SOGETI ITSEF

24, rue du Gouverneur Général Eboué
92136 Issy-les-Moulineaux

Tél. :+33(0)1.55.00.13.02
Fax: +33(0)1.55.00.12.30

Cible de sécurité CSPN

EZIO Mobile SDK

pour iOS

VALIDITE DU DOCUMENT

Identification		
Client	**Project**	**Provider**
GEMALTO	CSPN ST - EZIO Mobile Protector SDK 3.2.1 RMW 7 pour iOS	SOGETI – ITSEF

Modification		
Date	Version	Évolutions
21/05/2015	1.0	Première version
29/06/2016	2.0	SDK version 3.2.1 RMW 7 incluant trois nouvelles librairies de Gemalto.
19/08/2016	2.1	Précisions sur le « Password Manager » et le service interne « Property Persitent Storage ».
19/08/2016	2.1-LIGHT	Version allégée de la cible de sécurité pour publication et traduction en français.

SOMMAIRE

1 IDENTIFICATION DU PRODUIT

Organisation	Gemalto
Site web de l'organisation	http://www.gemalto.com
Nom du produit	EZIO Mobile Protector SDK pour iOS
Version du produit évalué	3.2.1 RMW 7
Catégorie du produit	Identification, authentification et contrôle d'accès ; Stockage Sécurisé

2 ARGUMENTAIRE DU PRODUIT

2.1 DESCRIPTION GENERALE DU PRODUIT

« EZIO Mobile SDK » est une solution de génération de mots de passe à usage unique (« One Time Password », OTP), de stockage sécurisé et d'échange de messages par canaux séparés (« Out-Of-Band », OOB). La solution est composée d'une bibliothèque de développement « EZIO Mobile SDK » pour application mobile ainsi que de composants serveurs « EZIO Mobile EPS » (« Enrollment and Provisionning Server », EPS) et « EZIO Mobile OOBS » (« Out-Of-Band Server », OOBS). La solution permet le développement d'application avec une authentification forte pour les utilisateurs mobiles.

La bibliothèque « EZIO Mobile SDK » fournit aux développeurs d'application mobile une couche d'abstraction pour des fonctions de sécurités liées à l'authentification et à la signature. Cette bibliothèque leur met à disposition des mécanismes de mise à disposition et de stockage des clés secrètes utilisées pour générer des OTP. La librairie met également à disposition un service d'échanges de messages et vérification de transaction ainsi qu'un mécanisme de stockage sécurisé.

Le serveur « EZIO Mobile EPS » prend en charge des serveurs d'authentification externe et s'intègre avec des CRM pour répondre à de multiple cas d'usage.

La solution EZIO Mobile supporte les protocoles de génération CAP, OATH, Gemalto OATH et « Dynamic Signature » (un algorithme propriétaire à Gemalto).

L'application d'authentification forte permet de générer un OTP, en utilisant la bibliothèque « EZIO Mobile SDK », à la demande de l'utilisateur. L'utilisateur est typiquement un client d'un service à distance pour lequel l'authentification doit être réalisée de manière fiable et rapide.

La bibliothèque « EZIO Mobile SDK » est disponible pour les téléphones mobiles utilisant iOS ou Android. Pour iOS, la bibliothèque est écrite en Objective-C et en C.

La génération d'OTP est initiée par la saisie d'un PIN ou l'utilisation du « touchID » par l'utilisateur afin de permettre l'accès à la clé secrète de l'utilisateur. La protection de cette clé est réalisée par la bibliothèque.

