SOGETI

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	**Projet**	**Fournisseur**
GEMALTO	Cible de sécurité CSPN - EZIO Mobile SDK iOS	SOGETI – CESTI

Modification		
Date	Version	Evolution
21/05/2015	1.0	Première version

SOMMAIRE

1 IDENTIFICATION DU PRODUIT

Organisation éditrice	Gemalto
Lien vers l'organisation	http://www.gemalto.com
Nom commercial du produit	EZIO Mobile SDK pour iOS
Numéro de la version évaluée	2.6
Catégorie du produit	Identification, authentification et contrôle d'accès

2 ARGUMENTAIRE DU PRODUIT

2.1 DESCRIPTION GENERALE DU PRODUIT

Gemalto EZIO Mobile est une solution de génération de mots de passe à usage unique (One Time Password, OTP). La solution est composée d'une bibliothèque de développement « EZIO Mobile SDK » pour application mobile ainsi qu'un composant serveur « EZIO Mobile EPS » (Enrollment and Provisionning Server, EPS). 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 sécurité 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.

Le serveur 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 et Gemalto OATH.

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 tandis que pour Android elle est écrite en Java.

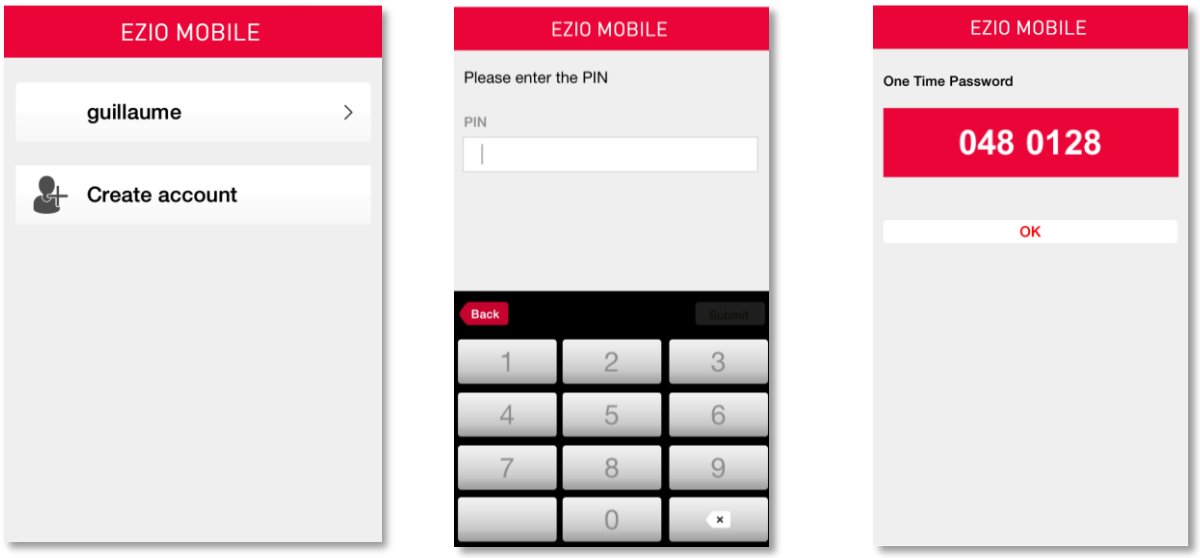
La génération d'un OTP, suite à la saisie du code PIN par l'utilisateur, implique l'accès à la clé secrète de l'utilisateur. La protection de cette clé est réalisée par la bibliothèque.

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.

2.2 DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT

Le client télécharge l'application d'authentification forte, développée avec la bibliothèque « EZIO Mobile SDK », à partir de l'AppStore (pour client iOS) ou du Google Play (pour client Android), puis accède au service de génération d'OTP avec les informations d'identification transmises par le service 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) Saisi du PIN* *(3) affichage de l'OTP*

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

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 2 illustre les composants essentiels de la solution et les interactions principales entre eux.

