PUBLIC

Cible de sécurité

mAccess app pour Android

IDENTIFICATION DU DOCUMENT	
Référence:	CSPN_Cible de sécurité_mAccess pour Android
Date de création:	Janvier 2022
Auteurs:	CDU
Classification:	PUBLIC

VERSION			
Version	**Date**	**Description - modification**	**Auteur**
1.0	03/12/2021	Version initiale	CDU
1.1	03/03/2022	Clarification des fonctions de sécurité et des hypothèses d'environnement	CDU

1.2	04/11/2022	Clarification sur la génération de l'OTP offline	CDU
1.3	13/04/2023	Précisions sur le format du code secret et la liste des librairies intégrées	CDU

Table des matières

1. Introduction

a. Objet du document

Ce document constitue la cible de sécurité pour l'application mobile «mAccess app pour Android » développée par inWebo technologies en vue d'une Certification de Sécurité de Premier Niveau (CSPN) par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Le terme TOE (Target Of Evaluation) sera utilisé dans la suite du document pour désigner l'application mobile candidate à la certification CSPN.

b. Identification du module évalué

Le module candidat à l'évaluation est l'application mobile «mAccess app pour Android » développé par inWebo technologies.

Identification du module

Organisation éditrice	InWebo Technologies
Lien vers l'organisation	https://www.inwebo.com/
Lien vers le produit	https://www.myinwebo.com/welcome
Catégorie de produit	Identification, authentification et contrôle d'accès
Nom commercial du module	mAccess app pour Android
Numéro de version évaluée	3.1

c. Document de référence

Document d'architecture de la solution	https://inwebo.atlassian.net/wiki/spaces/DOCS/overview **https://inwebo.atlassian.net/wiki/spaces/DOCS/pages/1688024/User+guide+mAccess+token+software+SDK**
Guide d'intégration	

Spécifications des mécanismes cryptographiques	20221104_Specifications_Crypto_mAccess_Android_inWebo technologies_v1.4.docx

d. Vocabulaire

Activation	Processus durant lequel l'association est faite entre un identifiant unique d'une personne physique et ses moyens d'authentification (smartphone + code secret)
Admin Console	Console d'administration d'un tenant, permettant à des administrateurs du tenant de le configurer, gérer les utilisateurs, définir les politiques de sécurité, etc.
Authentification offline	Opération d'authentification réalisée quand le device ne peut pas se connecter à un canal de communication sans fil (e.g mode avion, problème réseau…). Les échanges entre le secure device et le serveur sont donc impossibles.
Authentification online	Opération d'authentification réalisée quand le secure device peut se connecter à un canal de communication sans fil. Les échanges entre le secure device et le serveur sont donc possibles.
Code d'activation	Code aléatoire permettant d'activer un Secure Device et de lier le moyen d'authentification à son porteur. Le code d'activation est composé de 9 ou de 20 caractères. La durée de vie de ce code est relative à sa longueur; 15 minutes pour un code d'activation sur 9 caractères et 21 jours pour un code d'activation sur 20 caractères.
Code Secret	Facteur "ce que je sais" du MFA. Il s'agit d'un code PIN.
Connecteur	Objet technique permettant de connecter une application tierce à la plateforme d'authentification d'inWebo en définissant les caractéristiques de connexion et la politique d'accès à appliquer.
Partner Console	Console de gestion permettant à inWebo de définir des offres, et de gérer la relation entre offre, tenant, clients.
OTP	One Time Password généré selon le protocole breveté inWebo, tronqué pour permettre la ressaisie manuelle (généralement sur 6 digits). La durée de vie de cet OTP est limitée à 30 secondes.
Scellement	Opération d'authentification dont la preuve d'exécution lie fortement le contexte de l'opération à sa validation.
Secure Device	Facteur "ce que je possède" du MFA. Il s'agit d'un dispositif personnel comme un smartphone par exemple.
Serveur	Applicatif back-end produit déployé sur un serveur intégrant la validation des OTP, la base de données et le HSM.

Service	Instance du produit pour le client
Utilisateur	Personne physique souhaitant s'authentifier fortement pour accéder à des services et détentrice du dispositif personnel de type smartphone.

e. Abréviations

2FA	2 Factor Authentication
3DS	Protocole 3-D Secure ajoutant une validation supplémentaire hors bande lors des paiements sur internet.
DSP2	Directive sur les Services de Paiements 2 éditée par l'EBA (European Bank Authority)
HSM	Hardware Security Module
IHM	Interface Homme Machine
MFA	Multi Factor Authentication
OS	Operating System
OTP	One Time Password
PAM	Privileged Account Management
SaaS	Software As a Service
SDK	Software Development Kit
SE	Secure Element
SSO	Single Sign On
TEE	Trusted Execution Environment
TOE	Target Of Evaluation
VPN	Virtual Private Network

2FA	2 Factor Authentication
3DS	Protocole 3-D Secure ajoutant une validation supplémentaire hors bande lors des paiements sur internet.
DSP2	Directive sur les Services de Paiements 2 éditée par l'EBA (European Bank Authority)
HSM	Hardware Security Module
IHM	Interface Homme Machine
WIFI	Wireless Fidelity

2. Argumentaire du produit

a. Description générale

inWebo MFA est une plateforme logicielle opérée en mode Software As A Service permettant à un utilisateur de s'authentifier à des services tiers en ligne au travers d'une application mAccess app pour Android, installée sur son smartphone par exemple, et s'interfaçant avec le Serveur.

La plateforme met à disposition de l'intégrateur sous forme d'API sécurisées ou directement via des applications légères les fonctions :

- d'administration du service (gestion des différentes politiques de sécurité, gestion des utilisateurs et de groupes, gestion des moyens d'authentification, gestion des connecteurs et contrôles d'accès)
- de support (gestion des cas de blocage des moyens d'authentification, des utilisateurs ou de la plateforme de manière générale)
- de selfcare à la main de l'utilisateur (ajout d'un moyen d'authentification additionnel, modification du code secret, génération d'un OTP offline)
- d'initiation d'opérations d'activation, d'authentification ou de scellement

La solution inWebo MFA est composée de 2 composants principaux :

- mAccess est un module logiciel, fourni aux développeurs d'applications mobile ou intégré dans l'application inWebo, assurant les fonctions de génération de clés, de génération d'OTP à partir du code secret, du secure device et d'éléments aléatoires pour les fonctions d'authentification.

