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 EPS

VALIDITE DU DOCUMENT

Identification		
Client	**Projet**	**Fournisseur**
GEMALTO	Cible de sécurité CSPN - EZIO Mobile EPS	SOGETI – CESTI

Modification		
Date	Version	Evolution
21/05/2015	1.0	Première version
27/08/2015	1.1	Précision de l'utilisation des clés et des menaces
21/03/2016	1.2	Précision de la plateforme cible avec un HSM
29/04/2015	1.3	Précision du lien entre le HSM et le serveur d'authentification. Suppression du module firmware pour le HSM.

SOMMAIRE

1 IDENTIFICATION DU PRODUIT

Organisation éditrice	Gemalto
Lien vers l'organisation	http://www.gemalto.com
Nom commercial du produit	EZIO Mobile EPS
Numéro de la version évaluée	2.6.1
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.

La Figure 1 illustre les composants essentiels de la solution et les interactions principales entre eux.

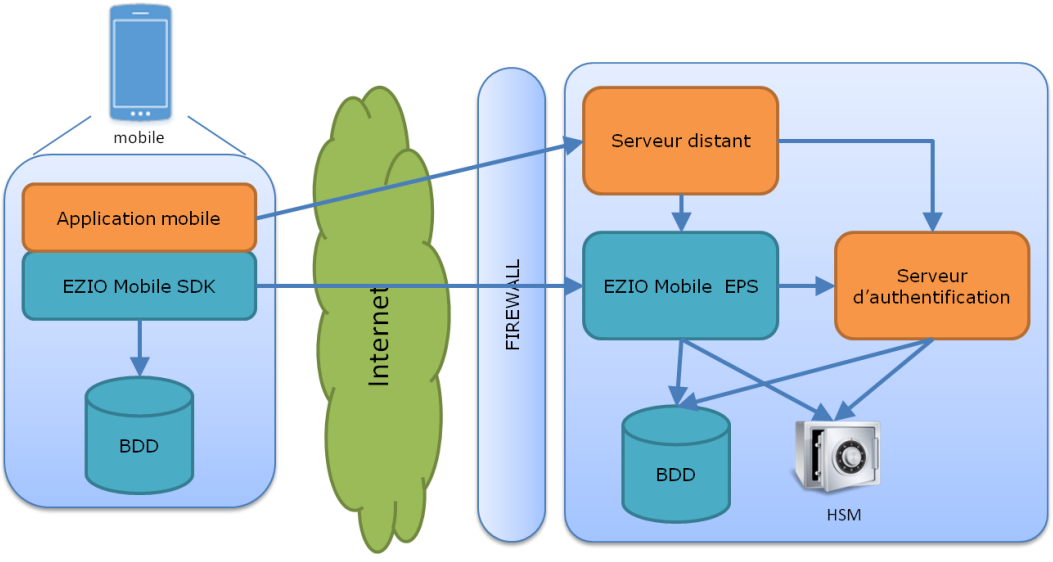

Figure 1 - aperçu de la solution EZIO Mobile

Le serveur « EZIO Mobile EPS » est un composant de service sur le SI de la banque. Il expose deux interfaces principales : une API REST pour la banque et une interface pour le protocole d'initialisation (enrollment) et de mise à disposition (provisionning).

L'API REST est utilisée par la banque pour initialiser les clés secrètes (token), réaliser des opérations d'audit et voir le statut du serveur. Le protocole d'initialisation est utilisé pour acheminer de manière sécurisée la clé secrète de l'utilisateur sur le téléphone mobile. A part l'interface publique, le serveur EPS a plusieurs outils en ligne de commande pour gérer le système. Pour l'intégration avec des systèmes externes tels que les serveurs d'authentification, le serveur EPS a un plug in avec API pour autoriser l'inscription et l'activation de la clé secrète sur le système externe.

2.2 DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT

Le cas d'usage principal destiné à générer un mot de passe à usage unique nécessite une phase d'initialisation de la clé secrète de l'utilisateur (client). La figure suivante illustre les étapes à réaliser avant toute utilisation de la fonctionnalité de génération d'un OTP par le client mobile.