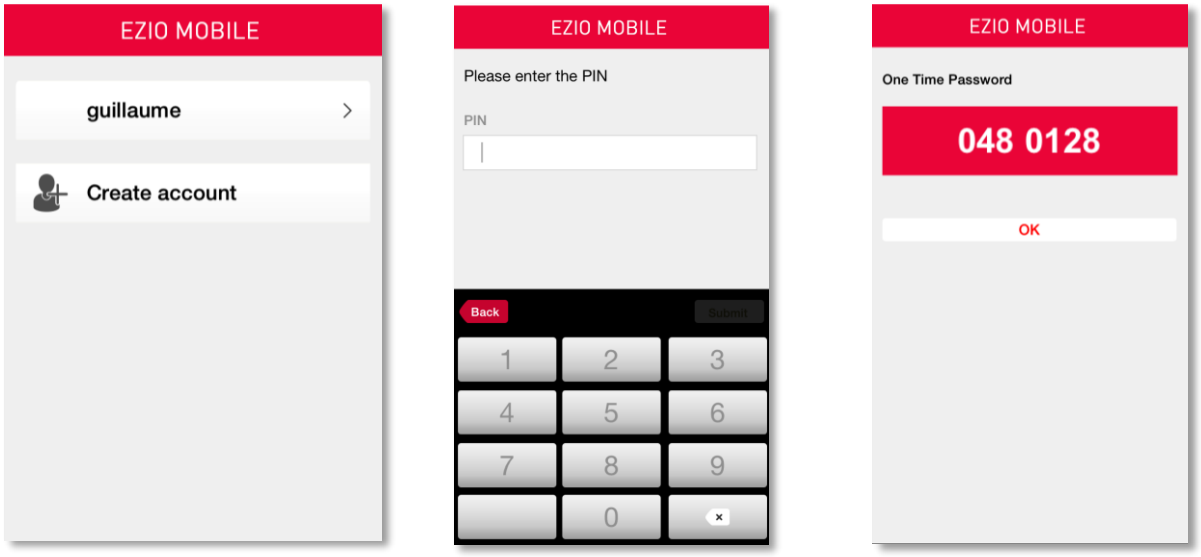
Une fois la clé secrète accessible, l'OTP est généré à partir de cette dernière suivant la méthode d'authentification OATH (HTOP, TOTP ou OCRA) ou CAP. La cible d'évaluation ne prend en compte que la méthode OATH et le Stockage Sécurisé, le service d'échange de messages par séparation de canaux n'est pas dans le périmètre de cette évaluation.

2.2 DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT

2.2.1 Mot de passe à usage unique (« OTP »)

Le client télécharge l'application d'authentification forte, développée avec la bibliothèque « EZIO Mobile SDK », à partir de l'Apple Store, puis accède au service de génération d'OTP avec les informations d'identification transmises par le service à distance via un autre canal (courrier).

Le client sélectionne son compte (1), saisi son PIN (2) et obtient un OTP (3) pour utiliser le service à distance comme l'illustre la figure suivante.



(1) Compte utilisateur

(2) Saisie du Pin (représenté ci-dessus) ou authentification par empreinte digitale

(3) affichage de l'OTP

Figure 1 – étapes de génération d'un mot de passe à usage unique

2.2.2 Stockage sécurisé

« EZIO Mobile SDK » fourni un service de Stockage Sécurisé pour enregistrer de façon persistante des données fournies par l'application. Le SDK assure la sécurité des données enregistrées. Les données sont représentées par des couples clé-valeurs. Le service de Stockage Sécurisé supporte la création de plusieurs instances de stockage, identifiées de manière unique par un identifiant choisi par l'application. Chaque instance de stockage peut sauvegarder un nombre quelconque de couples clé-valeur.

Le service de Stockage Sécurisé est protégé par une clé de domaine, elle-même sous la protection du « Password Manager ».

Les figures suivantes représentent les deux modes d'utilisation du « Password Manager » actuellement supportés par la bibliothèque: le mode simplifié et le mode avancé. Chaque boîte bleue représente une instance du « Property Persistent Storage », utilisé en interne pour l'enregistrement sécurisé des clés.

- Pour le mode simplifié, l'application ne peut utiliser qu'un seul mot de passe qui permet d'ouvrir les différents domaines (Stockage Sécurisé et Communication par canaux séparés).

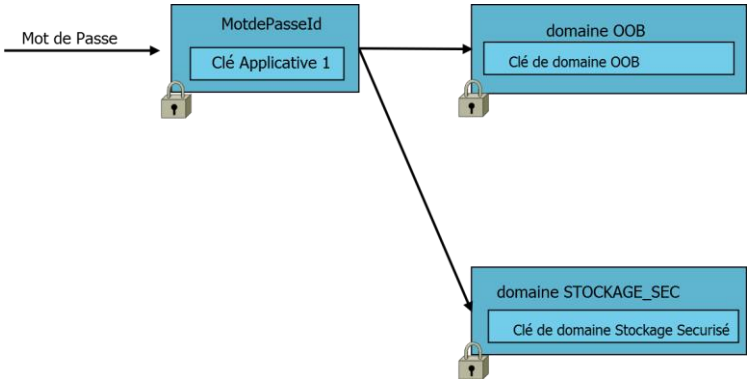


Figure 2 – Architecture du mode simplifié

- Pour le mode avancé, l'application peut configurer le « Password Manager » pour lier les domaines à des mots de passe différents.