- Le composant serveur comprend une base de données, un HSM embarquant un microcode exécutant la fonction d'authentification et un serveur d'application offrant des interfaces – notamment API Web Services – permettant l'intégration de la solution dans l'environnement d'utilisation chez l'organisation cliente de la solution. Une console web permet l'administration fonctionnelle de l'instance du composant serveur de l'organisation cliente. La console est une application web dont l'accès est protégé par authentification forte par le composant serveur, aucun accès direct à la base données n'est possible. Toutes les opérations sur l'instance – notamment les opérations d'administration - sont journalisées. Le journal (dit « audit trail ») peut être accédé via API ; des rapports peuvent être créés et exportés depuis la console web. Le schéma ci-dessous fournit une vue simplifiée de l'architecture.

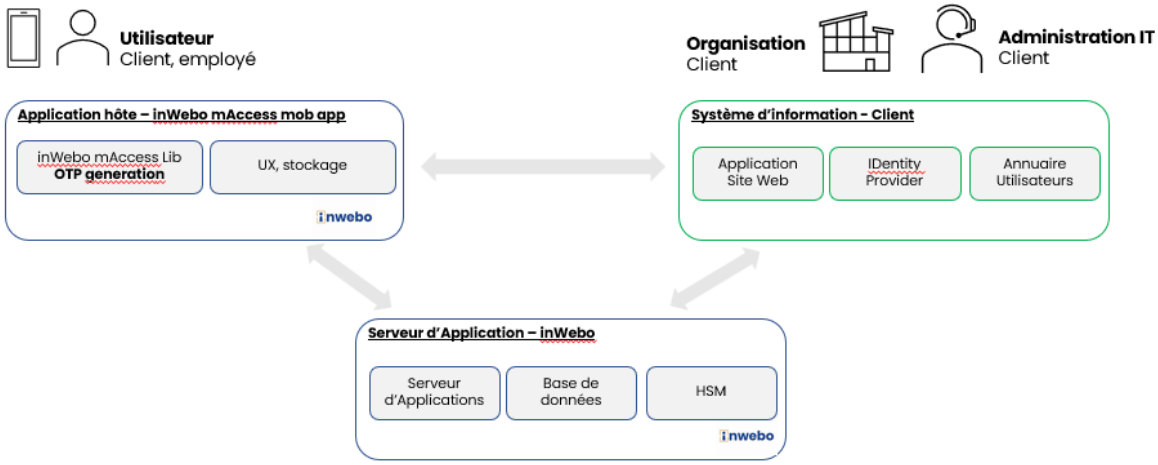

Figure 1- Architecture simplifiée

La librairie inWebo mAccess fournit au développeur les fonctions nécessaires à l'activation du moyen d'authentification, à sa gestion (notamment, déblocage, changement du PIN) et, bien sûr, à l'authentification de l'utilisateur. inWebo mAccess implémente plusieurs algorithmes d'authentification :

- Un protocole d'authentification multi-facteurs, dit « R0-R1-R2 ». Ce protocole est utilisé pour l'authentification de l'utilisateur au composant serveur de la solution préalablement à toute opération connectée nécessitant de garantir l'authenticité du demandeur (synchronisation du moyen d'authentification, ajout de moyen d'authentification au compte de l'utilisateur, génération d'OTP, changement de PIN). Le composant serveur vérifie indépendamment et successivement la détention de facteurs d'authentification statiques liés à l'application mobile (réponse « R0 »), la détention de facteurs d'authentification dynamiques liés à l'application mobile (réponse « R1 »), et lorsqu'il en a défini un, la connaissance par l'utilisateur du second facteur (code secret) (réponse « R2 »)

- Deux algorithmes de génération d'OTP dits respectivement « online » et « offline ». Le second ne nécessite pas de connectivité internet du moyen d'authentification mais est de ce fait sujet à désynchronisation. Le composant serveur implémente les

algorithmes de vérification d'OTP correspondants. L'organisation cliente n'a pas besoin de connaître lequel de ces algorithmes de génération est effectivement mis en œuvre, c'est entièrement transparent. La mise en œuvre du protocole R0-R1-R2 et des algorithmes online et offline pour le support des modes d'utilisation de la solution est expliquée dans la suite de ce document.

inWebo mAccess est une librairie purement « calculatoire » c'est-à-dire qu'elle n'implémente ni n'utilise directement les fonctions de la plate-forme mobile telles que le stockage, les IHM ou les communications. Dans le cas où l'intégrateur n'utilise pas l'application inWebo, il doit mettre en œuvre ces fonctions. Le site développeur inWebo[1] fournit une documentation développeur pour l'intégration de la librairie.

b. Utilisation du produit

i. Acteurs

- **Les rôles à privilèges**
    - **L'Administrateur du service :** l'administrateur du service (personne physique) a la charge de gérer les utilisateurs,, les connecteurs et la définition des accès conditionnels.
    - **Le Manager d'un groupe d'utilisateurs :** afin de répondre à des besoins d'organisation, l'administrateur du service peut déléguer ses droits pour un groupe d'utilisateurs donné au Manager d'un groupe d'utilisateurs (personne physique). Le Manager du groupe a la charge de gérer les utilisateurs et leurs moyens d'authentification au sein du groupe défini.
- **L'utilisateur :** il s'agit d'une personne physique utilisant la Librairie mAccess, embarquée dans une application mobile, pour générer un code à usage unique sur saisie de son Code Secret pour s'authentifier à un service tiers ou valider une opération.
- **Le fournisseur de service tiers :** il s'agit de l'organisation liée au tenant souhaitant protéger des ressources ou des opérations par authentification forte via l'intégration de la solution inWebo MFA dans son système d'information. Il est à l'origine des demandes d'activation et d'authentification.