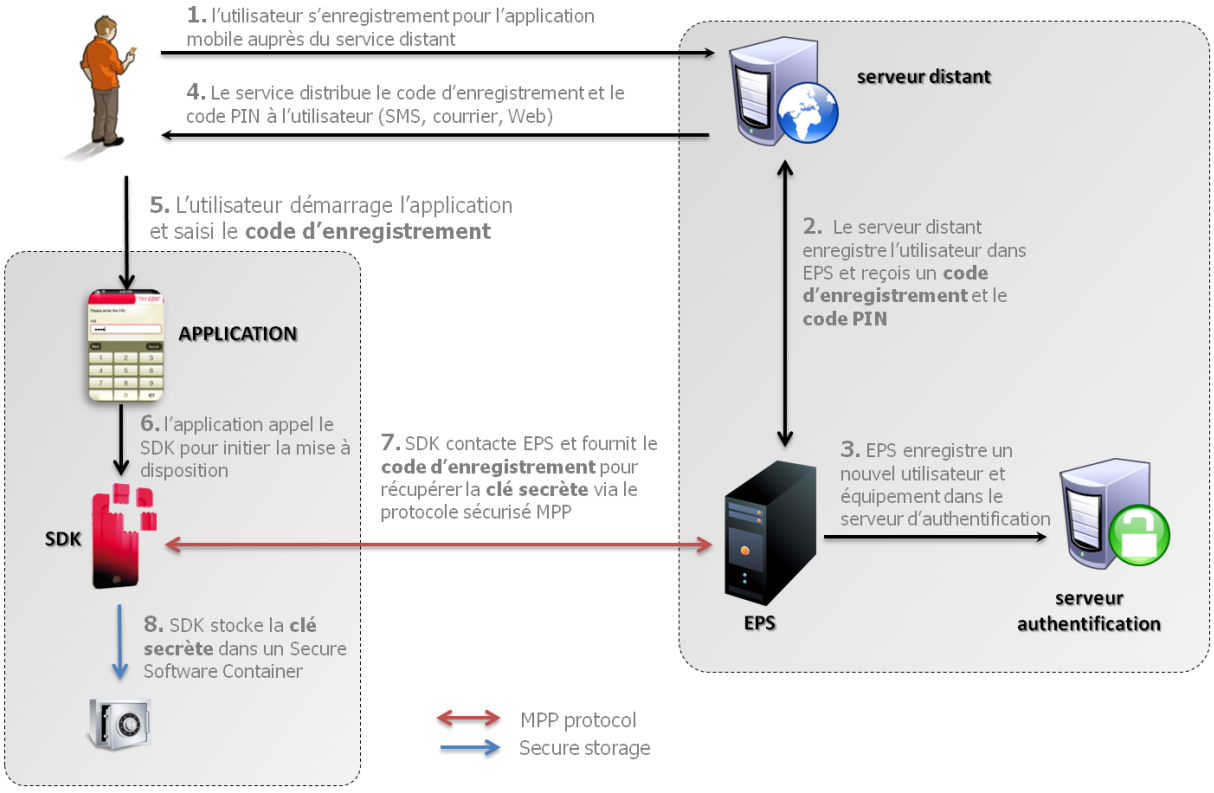

Figure 2 - inscription et mise à disposition de la clé secrète (token)

L'utilisateur dispose d'une interface pour demander l'utilisation d'une application mobile qui contiendra une clé secrète sous forme de « token ». La demande est faite auprès d'un serveur de service à distance (banque, portail e-commerce etc.). Les étapes de ce processus, décrites dans la Figure 2, montre que la génération et la transmission du « token » sont prises en charge par le service à distance en utilisant le serveur EZIO Mobile EPS.

2.2.1 Inscription (Enrollment)

Suite à la demande de l'utilisateur, un client initiateur, habituellement un serveur bancaire, demande la création d'une nouvelle clé secrète pour l'utilisateur. Le serveur EPS va dériver/générer des identifiants associés à la clé secrète et les inscrire dans les services de support (back-end) tel qu'un serveur d'authentification. Pendant l'inscription, le serveur EPS va générer un PIN et un code d'enregistrement unique pour l'utilisateur. Le client initiateur les récupère puis les délivre de manière sécurisé à l'utilisateur.