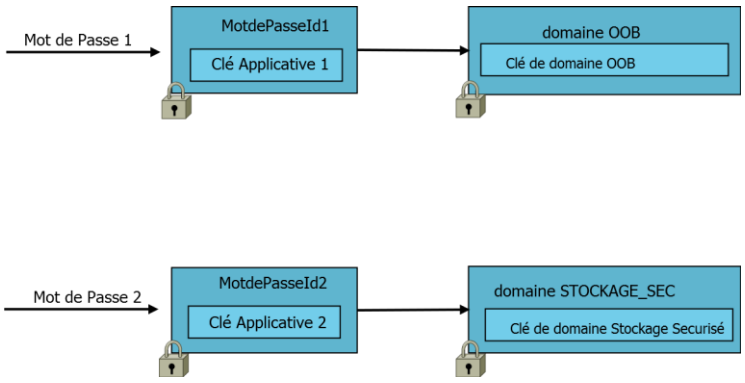


Figure 3 – Architecture du mode avancé avec deux mots de passe

Le « Password Manager » peut également gérer la clé de domaine pour la communication par canaux séparés, cette fonctionnalité est en dehors du périmètre d'évaluation.

2.3 DESCRIPTION DE L'ENVIRONNEMENT PREVU POUR L'UTILISATION DU PRODUIT

La solution « EZIO Mobile » permet de mettre en œuvre un contrôle d'accès à des services fournis à distance. La Figure 4 illustre les composants essentiels de la solution et les interactions principales entre eux.

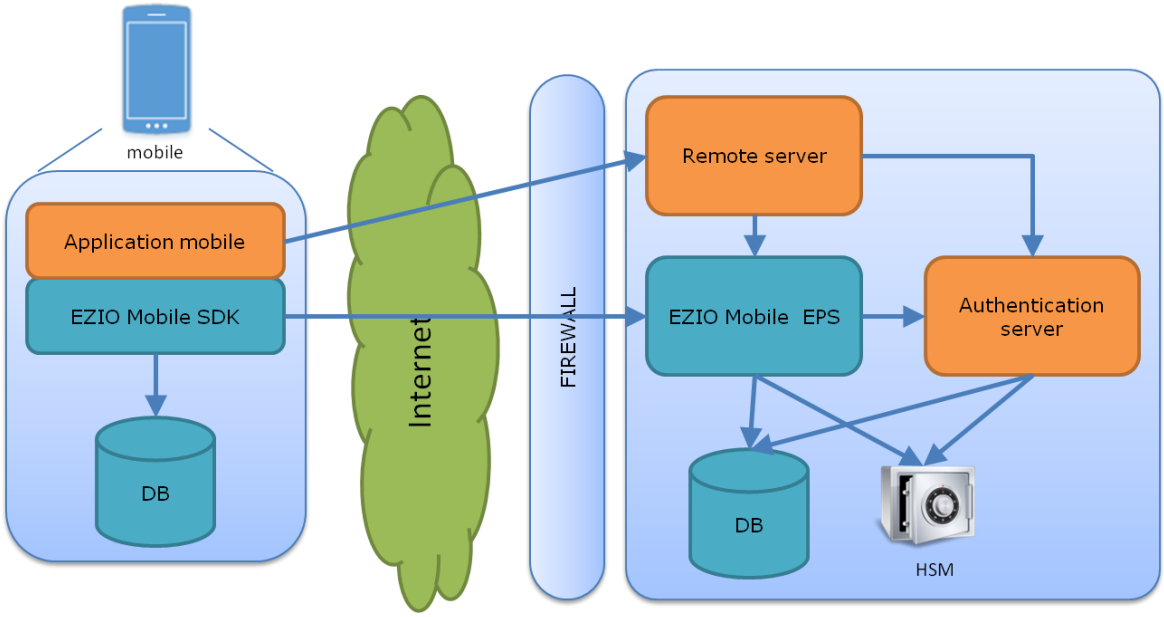


Figure 4 – Aperçu de la solution EZIO Mobile

L'environnement d'utilisation principal concerne des services de paiements à distance pour des banques ou des commerces en ligne pour lesquels l'utilisateur est mobile. La solution est également destinée à être utiliser pour authentifier les utilisateurs d'une entreprise.

Lorsqu'une authentification est requise par l'un de ces cas d'usage, l'OTP généré par l'utilisateur sur l'application mobile est saisi dans une interface lié au serveur distant, par exemple dans un formulaire en ligne ou dans une application tierce.

À la réception de l'OTP de l'utilisateur, le service distant vérifie l'OTP à partir du serveur d'authentification lié au serveur « EZIO Mobile EPS ».

2.4 DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

HM1 : le système d'exploitation de l'équipement mobile est à jour et dispose des derniers correctifs de sécurité publiés.