[1] http://developer.inwebo.com

ii. Activation du 2FA

L'association entre une identité et ses facteurs d'authentification (secure device (possession) et code secret (savoir)) s'effectue lors de la phase d'activation d'un utilisateur.

La figure suivante illustre le processus d'activation implémenté dans inWebo MFA :

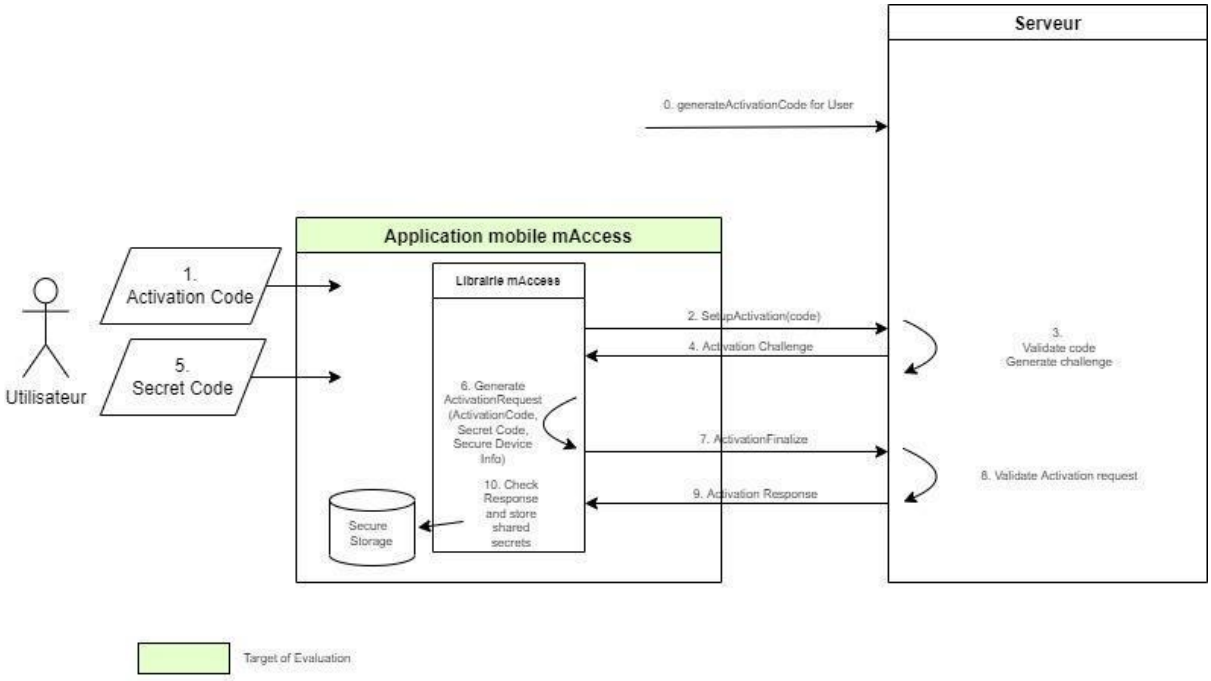

Figure 2- Processus d'activation

Le composant serveur émet (génération par le HSM) un code d'activation à usage unique pour chaque profil utilisateur ou moyen d'authentification créé. L'organisation cliente peut choisir l'émission d'un code court (9 chiffres en base 10, valide 15 minutes) ou d'un code long (20 chiffres en base 10, valide 3 semaines) selon ses procédures de mise à disposition et en particulier la durée de validité nécessaire, ou selon le fait que l'utilisateur doive ou non saisir le code manuellement.

L'utilisateur reçoit via un canal dédié son code d'activation. La mise à disposition s'achève par une phase dite d'activation d'un moyen d'authentification lorsque le code d'activation est saisi par l'utilisateur ou directement fourni à mAccess via l'application mobile, puis envoyé au composant serveur par mAccess (1,2,3,4).

L'utilisateur définit un second facteur (5).

Après la fourniture du code d'activation et la définition (ou la vérification) du second facteur, mAccess et le composant serveur se synchronisent et s'échangent les facteurs d'authentification de l'utilisateur (6,7,8,9,10). Le code d'activation est la seule donnée permettant l'authentification de l'utilisateur lors d'une mise à disposition, c'est pour cela qu'il est important que l'organisation cliente choisisse un procédé de distribution du code d'activation qui soit adapté au niveau de risque d'usurpation d'identité qu'elle tolère lors de la mise à disposition.

iii. Authentification à un service tiers

Quand l'utilisateur a activé son / ses moyens d'authentification, il est en capacité de les utiliser pour accéder aux applications de ses fournisseurs de service.

Authentification online

La figure suivante décrit le processus d'authentification Online.