Sur le serveur EPS, l'application responsable de l'inscription est une application web qui fourni des API REST permettant également l'audit et la surveillance du statut des opérations.

2.2.2 Mise à disposition (Provisioning)

Une fois en possession du PIN et du code d'enregistrement, l'utilisateur peut télécharger l'application développée à partir de la bibliothèque EZIO Mobile SDK. En utilisant le code d'enregistrement fourni à l'utilisateur, le SDK envoie une requête d'inscription avec les identifiants au serveur EPS en utilisant le protocole « EZIO Mobile Provisionning Protocol » (MPP). Le serveur EPS va authentifier et autoriser la requête et fournir les identifiants du token.

Optionnellement, une étape additionnelle d'activation peut être requise pendant laquelle un OTP est calculé par le SDK avec le PIN de l'utilisateur puis vérifié par le serveur EPS afin d'activer le token. Cette étape optionnelle est en dehors de la cible d'évaluation.

Les identifiants du token sont à partir de là inscris dans le téléphone mobile.

Sur le serveur EPS, l'application responsable de la mise à disposition de la clé secrète est une application web qui fourni des API REST permettant également l'audit des opérations.

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

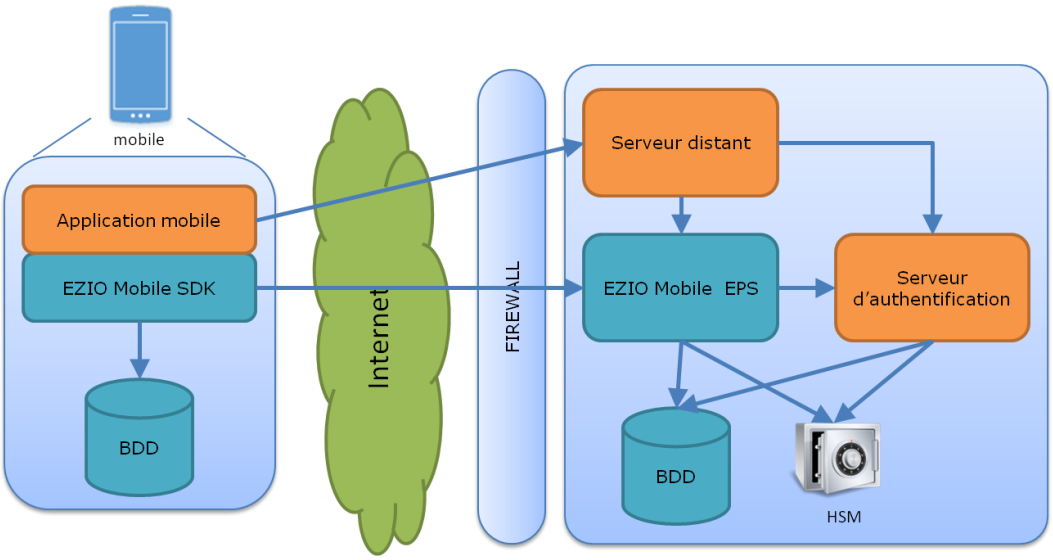

Figure 3 - aperçu de la solution EZIO Mobile

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

HS1 : le serveur de service à distance et le serveur EPS sont déployés chacun sur un serveur dédié dans une zone de confiance du SI.

HS2 : le serveur EPS est installé suivant les guides d'intégration, de sécurité et d'administration.

HS3 : les connexions des clients mobiles invoquent les services du serveur EPS au travers d'un canal HTTP sécurisé avec TLS.

HS4 : les profils des utilisateurs du serveur EPS sont configurés conformément à la politique de sécurité du SI.

HS5 : le HSM est un composant de confiance du SI, il est supposé réaliser les fonctions cryptographiques attendues suivants ses spécifications. Il est administré suivant ses guides de sécurité et d'administration et n'est pas considéré comme un vecteur d'attaque.