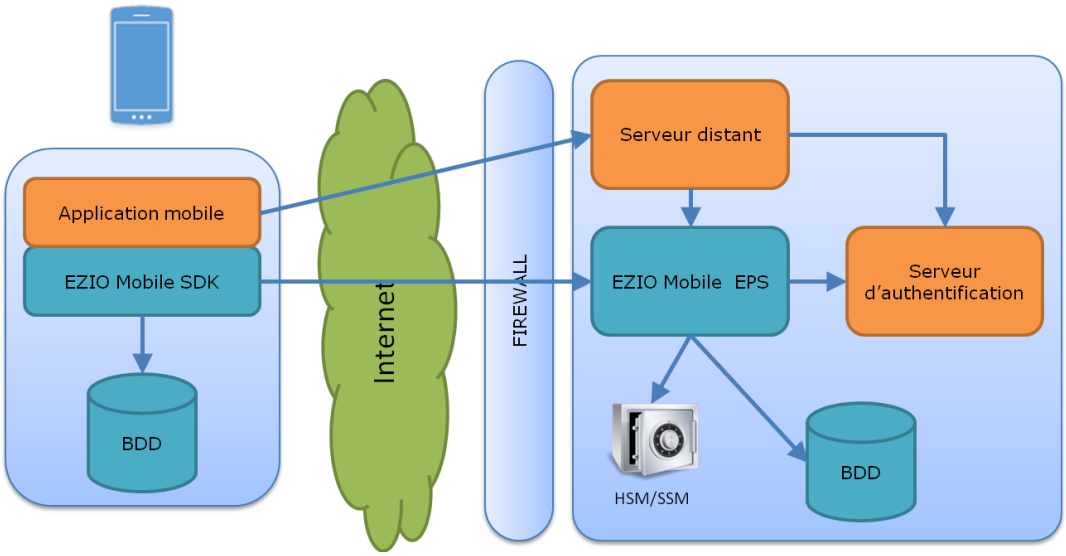


Figure 2 - aperçu de la solution EZIO Mobile

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.

A 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.

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 OTP OATH (incluant OCRA) ;
- Inscription des graines OATH à partir du serveur EPS ;
- Stockage des graines OATH sur l'équipement.

Tandis que les éléments suivants sont hors périmètre :

- OTP CAP : calcul et mise à disposition (provisionning) ;
- Dynamic Signature (protocole propriétaire de Gemalto, conforme à CAP) ;
- Mise à disposition hors ligne, héritage de l'importation de graine (migration du SDK 1.x au 2.x) ;
- Vérification OTP VIC ;
- Support du « dual seed » pour OATH ;
- Secure Pin Pad.

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 en version 2.6 pour iOS nécessite un équipement disposant du système d'exploitation iOS 32 bit (version 6.x, 7.x et 8.x) ou iOS 64 bit (version 7.x and 8.x).

4 DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Les biens sensibles à protéger sont le code PIN et la clé secrète générés par le serveur EZIO Mobile EPS et attribués à un utilisateur donné. Lors de la mise à disposition de la clé secrète sur l'équipement mobile, d'autres clés sont également utilisées. L'ensemble de ces informations sont utilisées pour générer un OTP permettant l'authentification de l'utilisateur concerné.

Les biens sensibles suivants sont identifiés :

B1 : le code PIN, volatile et unique à chaque service.

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

B3 : la clé maitre stockée sur l'équipement mobile par les mécanismes de la plateforme. Donnée persistante et unique pour chaque instance de l'application.

B4 : la clé de stockage volatile.

B5 : la clé d'environnement volatile et unique à chaque service.

B6 : la clé de chiffrement volatile, dérivée du PIN et unique à chaque code PIN.

L'OTP généré est un bien sensible du point de vu 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 claire 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.

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 pendant les opérations cryptographiques.

Les scénarios d'attaques suivants ont été identifiés

- M1 : équipement volé ;
- M2 : Code PIN 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 la clé secrète en claire en temps réel pendant les opérations cryptographiques ;
- M7 : attaque par force brute sur la clé secrète ;

Le profil de l'attaquant retenu pour l'application d'authentification, développée à partir de la bibliothèque EZIO Mobile SDK, qui tente de générer un OTP en lieu et place de l'utilisateur légitime, met en œuvre les menaces M1, M2, M3, M4, M5, M6 et M7.

6 DESCRIPTION DES FONCTIONS DE SECURITE

6.1 BLOCAGE DU PIN.

La clé secrète est chiffrée avec le code PIN sur l'équipement mobile (et sur le serveur EPS). 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 correcte. 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.

6.2 PROTECTION EN CONFIDENTIALITE DES CLES STOCKEES

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.

6.2.1 Protection de la clé secrète

- La clé secrète est protégée par le mécanisme KeyChain.

6.3 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 le SDK.

2) Le 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 le SDK.

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 au SDK.

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

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

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.

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 brute force (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/rooté avec une application malveillante dédiée tandis que les données sensibles sont effacées après utilisation. La détection d'un environnement jailbreaké/rooté rend également plus difficile l'attaque.

6.5 PROTECTION EN INTEGRITE DES BIENS SENSIBLES

Les biens sensibles n'ont pas de protection en intégrité dédiée 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 correcte, 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.

6.6 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.

6.7 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 : Code PIN 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	Des outils d'obfuscation du code sont utilisés pour Android. 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 la clé secrète pendant les opérations cryptographiques	Requiert un équipement jailbreaké/rooté et un malware dédié installé sur l'équipement. Le SDK utilise un objet « Secure Data » pour manipuler toute les informations sensibles puis l'efface a la fin de l'utilisation.
M7 : Attaque par brute force sur la clé secrète	Requiert un équipement jailbreaké/rooté, 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.

FIN DU DOCUMENT