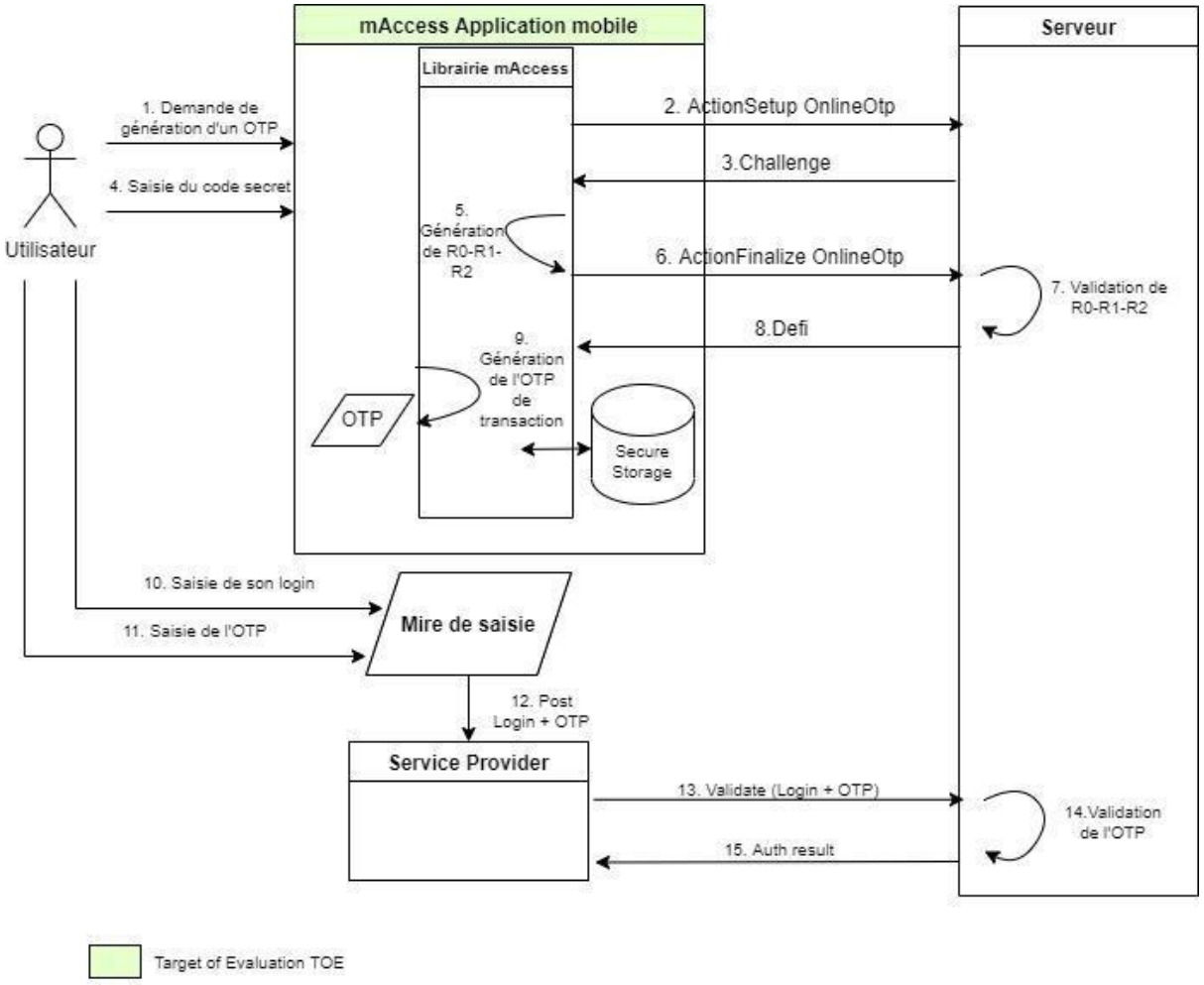

Figure 3- Processus d'authentification online

L'application mobile ne gère pas les notifications. Dans ce mode, l'utilisateur doit obtenir un OTP et le ressaisir pour accéder au service ou à l'accès distant. Pour cela, il lance l'application mobile, sélectionne le compte auquel il souhaite accéder (celui correspondant au service ou à l'accès distant de l'organisation cliente) et se voit présenter une demande de consentement (par exemple saisie d'un PIN, « swipe », clic de confirmation, utilisation du capteur d'empreinte, etc.) qu'il choisit d'accepter ou de rejeter (1,2,3).

Après que l'utilisateur a fourni son consentement, l'application mobile mAccess app appelle localement la fonction d'authentification en fournissant les données nécessaires pour l'exécution de cette fonction. inWebo mAccess met en œuvre un algorithme de génération d'OTP. Le calcul de l'OTP est réalisé localement par l'algorithme de génération d'OTP online après la mise en œuvre du protocole R0-R1-R2 entre mAccess app et le composant serveur (5,6,7,8).

L'OTP est fourni en retour à l'application mobile, pour affichage à l'utilisateur (9).

L'utilisateur le saisit dans un formulaire d'authentification (10,11). Cet OTP n'est pas interprété par le serveur de l'organisation cliente, il est fourni au composant serveur pour vérification (12). Le composant serveur détient un challenge créé pour l'utilisateur après l'authentification par le protocole R0-R1-R2 (13,14,15).

Authentification offline

La figure suivante décrit le processus d'authentification offline. Dans ce cas, le Secure Device de l'utilisateur est déconnecté et n'a pas accès au réseau. Ce mode correspond à un usage ponctuel pour pallier au manque temporaire de connectivité. L'utilisateur va donc générer un OTP sur son Secure Device qui sera validé par le serveur.