HM2 : l'utilisateur n'enregistre nulle part son code PIN dans l'équipement mobile ni ne le communique à des tiers. Le code PIN n'est pas utilisé pour un autre usage sur le serveur EZIO.

HM3 : l'utilisateur n'installe pas d'application malveillante sur l'équipement mobile et autorise les connexions réseaux vers des services externes que pour des applications de confiance.

HM4 : l'équipement mobile sur lequel est exécutée l'application d'authentification forte développée à partir de la bibliothèque « EZIO Mobile SDK » doit disposer de moyens de communication réseaux permettant d'atteindre le serveur EPS du service à distance. En particulier l'utilisateur doit disposer d'un accès de type « donnée » dans le cas d'une connexion réseau à partir d'une carte SIM de l'équipement mobile.

HM5 : le service à distance doit disposer d'un serveur EPS opérationnel et présumé de confiance. L'utilisation du service à distance par un client mobile doit permettre d'associer l'OTP avec le profil utilisateur correspondant déclaré dans le serveur d'authentification.

2.5 DESCRIPTION DES DEPENDANCES

L'application d'authentification forte développée à partir de la bibliothèque « EZIO Mobile SDK » n'a pas de dépendance matérielle ou logicielle.

Cependant l'authentification de l'utilisateur par empreinte digitale biométrique n'est possible uniquement lorsque l'application est installée sur une plate-forme qui le supporte (« touchID » d'Apple).

2.6 DESCRIPTION DES UTILISATEURS ET ROLES TYPIQUES

UM1 : l'utilisateur final accède sur son téléphone mobile à l'application d'authentification forte développée à partir de la bibliothèque « EZIO Mobile SDK ». Il n'est pas considéré malveillant ni excessivement négligent (HM1, HM2 et HM3).

2.7 DESCRIPTION DU PERIMETRE D'EVALUATION DU PRODUIT

Les éléments suivants sont considérés dans le périmètre d'évaluation de l'application d'authentification forte développée à partir de la bibliothèque « EZIO Mobile SDK » :

- Calcul des Mots de Passe à usage unique (« OTP ») OATH (OCRA inclus) ;
- Inscription des graines OATH à partir du serveur EPS ;
- Stockage des graines OATH sur l'équipement ;
- Utilisation du « PinPad » sécurisé pour l'entrée du PIN ou utilisation du lecteur d'empreinte digitale pour l'authentification de l'utilisateur ;
- Le service de Stockage Sécurisé ;
- Le « Password Manager »;
- Le service interne de « Property Persistent Storage ».

Les éléments suivants ne sont pas à considérer dans le périmètre d'évaluation :

- Le calcul des Mots de Passe à usage unique (« OTP ») et l'inscription des graines du serveur pour le standard CAP ;
- L'algorithme propriétaire de Gemalto « Dynamic Signature » ;
- Inscription des graines sans serveur EPS et la migration des graines depuis une version d' « EZIO Mobile SDK » de la branche 1.x ;
- La vérification des Mots de Passe à usage unique de type « VIC »;
- L'inscription des doubles graines pour OATH;
- Le service de Communication par Canaux Séparés (« OOB »);
- Le mécanisme de détection de plate-forme « Jailbreak ».

3 DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

3.1 MATERIEL COMPATIBLE OU DEDIE

L'environnement technique pour le fonctionnement de l'application d'authentification forte, développée à partir de la bibliothèque « EZIO Mobile SDK », nécessite un équipement physique (téléphone ou tablette) capable de supporter un environnement d'exécution d'application mobile et disposant d'interfaces de communication réseau IP (via carte SIM supportant les échanges de données ou par WIFI).

3.2 SYSTEME D'EXPLOITATION RETENU

L'exécution de l'application d'authentification développée à partir de la bibliothèque « EZIO Mobile SDK » version 3.2.1 RMW 7 pour iOS nécessite un équipement disposant du système d'exploitation iOS entre les versions 7.0 et 9.x et une architecture CPU ARM Cortex-A8, ARM Cortex-A9, ARMv7 ou ARMv8-A 64-bit.

4 DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Les biens sensibles à protéger sont ceux impliqués dans l'authentification de l'utilisateur (PIN et/ou empreinte digitale), la clé secrète générée par le serveur « EZIO Mobile EPS » et attribuée à un utilisateur donné et les données protégées par le service de Stockage Sécurisé. Lors de la mise à disposition de la clé secrète sur l'équipement mobile, d'autres clés sont également utilisées.

Les biens sensibles suivants sont identifiés pour le périmètre concernant la génération des Mots de Passe à usage unique (« OTP ») :

B1: PIN et/ou empreinte digitale utilisée à travers le « touchID », volatile et unique à chaque service.