2.5 DESCRIPTION DES DEPENDANCES

Le serveur EZIO Mobile EPS a les dépendances suivantes :

- Matérielle :
  - HSM Safenet PSE-I PL220 K5 PCI.
- Logicielle :
  - Serveur d'authentification DS3 2.2.1-SP ;
  - Serveur de base de données MariaDB 5.5.31.

2.6 DESCRIPTION DES UTILISATEURS ET ROLES TYPIQUES

US1 : le serveur du service à distance, qui utilise le serveur EPS pour l'inscription des utilisateurs finaux, est correctement déployé et géré dans une zone de confiance du SI (HS1).

US2 : l'administrateur en charge de l'installation, de la configuration et du maintien en conditions opérationnelles du serveur EPS, sur le SI du service à distance, n'est pas malveillant (HS1, HS2).

US3 : le gestionnaire des clés opérationnelles, dont à besoin le serveur EPS, n'est pas malveillant et réalise les configurations nécessaires au respect des conditions de sécurité (HS3, HS4 et HS5).

2.7 DESCRIPTION DU PERIMETRE D'EVALUATION DU PRODUIT

Les éléments suivants sont considérés dans le périmètre d'évaluation du serveur « EZIO Mobile EPS » :

- Opérations d'inscription et de mise à disposition d'une clé secrète (enrollment & provisionning) ;
- Protocol OATH (incluant OCRA) ;
- Interface avec le module de sécurité (HSM) ;
- Le plug-in API pour le serveur d'authentification ;
- Opération de gestion des clés ;

Tandis que les éléments suivants sont hors périmètre :

- Le système d'exploitation ;
- Le serveur de base de données ;
- Le serveur d'authentification.

3 DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

3.1 MATERIEL COMPATIBLE OU DEDIE

Le serveur EPS est exécuté sur un serveur physique IBM 3650 M4.

3.2 SYSTEME D'EXPLOITATION RETENU

Le serveur EPS est exécuté sur un système d'exploitation Linux avec notamment un environnement d'exécution Java 1.7 (JDK), un serveur d'application web pour Servlet Java et un HSM.

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 des opérations d'inscription et de mise à disposition d'une clé secrète (enrollment & provisionning), d'autres clés sont également utilisées.

Les biens sensibles suivants sont identifiés :

B1 : le code PIN, employé par l'utilisateur final pour générer un OTP, volatile et unique à chaque service.

B5 : la paire de clé RSA et le mot de passe pour le protocole de mise à disposition (MPP), stockée dans la base de données sous forme chiffrée ;

B6 : le code d'enregistrement `RC`, employé par l'utilisateur final pour s'authentifier lors de la mise à disposition, stocké dans la base de données sous forme chiffrée ;

B7 : la clé secrète 'TOK' (graine OATH) stockée en base de données sous forme chiffrée. Donnée persistante et unique pour chaque service.

Le serveur EPS délègue la gestion des clés suivantes à un HSM :

`DBK` : la clé de base de donnée est utilisée pour chiffrer la clé secrète (graine OATH) lors du stockage en base de données ;

`TRK` : la clé de transport pour le serveur d'authentification est utilisée pour chiffrer la clé secrète (graine OATH) pendant la mise à disposition avec le serveur d'authentification ;

`ZMK` : la clé de transport est utilisée pour l'importation de clé à partir d'un module de sécurité (SM) externe. Elle est utilisé pour chiffrer les clés entre le gestionnaire de clé et le module de sécurité ;

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 les biens sensibles stockés sur le serveur ;
- Attaque pendant les opérations cryptographique.

Le profile de l'attaquant retenu pour le serveur EPS qui tente de générer un OTP en lieu et place des utilisateurs légitimes, met en œuvre les menaces suivantes :

- M1 : Un attaquant externe intercepte les requêtes sur le serveur EPS ;
- M2 : Un attaquant externe modifie les requêtes vers le serveur EPS ;

6 DESCRIPTION DES FONCTIONS DE SECURITE

6.1 BLOCAGE DU PIN

La clé secrète est chiffrée avec le code PIN sur le serveur EPS (sur l'équipement mobile). L'application ne peut pas influencer ce principe qui est fondamentale. 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 le serveur est assurée par les mécanismes suivants :