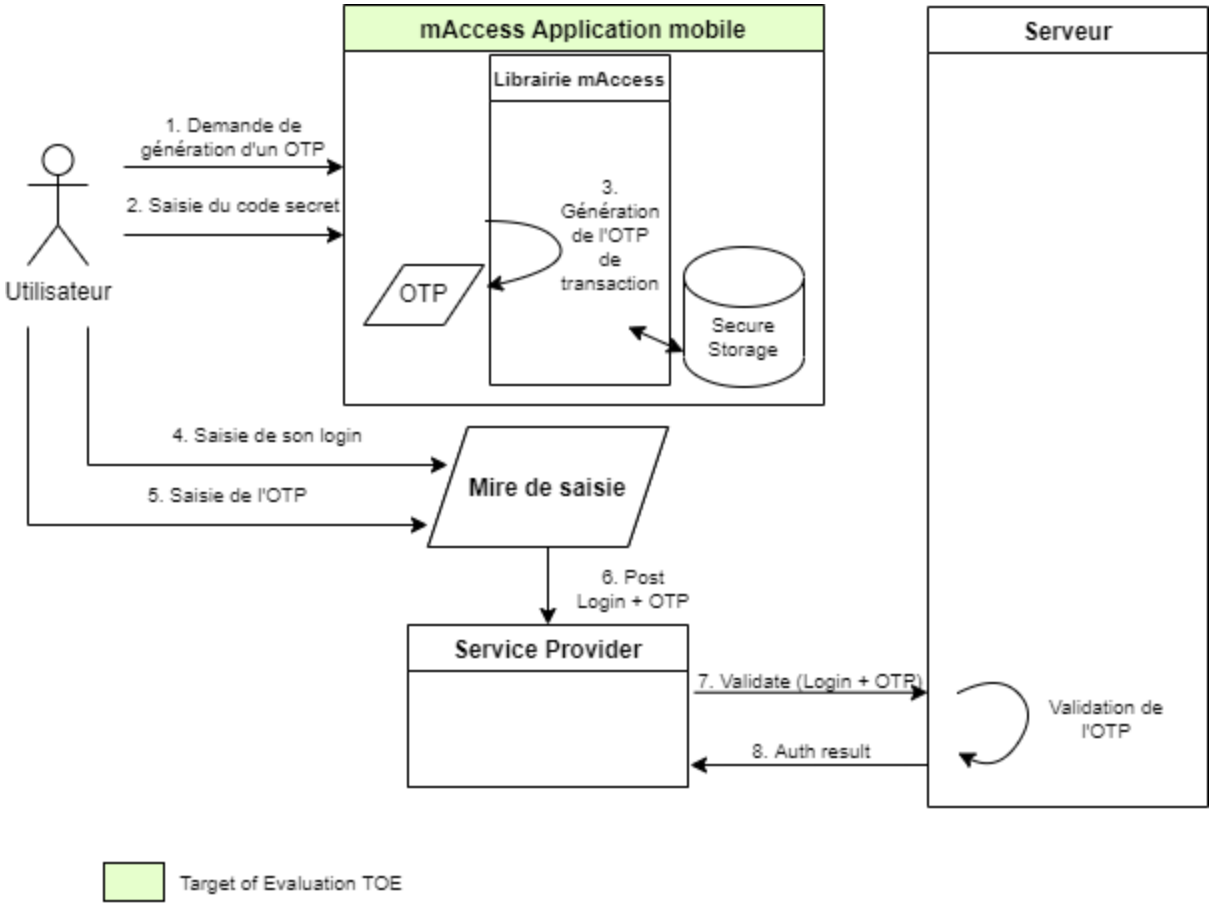

Figure 4- Processus d'authentification offline

Dans ce mode offline, l'utilisateur doit obtenir un OTP et le ressaisir pour accéder au service ou à l'accès distant. Pour cela, il lance l'application mobile, sélectionne le compte auquel il souhaite accéder (celui correspondant au service ou à l'accès distant de l'organisation cliente) et saisit son code secret. La saisie d'un code secret est nécessaire mais la vérification sera réalisée côté serveur, à la validation de l'OTP.

Après que l'utilisateur ait saisi son code secret, l'application mobile mAccess app appelle localement la fonction d'authentification en fournissant les données nécessaires pour

l'exécution de cette fonction. inWebo mAccess met en œuvre un algorithme de génération d'OTP offline pour calculer localement l'OTP, sans échange avec le composant serveur (3).

L'OTP est fourni en retour à l'application mobile mAccess app, pour affichage à l'utilisateur.

L'utilisateur le saisit dans un formulaire d'authentification (4,5). Cet OTP n'est pas interprété par le serveur de l'organisation cliente, il est fourni au composant serveur pour vérification (6). Le composant serveur fait l'hypothèse que l'algorithme offline a été mis en œuvre et il tente de valider l'OTP avec cet algorithme (7,8).

iv. Modification du code secret

Lorsque l'utilisateur doit ou souhaite modifier son code secret, il peut le faire via son Secure Device.

Il lui est alors demandé de saisir le code secret courant avant de saisir le nouveau et de le confirmer.

v. Reset du code secret

Lorsque l'utilisateur a bloqué son code secret ou a oublié sa valeur, il peut recevoir un code de déblocage sous la forme d'un code d'activation. Il peut alors choisir une nouvelle valeur pour son code secret.

c. Environnement d'utilisation

L'application mAccess app pour Android fait partie de la solution inWebo MFA intégrant également une partie serveur portant la fonction de validation d'OTP, de support, d'audit, de configuration et de gestion des connecteurs. L'application mobile mAccess app n'est donc pas autonome dans la fonction d'authentification d'un utilisateur.

La solution inWebo MFA est disponible en SaaS et permet de sécuriser les accès aux applications déployées par les entreprises pour des besoins internes (VPN, SSO…) ou des besoins externes (3DS, DSP2…)

d. Dépendances

L' application mobile mAccess app possède les dépendances logicielles & matérielles sur:

- android 12 API Level 31
- iwlib-mac (librairie interne) : 3.4.0
- androidx.appcompat:appcompat : 1.4.2
- com.google.android.material:material : 1.6.1
- google conscrypt-android : 2.5.2
- tink open-source crypto library 1.7.0 (https://developers.google.com/tink)
- Platform-bom 2.0.5

- fest-assert 1.4
- fest-reflect 1.4.1
- biometric 1.1.0
- firebase-messaging 23.0.7
- firebase-inappmessaging 20.1.2
- firebase-inappmessaging-display 20.1.2
- lifecycle-viewmodel 2.5.0
- junit 4.13.2

e. Périmètre d'évaluation

Le périmètre d'évaluation est limité au composant en bleu sur le schéma suivant:

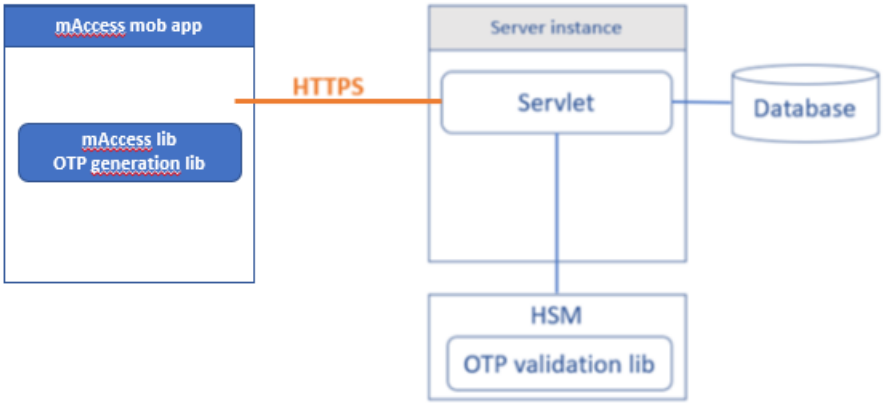

Figure 3- Périmètre d'évaluation

Le périmètre de l'évaluation est restreint à l'application mobile mAccess app pour Android pour isoler au mieux les fonctions de sécurité et s'assurer du niveau de sécurité d'un composant déployé dans un environnement tiers.

