✓		✓				

Tableau 3 - Matrices des fonctions de sécurité en fonction des menaces