B2: la clé secrète stockée sur l'équipement. Donnée persistante et unique à chaque service.

B4: la clé maîtresse stockée sur l'équipement mobile par les mécanismes de la plate-forme. Donnée persistante et unique pour chaque instance de l'application.

B5: la clé de stockage, volatile.

B6: la clé d'environnement, volatile et unique pour chaque service.

B7: la clé de « wrapping » stockée sur l'équipement. Donnée persistante protégée par un des mécanismes d'authentification (PIN ou authentification biométrique).

B8: la clé de protection dérivée du PIN. Donnée volatile et unique pour chaque PIN.

B9: la clé de protection prise en charge par les mécanismes de la plate-forme contrôlés par l'authentification biométrique. Donnée persistante.

L'OTP généré est un bien sensible du point de vue du mécanisme d'authentification recherché par l'utilisation de l'application développée à partir de la bibliothèque « EZIO Mobile SDK ». En revanche les conditions d'utilisation de l'application sur l'équipement mobile implique d'afficher en clair l'OTP sur l'écran pendant une période de temps donnée. De ce fait l'application ne doit pas protéger l'OTP en particulier mais bien tous les éléments nécessaires à sa génération.

Les biens sensibles suivants sont identifiés pour les périmètres du Stockage Sécurisé et le « Password Manager » :

B10: la clé de domaine pour le Stockage Sécurisé.

- Ce bien sensible est stocké sur l'équipement mobile, pris en charge par le « Password Manager » et protégé par le service interne de « Property Persistent Storage ». Ce service interne utilise une clé applicative (B21).

- Ce bien sensible est utilisé par le Stockage Sécurisé comme une donnée volatile fournie par le « Password Manager » pour permettre l'ouverture du « Property Persistent Storage » interne.

Les biens sensibles suivants sont identifiés pour le périmètre de Stockage Sécurisé :

B17: les données fournies par l'application à la bibliothèque « EZIO Mobile SDK » pour leur protection.

B18: les données stockées par le service de Stockage Sécurisé.

Les biens sensibles suivants sont identifiés pour le périmètre du « Password Manager » :

B20: un mot de passe. Ce bien est volatile et peut être fourni par l'application pour permettre l'ouverture une instance du service de « Property Persistent Storage » utilisé en interne par le « Password Manager ».

B21: les clés d'application. Ces biens (un seul pour le « Password Manager » en mode simplifié ou plusieurs, au choix pour l'application, pour le mode d'utilisation avancé) sont stockés sur l'équipement mobile, protégés par le « Property Persistent Storage » qui utilise le ou les mots de passe fournis (B20).

Les biens sensibles suivants sont identifiés pour le périmètre du « Property Persistent Storage » :

B30: un mot de passe ou une clé (le « Property Persistent Storage » utilise un tableau de d'octets en entrée et donc accepte les deux). Ce bien est volatile.

B31: la clé volatile, dérivée du mot de passe ou de la clé (B30), utilisée pour protéger la clé maîtresse de la couche 1 de sécurité.

B32: la clé maîtresse persistante de la couche 1, stockée dans l'équipement et protégée par B31.

B33: la clé volatile de confidentialité de la couche 1, dérivée de B32.

B34: la clé volatile d'authentification de la couche 1, dérivée de B32.

B35: la clé volatile de chiffrement de la couche 2, dérivée d'informations provenant de l'équipement et permettant la mise en œuvre d'un service d'anti-copie.

B36: la clé volatile de chiffrement de la couche 3, dérivée d'informations provenant de l'application.

B37: les données stockées de manière sécurisées par le « Property Persistent Storage ».

Le service de « Property Persistent Storage » est utilisé par le service de Stockage Sécurisé offert à l'application et par le « Password Manager ».

5 DESCRIPTION DES MENACES

Le modèle de sécurité de la solution EZIO Mobile a été établi à partir des vecteurs d'attaques suivants :

- Pendant la transmission de la clé secrète sur l'équipement mobile à partir du serveur EPS ;
- Attaque sur la clé secrète stockée sur l'équipement mobile (attaque hors ligne) ;
- Attaque sur les données protégées par le service de Stockage Sécurisé sur l'équipement (attaque hors ligne) ;
- Attaque sur les clés protégées par le « Password Manager » ;
- Attaque pendant les opérations cryptographiques.