Il est à noter que, côté serveur, un HSM exécute le microcode inWebo implémentant la partie serveur des algorithmes d'authentification. La gestion de clés de cet HSM permet de restreindre l'usage de certaines clés au seul microcode inWebo et exige l'authentification d'un quorum d'officiers de sécurité pour toute modification. Les facteurs d'authentification liés à l'application mobile sont des informations arbitraires générées aléatoirement par le HSM.

3. Environnement technique

a. Matériel compatible et dédié

L'application doit être installée à partir du magasin d'application officiel Play Store sur un équipement physique de type smartphone ou tablette sur lequel le système d'exploitation

Android est installé. L'équipement doit être relié à Internet soit par le réseau mobile (3G, 4G) soit par WIFI.

Hors périmètre TOE :

Le modèle du HSM est Utimaco CryptoServer LAN Se1500 V5

Certifications :
• FIPS 140-2 Level 3*
• CE, FCC Class B
• UL, IEC/EN 60950-1
• CB certificate
• RoHS II, WEEE

b. Système d'exploitation

L'application mobile mAccess app a été développée pour être compatible avec les versions Android 8 et supérieures.

c. Environnement d'évaluation

Le produit est évalué sur des terminaux ayant une version 12 d'Android installée.

d. Description des hypothèses de l'environnement

Les hypothèses suivantes sont retenues pour l'évaluation du produit :

- **[HE1_USER_SEC]** L'utilisateur est de confiance :
  - Il ne partage pas son Code Secret et s'assure de la confidentialité de sa saisie à chaque usage
  - Il définit un Code Secret robuste selon les règles demandées et décrites dans le guide de configuration disponible sur le site développeur d'inWebo[2].
- **[HE2_DEV_SEC]** L'équipement mobile d'exécution est de confiance :
  - Le système d'exploitation de son équipement est à jour des derniers correctifs de sécurité
  - Le système Android installé est fourni par le constructeur et n'est pas personnalisé, le bootloader de l'appareil est verrouillé.
  - Il n'est pas rooté et le mode développeur est désactivé.
  - Aucun programme malveillant n'est installé sur son équipement
  - Le magasin de certificats est de confiance. Les certificats des autorités racines sont reconnues par les développeurs des systèmes d'exploitation mobiles.
  - Il embarque un TEE (Trusted Execution Environment) ou un SE (Secure Enclave).
  - L'appareil est compatible FCM (Firebase Cloud Messaging).

[2] http://developer.inwebo.com

- **[HE3_DEV_SEC]** L'application mobile est développée selon l'état de l'art et les bonnes pratiques reprises dans le guide d'intégration disponible sur le site développeur d'inWebo[2].

- **[HE4_SP_SEC]** Les fournisseurs de service sont de confiance :
  - Ils envoient des requêtes d'authentification intègres et légitimes.
  - Ils provisionnent des utilisateurs (personnes physiques) dont l'identité a été vérifiée au préalable.
  - Ils s'assurent de la distribution sécurisée (canaux séparés) du code d'activation.

- **[HE5_SRV_SEC]** Le serveur inWebo MFA est de confiance :
  - Il est développé et installé selon les règles de l'art de la sécurité
  - Il est configuré selon les recommandations retenues pour l'évaluation (configuration des algorithmes cryptographiques, politiques de sécurité, configuration base de données, configuration HSM…)
  - Il est opéré selon les guides de sécurité et d'administration disponibles sur le site développeur d'inWebo[2]
  - Il utilise le HSM pour générer les clés, les secrets et les challenges nécessaires à la génération de l'OTP et à la protection en intégrité et confidentialité des échanges.

4. Description des biens sensibles

Les biens sensibles à protéger sont les éléments permettant de générer ou de récupérer des codes d'authentification OTP à l'insu de l'utilisateur et donc de valider des opérations illégitimes.

- **[BS1] Le Code Secret**
  Le code secret de l'utilisateur est saisi à chaque authentification. Il n'est pas stocké sur l'équipement mobile de l'utilisateur, il déclenche la génération de l'OTP à usage unique.
  Le code secret doit être protégé en confidentialité. Il doit de plus être protégé en authenticité et en intégrité lors d'une mise à disposition.

- **[BS2] La clé statique K0**
  La clé statique K0 est liée à l'instance de la Librairie mAccess et est échangée lors de l'activation du secure device. Elle intervient dans la génération de l'OTP online.
  Elle doit être protégée en confidentialité. Elle doit de plus être protégée en authenticité et en intégrité lors d'une mise à disposition et en authenticité dans le stockage.

- **[BS3] La clé dynamique K1**
  La clé dynamique K1 est liée à l'instance de la Librairie mAccess et est renouvelée à chaque demande d'authentification. Elle intervient dans la génération de l'OTP online.
  Elle doit être protégée en confidentialité. Elle doit de plus être protégée en authenticité et en intégrité lors d'une mise à disposition et en authenticité dans le stockage.

- **[BS4] Les données d'authentification**
  Les données d'authentification nécessaires à la génération de l'OTP et échangées entre le serveur et l'application mobile.
  Elle doivent être protégées en confidentialité et intégrité lors de leur transmission au composant serveur. Elles doivent être non-prédictibles, non-rejouables et exclusives.

- **[BS5] Le code d'activation**
  Le code d'activation permet à l'utilisateur de lier ses facteurs d'authentification à son identité. Le code d'activation couvre également le cas de blocage du code secret.
  Il doit être protégé en confidentialité et intégrité lors de leur fourniture au composant serveur. Il doit être non-prédictible et non-rejouable.

- **[BS6] L'OTP**
  L'OTP permet de valider la demande d'authentification par recueil du consentement de l'utilisateur (saisie du code secret). Son interception pourrait permettre d'accéder à la ressource visée.
  Il doit être protégé en confidentialité et intégrité lors de sa fourniture au composant serveur. Il doit être non-prédictible, non-rejouable et exclusif au client.