1) Un module de sécurité (SM) gère les clés suivantes :
    a. La clé secrète `TOK` doublement chiffrée, une première couche avec la clé `KEK` et une seconde couche avec la clé `DBK` ;
    b. La clé `DBK`chiffrée avec la clé `MK` du SM ;
    c. La clé `TRK`chiffrée avec la clé `MK` du SM ;
    d. Le mot de passe de la pair de clé RSA chiffré avec la clé `DBK`.
2) Une base de données stock les clés suivantes :
    a. La clé `DBK`chiffrée avec la clé `MK` du SM ;
    b. La clé `TRK`chiffrée avec la clé `MK` du SM ;
    c. La pair de clé RSA (keystore) ;
    d. Le mot de passe de la pair de clé ((keystore password)DBK) ;
    e. La clé secrète `TOK`doublement chiffrée (((TOK)KEK)DBK) ;
    f. Le code d'enregistrement `RC`.

6.2.1 Protection de la clé secrète

En base de données, la clé secrète est protégée par deux enveloppes de chiffrement, une première avec une clé AES dérivée du code PIN puis une seconde avec la clé de la base de données.

Sur le serveur d'authentification, la clé secrète est protégée par un module de sécurité. La clé secrète est transmise chiffrée avec une clé de transport entre le serveur EPS et le module de sécurité du serveur d'authentification.

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 génère une clé de session K1 pour le chiffrement et une clé K2 pour l'authentification.

3) Les clés K1, K2 et le code d'enregistrement sont chiffrés avec la clé publique du serveur EPS puis envoyés à ce dernier.

4) Côté serveur EPS, le HSM déchiffre les clés K1, K2 et le code d'enregistrement avec la clé privée sur serveur EPS.

5) Le serveur EPS trouve la clé secrète (chiffrée avec le code PIN préalablement généré) correspondante au code d'enregistrement.

6) Le HSM chiffre une nouvelle fois la clé secrète avec K1 puis calcul un HMAC avec K2. Le serveur EPS récupère la clé secrète (avec 2 niveaux de chiffrement et une enveloppe d'authentification) et la transmet à l'application mobile.

7) Sur l'application mobile, la clé secrète est transmise au SDK.

8) La clé secrète est authentifiée avec le HMAC et k2.

9) La première couche de chiffrement de la clé secrète est enlevée avec la clé K1 puis la clé secrète chiffrée avec le PIN est chiffrée avec une clé de stockage et une clé d'environnement puis stockée sur l'équipement.

La confidentialité de la clé secrète est assurée pendant toute les étapes car la clé n'est jamais manipulée en claire (la clé secrète est toujours sous une forme chiffrée avec le code PIN) et qu'une authentification mutuelle de l'application et du serveur EPS est mise en œuvre, en effet :

- L'application mobile qui reçoit la clé secrète est préalablement authentifiée via la validation du code d'enregistrement. Ainsi la clé secrète est délivrée à un utilisateur autorisé.

- Le code d'enregistrement est chiffré avec la clé publique du serveur EPS visé. Ceci assure que le code d'enregistrement n'est utilisé que par le serveur EPS autorisé.

6.4 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.

6.5 SYNTHESE DES PROTECTIONS CONTRE LES MENACES IDENTIFIEES

Le tableau suivant présente une synthèse des mécanismes de protection mis en œuvre dans le serveur EPS de la solution EZIO Mobile.

Menace	Protection
M1 : Un attaquant externe intercepte les requêtes sur le serveur EPS	Tous les échanges entre l'équipement mobile et le serveur EPS sont chiffrés via les protocoles MPP et TLS. La clé secrète a plusieurs couche de chiffrement dont une liée au PIN qui n'est jamais stocké.
M2 : Un attaquant externe modifie les requêtes vers le serveur EPS	L'interface interne pour l'enregistrement est dans une zone de confiance du SI. L'interface publique pour l'API de mise à disposition est utilisée que par les protocoles MPP et TLS. Toutes les données sensibles sur le serveur EPS sont chiffrées. Le code d'enregistrement est généré aléatoirement. Le PIN n'est jamais stocké.

FIN DU DOCUMENT