Les scénarios d'attaques suivants ont été identifiés

- M1 : équipement volé ;
- M2 : code PIN et/ou empreinte et/ou mot de passe volé ;
- M3 : interception pendant la mise à disposition de la clé secrète ;
- M4 : « reverse engineering » de l'application ;
- M5 : clone de la clé secrète ;
- M6 : accès au PIN ou au mot de passe ou à la clé secrète en clair en temps réel pendant les opérations cryptographiques ;
- M7 : attaque par force brute sur la clé secrète ;
- M8 : attaque par force brute sur la clé maîtresse.

Le profil de l'attaquant retenu pour l'application d'authentification, développé à partir de la bibliothèque « EZIO Mobile SDK », est un attaquant qui :

- essaie de générer un OTP en lieu et place de l'utilisateur légitime en utilisant les menaces : M1, M2, M3, M4, M5, M6 et M7.

- essaie d'accéder aux données stockées dans le service de Stockage Sécurisé en utilisant les menaces: M1, M2, M4, M6, and M8.

6 DESCRIPTION DES FONCTIONS DE SECURITE

6.1 GESTION DU PIN

6.1.1 Pin Pad sécurisé

Le Pin Pad Sécurisé est un composant visuel qui fournit des services de sécurité pour l'entrée de PIN. L'objectif du Pin Pad Sécurisé est d'assurer que la gestion et la manipulation du PIN sont effectuées de manière sécurisée, contrôlée et vérifiée. Il assure qu'un minimum de protections est en place contre les enregistreurs de frappe, l'espionnage de l'écran, les copies de mémoire et les captures d'écran. Le Pin Pad Sécurisé participe à la protection de la solution globale contre des attaques ciblées.

Le service Pin Pad Sécurisé utilise en interne une bibliothèque produite par Gemalto pour la gestion du composant visuel. Différents éléments du Pin Pad Sécurisé peuvent être configurés à l'initialisation ou par le bais d'interfaces offertes par la bibliothèque « EZIO Mobile SDK ». Une fois le PIN saisi, le Pin Pad Sécurisé génère un objet « Pin Sécurisé » qui peut être utilisé par la suite dans les processus de changement de PIN ou de calculs d'OTP.

6.1.2 Blocage du Pin

La clé secrète est chiffrée avec le code PIN et/ou le « touchID » sur l'équipement mobile. L'application ne peut pas influencer ce principe qui est fondamental. La sécurité de la solution repose sur la propriété qu'un mauvais code PIN doit générer un mauvais OTP qui est indiscernable d'un correct.

L'attaquant ne peut valider un OTP sans le soumettre au serveur pour vérification. Ce dernier limite le nombre d'OTP incorrect et bloque le compte si nécessaire.

6.1.3 Changement du Pin

Le code PIN peut être changé dans l'application d'authentification forte développée à partir de la bibliothèque « EZIO Mobile SDK ». Cette opération implique la modification de la couche de chiffrement de la clé secrète en utilisant le nouveau code PIN.

6.2 PROTECTION EN CONFIDENTIALITE DE LA CLE SECRETE PENDANT LA MISE A DISPOSITION

La mise à disposition de la clé secrète sur l'équipement mobile à partir du serveur EPS implique les étapes suivantes qui protègent la clé secrète pendant toutes les phases de l'échange :

1) L'application mobile est démarrée et détecte que la clé secrète est manquante. Ceci déclenche un formulaire pour que l'utilisateur saisisse son code d'enregistrement et déclenche une session avec la bibliothèque « Ezio Mobile SDK ».

2) La bibliothèque « EZIO Mobile SDK » authentifie l'EPS et envoi de manière sécurisé les éléments d'identification et de protection à l'EPS.

3) Coté serveur EPS, le module de sécurité déchiffre la requête et identifie la clef secrète grâce aux informations transmises par la bibliothèque.

4) Coté server EPS, le module de sécurité protège la clef secrète en confidentialité et authentifie la réponse.

5) Le server EPS envoie la réponse à la bibliothèque « EZIO Mobile SDK ».

6) Le SDK vérifie que la réponse est authentique, récupère la clef secrète puis applique les schémas de protection propres à l'équipement mobile.

La confidentialité de la clé secrète est assurée pendant toute les étapes car la clé est protégée par le PIN et n'est jamais manipulée en clair.

La bibliothèque « EZIO Mobile SDK » rejette toutes les communications en clair, les certificats auto-signés, les mauvaises adresses de serveur (par rapport au certificat) et accepte uniquement le certificat du serveur si celui-ci est signé par une autorité reconnue fiable par l'équipement mobile. Ces vérifications de sécurité ne peuvent pas être désactivées.