5. Description des menaces

Les menaces considérées sont les suivantes :

- **[M1] Vol du code d'activation**

  Description de la menace :
  L'attaquant dérobe le code d'activation avant que celui-ci ne parvienne à l'utilisateur légitime ou après saisie par espionnage des communications entre l'application mobile et le Serveur.
  Biens sensibles impactés : [BS5]
  Profil attaquant : Attaquant malveillant externe

- **[M2] Vol du code secret**

  Description de la menace :
  L'attaquant dérobe le code secret de l'utilisateur par n'importe quel moyen ou technique : attaque par ingénierie sociale, observation de la saisie du code secret sur l'application, attaque par brute force pour deviner la valeur du code secret…
  Biens sensibles impactés : [BS1]
  Profil attaquant : Attaquant malveillant externe

- **[M3] Vol de l'équipement mobile**

  Description de la menace :
  L'attaquant dérobe l'équipement mobile sur lequel la Librairie mAccess a été activée.
  Biens sensibles impactés : [BS1], [BS2], [BS3]
  Profil attaquant : Attaquant malveillant externe

- **[M4] Accès à la mémoire de l'équipement mobile lors des opérations**

  Description de la menace :
  L'attaquant est en possession de l'équipement mobile sur lequel la librairie est instanciée et activée. Il parvient à accéder aux secrets stockés dans la mémoire de l'équipement (accès au code source, mémoire volatile, mémoire persistante)
  Biens sensibles impactés : [BS2], [BS3], [BS6]
  Profil attaquant : Attaquant malveillant avec accès à l'équipement mobile

- **[M5] Demande d'authentification frauduleuse**

  Description de la menace :
  Un attaquant se connectant à l'application du fournisseur de service entre l'identifiant de connexion de l'utilisateur. L'utilisateur valide l'opération via acceptation de la notification sans vérification du contexte.
  Biens sensibles impactés : Aucun
  Profil attaquant : Attaquant malveillant externe

- **[M6] Capture et rejeu de trames réseau**

  Description de la menace :
  Un attaquant capture et analyse les trames réseaux échangés entre le client et le serveur lors d'une authentification légitime. Il tente alors de rejouer les trames avec ou sans modification afin de tromper le serveur.
  Biens sensibles impactés : [BS1],[BS2],[BS3], [BS4],[BS5], [BS6]
  Profil attaquant : Attaquant malveillant externe avec accès actif au réseau

- **[M7] Usurpation du serveur**

  Description de la menace :
  Un attaquant redirige les flux de l'équipement de l'utilisateur et tente de se faire passer pour le serveur inWebo MFA afin de récupérer les références de l'utilisateur.
  Biens sensibles impactés : [BS1],[BS2],[BS3], [BS4],],[BS5], [BS6]
  Profil attaquant : Attaquant malveillant externe avec accès actif au réseau

6. Description des fonctions de sécurité

- **[FS1] Gestion du code d'activation**

  Le code d'activation est à usage unique et à une durée de vie limitée dans le temps.
  Les codes d'activation sont générés de façon aléatoire via la routine de génération d'aléas du HSM piloté par le composant serveur. Il vérifie que chaque code d'activation nouvellement créé est unique parmi tous les codes en cours de validité.
  Le composant serveur vérifie également que la proportion de codes d'activation en

cours de validité dans chaque classe (codes de longueur 9 ou 20 chiffres) demeure sous un seuil lié à la durée de validité associée à cette classe.
Lors de la phase d'activation (fin de la mise à disposition), le composant serveur vérifie que le code obtenu est toujours en cours de validité et l'invalide.
Les codes d'activation sont ainsi non-prédictibles (ni par calcul, ni par essai multiple) et non-rejouables.

- **[FS2] Gestion du code secret**

  A la mise à disposition, le format et la longueur du code secret sont imposés à l'utilisateur par la politique de sécurité. La vérification de ces contraintes est directement faite dans le HSM du composant serveur. Les combinaisons triviales sont rejetées (redondance des mêmes chiffres).

  A l'authentification, le code secret n'est vérifié par le composant serveur dans une information d'authentification que si le facteur possession est correct. De plus, le composant serveur bloque le code secret dans le profil de l'utilisateur dès que le compteur d'essais est atteint, 4 essais sont autorisés, afin d'éviter toute attaque par force brute.

  Le code secret n'est jamais stocké sur le téléphone (facteur possession) et la mémoire est systématiquement écrasée après chaque calcul.

  En cas de suspicion de compromission du code secret, l'utilisateur a la capacité de procéder à :
    - La modification de son code secret : il devra alors définir un nouveau code secret après avoir démontré la connaissance du code secret courant par saisie,
    - La réinitialisation de son code secret : un code de déblocage ayant les mêmes propriétés que le code d'activation lui sera fourni par des canaux dédiés et sécurisés après vérification de l'identité du demandeur. A la différence de la mise à disposition, le facteur possession est déjà enregistré et peut être vérifié,
    - Le blocage temporaire ou définitif de son dispositif à partir de celui-ci ou via un administrateur.

- **[FS3] Gestion du stockage des clés et secrets**

  Les clés et secrets nécessaires à la génération des OTP ou à la mise en place d'une communication sécurisée avec le serveur sont stockés avec les attributs et propriétés nécessaires selon les hypothèses [HE2_DEV_SEC] et [HE3_DEV_SEC]. Ces hypothèses sont vérifiées et le niveau jugé adéquat.
  Par ailleurs, les facteurs d'authentification liés à l'application mobile sont chiffrés avec une clé dérivée du code secret. Ils sont donc protégés en confidentialité.