6.3 PROTECTION EN CONFIDENTIALITE DES CLES STOCKEES

6.3.1 Protection de la clé secrète de calcul d'« OTP »

La protection en confidentialité des clés stockées sur l'équipement mobile suit les principes suivant :

1) La clé secrète est envoyée à l'équipement déjà chiffrée avec le code PIN. Sans le code PIN, un attaquant qui intercepte la clé ne peut pas la lire.

2) La clé secrète chiffrée est de nouveau chiffrée avec une clé d'environnement.

3) La clé secrète doublement chiffrée est de nouveau avec une clef protégée par les services du système.

4) L'ensemble des données est protégée nativement par les mécanismes d'isolation du système d'exploitation qui empêche une application d'accéder aux données d'une autre application.

6.3.2 Modes d'authentification multiple

La bibliothèque « EZIO Mobile SDK » fournissent plusieurs moyens d'authentifier l'utilisateur avant l'accès aux biens nécessaires aux calculs d'OTP. À un instant donné, un mode d'authentification peut être actif ou non (mis à part le mode PIN qui est toujours actif).

« EZIO Mobile SDK » supporte deux services pour authentifier l'utilisateur:

- Avec un Pin que l'utilisateur connait ;
- Avec une empreinte biométrique que l'utilisateur possède.

Le mode d'authentification identifie le service et l'entrée d'authentification transporte la valeur nécessaire à l'authentification. Les différents modes d'authentification peuvent être utilisés indépendamment les uns des autres.

Les représentations des clés de calculs d'OTP doivent être mise à jour afin de supporter le mode d'authentification multiple. La mise à jour permet à une représentation compatible uniquement avec un PIN à être transformée pour supporter plusieurs types. Cette mise à jour n'est pas réversible, une fois appliquée il n'est pas possible de désactiver le support de plusieurs moyens d'authentification.

Après la mise à jour, toute opération qui nécessitait un accès à la représentation de la clé, comme la génération d'OTP, peut utiliser chacun des modes d'authentification actifs.

6.4 PROTECTION EN CONFIDENTIALITE DES CLES PENDANT LE CALCUL DE L'« OTP »

Le calcul d'un OTP requiert des secrets qui proviennent de 3 environnements différents :

- Le système d'exploitation.
- L'environnement d'exécution.
- Le secret de l'utilisateur:
    - Le Pin
    - L'empreinte digitale.

Une fois la clé secrète accessible en mémoire, la génération de l'OTP est réalisée.

En cas de vol de l'équipement (M1) et sans le code PIN, l'attaque n'est pas réalisable par force brute (M7) de la clé secrète dans un temps raisonnable. L'attaque sur le code PIN n'est pas réalisable du fait de l'absence de conditions d'arrêt et de la validation côté serveur.

En cas de code PIN volé (M2) et sans accès à l'équipement, l'attaque n'est pas faisable du fait de la validation côté serveur.

En cas d'interception de la clé secrète pendant la mise à disposition (M3), i.e connaitre la clé secrète mais pas le PIN, l'attaque n'est pas faisable pour distinguer un PIN valide du fait de l'absence de condition d'arrêt.

En cas d'accès à l'équipement avec reverse engineering (M4) de l'application, l'attaque ne permet pas l'accès au code PIN. Le reverse engineering est rendu plus difficile du fait de l'utilisation de techniques d'« obfuscation » pour les applications sous Android et de l'utilisation de code C avec des drapeaux spécifiques lors de la compilation pour les applications sous iOS.

En cas de copie de l'application (M5) sur un autre équipement et sans le code PIN, l'attaque n'est pas faisable dans un temps raisonnable et du fait de la validation côté serveur.

En cas d'accès au code PIN ou à la clé secrète en temps réel pendant les opérations cryptographiques (M6), l'attaque est difficile et requiert un téléphone « jailbreaké » avec une application malveillante dédiée tandis que les données sensibles sont effacées après utilisation. La détection d'un environnement « jailbreaké » rend également plus difficile l'attaque.

6.5 PROTECTION EN INTEGRITE DES BIENS SENSIBLES

Les biens sensibles en relation avec les calculs d'OTP n'ont pas de protection en intégrité dédiés par construction. En effet, suivant le principe fondamental, utilisé par la solution « EZIO Mobile », qui veut qu'un mauvais OTP ne puisse être distingué d'un OTP correct, les biens sensibles peuvent être altérés par un attaquant sans que le modèle de sécurité ne soit remis en question. Ainsi, un attaquant n'est pas en mesure d'obtenir un secret (clé secrète ou PIN) ou de générer une des clés en altérant les biens sensibles.

Les biens sensibles pris en charge par le Stockage Sécurisé sont protégés en intégrité.