  Le protocole d'authentification R0-R1-R2 et l'algorithme de génération d'OTP offline utilisent une information d'identification de l'équipement où est installée l'application

mobile. Cette information a été mesurée et fournie au composant serveur lors de la mise à disposition. Lors de l'authentification, quel que soit le mode mis en œuvre, le composant serveur est ainsi capable de détecter la copie des facteurs d'authentification sur un autre équipement et de bloquer le moyen d'authentification dans le profil de l'utilisateur. Par ailleurs, les facteurs d'authentification dynamiques liés à l'application mobile étant mis à jour de façon aléatoire lors de chaque requête où ils sont mis en œuvre, les facteurs dynamiques de l'application mobile et ceux de sa(ses) copie(s) ne peuvent être identiques. Lorsqu'il examine une requête d'authentification, le composant serveur bloque dans le profil de l'utilisateur une application mobile qui n'a pas les valeurs de facteurs dynamiques auxquelles il s'attend.
Les facteurs d'authentification liés à l'application mobile sont ainsi protégés en authenticité.

- **[FS4] Génération de l'OTP**

Les opérations cryptographiques réalisées par la Librairie mAccess sont implémentées au sein d'un composant dédié selon [HE2_DEV_SEC] complexifiant les attaques en mémoire. Les clés et les résultats de calculs intermédiaires sont immédiatement effacés de la mémoire après utilisation.

mAccess et le composant serveur mettent en œuvre les mesures suivantes :
- Le calcul des OTP online, des OTP offline comme des informations R0-R1-R2 par mAccess met en œuvre un diversifiant aléatoire dont le rejeu est contrôlé par le serveur,
- L'authentification est multi-facteurs quel que soit le mode mis en œuvre :
    - Un OTP offline est calculé et vérifié comme une fonction non-inversible d'un diversifiant aléatoire, de certains facteurs d'authentification liés à l'application mobile et du code secret
    - Les informations R0 et R1 sont calculées et vérifiées comme des fonctions non-inversibles d'un diversifiant aléatoire et de certains facteurs d'authentification liés à l'application mobile ; l'information R2 est en plus calculée et vérifiée comme une fonction du code secret
    - Un OTP online est calculé et vérifié comme une fonction non-inversible d'un diversifiant aléatoire et de certains facteurs d'authentification liés à l'application mobile. Ce diversifiant aléatoire n'étant émis par le serveur que si l'authentification R0-R1-R2 a préalablement réussi, l'authentification à l'aide d'OTP online est donc bien multi-facteurs
- Les facteurs d'authentification liés à l'application mobile sont des informations arbitraires générées aléatoirement par le HSM. Cela représente plusieurs centaines de bits d'information, il est donc quasiment impossible que deux utilisateurs aient les mêmes facteurs d'authentification à un moment donné. Il est également quasiment impossible que le moyen mAccess de deux utilisateurs n'ayant pas les mêmes facteurs d'authentification liés à l'application mobile puisse calculer des informations d'authentification identiques (OTP online, OTP offline ou informations R0-R1-R2) à partir du même diversifiant aléatoire. Enfin, pour les mêmes raisons, des informations

d'authentification valides pour une organisation cliente A ne le seront pas pour une organisation cliente B quand bien même un utilisateur aurait des profils d'authentification pour ces deux organisations,
- La durée de validité des OTP est très limitée. Lorsque le diversifiant aléatoire est généré par le composant serveur (OTP online, informations R0-R1-R2), un délai de validité lui est associé dans le composant serveur. Lorsque le diversifiant aléatoire est fourni par mAccess (OTP offline), le calcul de l'OTP inclut des éléments permettant au composant serveur de détecter lors de la vérification si l'OTP offline est correct mais n'est plus valide,
- Dans le mode OTP offline, le composant serveur limite le nombre de tentatives d'authentification liées à un profil un utilisateur par unité de temps
- Le calcul des informations d'authentification par mAccess utilise des facteurs d'authentification statiques et dynamiques liés à l'application mobile. Pour éviter la désynchronisation de ces facteurs dynamiques, ils ne sont mis à jour dans le profil de l'utilisateur lors de la vérification d'une information d'authentification par le composant serveur qu'après vérification que le facteur Possession (valeurs statiques et dynamiques) est correct,
- Le code secret (facteur Connaissance) n'est vérifié par le composant serveur dans une information d'authentification que si le facteur Possession est correct. De plus, le composant serveur bloque le code secret dans le profil de l'utilisateur si le nombre d'essais infructueux atteint la limite définie.

Ainsi, l'OTP est non-prédictible (ni par calcul, ni par essai multiple), non-rejouable et exclusif. Il ne peut pas être désynchronisé par un attaquant externe et ne peut pas être attaqué par force brute.

- **[FS5] Gestion de la confidentialité et de l'intégrité des échanges**

  L'application mAccess communique avec le serveur inWebo MFA à travers un canal sécurisé TLS avec authentification du serveur. Le certificat présenté par le serveur doit être signé par une autorité de certification reconnue. De plus, l'empreinte du certificat présenté par le serveur doit correspondre à celle attendue par l'application cliente.

  Lors de la phase d'activation (fin de la mise à disposition), l'application mobile transmet au composant serveur plusieurs informations – dont un « nonce » et le code secret - chiffrées par clé publique. En retour, lorsque le composant serveur fournit à l'application mobile les facteurs d'authentification liés à l'application mobile, il doit inclure ce nonce chiffré par une clé dérivée. Si la clé publique n'a pas été altérée préalablement à la mise à disposition ([HE2_DEV_SEC]), mAccess peut s'assurer que les informations échangées avec le composant serveur lors de la mise à disposition n'ont pas été interceptées ni modifiées.

  Une fois activée, mAccess s'authentifie sur l'API du composant serveur lors de toutes les requêtes qu'elle effectue. Le protocole R0-R1-R2 est mis en œuvre.

7. Couverture des menaces

	[M1] Vol du code d'activation	[M2] Vol du code secret	[M3] Vol de l'équipement mobile	[M4] Accès à la mémoire de l'équipement mobile lors des opérations	[M5] Demande d'authentification frauduleuse	[M6] Capture et rejeu de trames réseau	[M7] Usurpation du serveur
[FS1] Gestion du code d'activation	X						
[FS2] Gestion du code secret		X	X				
[FS3] Gestion du stockage des clés et secrets		X	X	X	X	X	X
[FS4] Génération de l'OTP			X	X	X		X
[FS5] Gestion de la confidentialité et de l'intégrité des échanges					X	X	X

Figure 5- Couverture des menaces