6.6 PROTECTION EN CONFIDENTIALITE DES CLES PRISES EN CHARGE PAR LE « PASSWORD MANAGER » ET LE STOCKAGE SECURISE

Les deux services utilisent le même service interne, le « Property Persistent Storage », pour assurer la confidentialité et l'authenticité des données. Ce service interne n'est pas directement exposé à l'application qui utilise la bibliothèque « EZIO Mobile SDK ».

6.6.1 Confidentialité et authenticité des données dans le « Property Persistent Storage »

La confidentialité et l'authenticité des données stockées dans l'équipement mobile suivent les principes suivants :

1) Une clé maîtresse est stockée sur l'équipement et protégée par une clé dérivée de l'entrée fournie au « Property Persistent Storage » (cette entrée peut prendre la forme d'un mot de passe ou d'une clé, en fonction du service qui utilise le « Property Persistent Storage »).

2) La donnée fournie est chiffrée par 3 couches qui utilisent des secrets qui proviennent de 3 environnements différents :

    a. Une clé maîtresse est utilisée pour dériver deux sous clés :

        i. pour la confidentialité ;

        ii. pour l'authentification.

    b. L'environnement d'exécution.

    c. L'environnement de l'application.

6.6.2 Confidentialité et authenticité des clés prises en charge par le « Password Manager »

Le « Password Manager » utilise plusieurs instances du service interne de « Property Persistent Storage ». Afin de libérer les clés protégées, les principes suivant sont appliqués :

- Un mot de passe fourni par l'application est utilisé pour débloquer un premier niveau de « Property Persistent Storage ». Ce premier niveau contient une clé applicative.
- La clé applicative est alors utilisée pour débloquer un deuxième niveau de « Property Persistent Storage ». Ce deuxième niveau contient les clés de domaines.

6.6.3 Confidentialité et authenticité des données dans le Stockage Sécurisé

Le Stockage Sécurisé utilise des instances du « Property Persistent Storage ». L'application peut en créer un nombre quelconque, chacun identifiés par un nom unique. Chacune de ces instances peut être débloquée par la clé de domaine pour le Stockage Sécurisé, fournie par le « Password Manager » :

- Le service de Stockage Sécurisé récupère la clé depuis le « Password Manager » si le mot de passe fournit est correct.
- Le service de Stockage Sécurisé peut alors débloquer le service interne de protection.
- L'application peut alors lire ou écrire des données qui seront protégées en confidentialité et authenticité dans l'équipement mobile.

6.7 SYNTHESE DES PROTECTIONS CONTRE LES MENACES IDENTIFIEES

Le tableau suivant présente une synthèse les mécanismes de protection mis en œuvre dans la solution « EZIO Mobile ».

Menace	Protection
M1 : équipement volé	La clé secrète est protégée par le code PIN qui n'est pas connu du voleur. Aucune donnée qui a été dérivée du PIN n'est stockée en mémoire persistante.
M2: PIN et/ou empreinte et/ou mot de passe volé	Inutile sans connaissance de la clé secrète stockée sur l'équipement.
M3 : Interception pendant la mise à disposition de la clé secrète	Tous les échanges entre l'équipement mobile et le serveur EPS sont chiffrés via les protocoles MPP et TLS.
M4 : Reverse Engineering de l'application	Pour iOS, les opérations sensibles sont réalisées en C qui est compilé avec des options rendant plus difficile l'analyse.
M5 : clone de la clé secrète	Ne fonctionnera pas sur d'autres équipements car la clé est chiffrée avec l'empreinte numérique de l'équipement. Inutile sans le code PIN.
M6 : Accès au PIN ou à l'empreinte ou au mot de passe ou à la clé secrète pendant les opérations cryptographiques	Requiert un équipement « jailbreaké » et un malware dédié installé sur l'équipement. Le SDK utilise un objet « Secure Data » pour manipuler toute les informations sensibles puis l'efface à la fin de l'utilisation.
M7 : Attaque par brute force sur la clé secrète	Requiert un équipement « jailbreaké », un malware dédié installé sur l'équipement et la compromission du chiffrement de la base de données. L'attaque ne sera pas réalisable car le code PIN n'est pas stocké et qu'il n'y a pas de condition d'arrêt dans les algorithmes de chiffrement/déchiffrement.
M8: Attaque par brute force sur une clé maîtresse	Requiert un équipement « jailbreaké » et un malware dédié installé sur l'équipement. L'attaquent n'est pas capable de réaliser une attaque par brute force sur une clé maîtresse en un temps raisonnable.

FIN DU DOCUMENT