Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2016/14

Serveur EZIO EPS, version 2.6.1

Paris, le 6 janvier 2017

Le directeur général de l'agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2016/14**
Nom du produit **Serveur EZIO EPS**
Référence/version du produit **Version 2.6.1**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire ***GEMALTO*** **Avenue du Jujubier** **Z.I. Athelia IV** **13705 La Ciotat Cedex** **France**
Centre d'évaluation ***SOGETI*** **24, rue du Gouverneur Général Félix Eboué** **92136 Issy-les-Moulineaux Cedex** **France**
Fonctions de sécurité évaluées **Blocage du PIN** **Protection en confidentialité des clés stockées** **Protection de la clé secrète** **Protection en confidentialité de la clé secrète pendant la mise à disposition** **Protection en intégrité des biens sensibles**
Fonction(s) de sécurité non évaluées **Aucune**
Restriction(s) d'usage Oui **(cf. §3.2)**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. LE PRODUIT 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT EVALUE 8
1.2.1. Catégorie du produit 8
1.2.2. Identification du produit 8
1.2.3. Fonctions de sécurité 8
1.2.4. Configuration évaluée 9

2. L'EVALUATION 10

2.1. REFERENTIELS D'EVALUATION 10
2.2. CHARGE DE TRAVAIL PREVUE ET DUREE DE L'EVALUATION 10
2.3. TRAVAUX D'EVALUATION 10
2.3.1. Installation du produit 10
2.3.2. Analyse de la documentation 10
2.3.3. Revue du code source (facultative) 10
2.3.4. Analyse de la conformité des fonctions de sécurité 11
2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité 11
2.3.6. Analyse des vulnérabilités (conception, construction, etc.) 11
2.3.7. Accès aux développeurs 11
2.3.8. Analyse de la facilité d'emploi et préconisations 11
2.4. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES 12
2.5. ANALYSE DU GENERATEUR D'ALEAS 12

3. LA CERTIFICATION 13

3.1. CONCLUSION 13
3.2. RESTRICTIONS D'USAGE 13

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « Serveur EZIO EPS, version 2.6.1 » développé par *GEMALTO*.

Ce serveur assure les fonctions d'enrôlement et de *provisioning* au sein du système EZIO Mobile, permettant aux utilisateurs en possession d'une application sur *smartphone* développée à partir du SDK EZIO Mobile de s'authentifier auprès d'un service tiers (serveur bancaire notamment).

La figure ci-dessous explicite l'architecture du système EZIO.

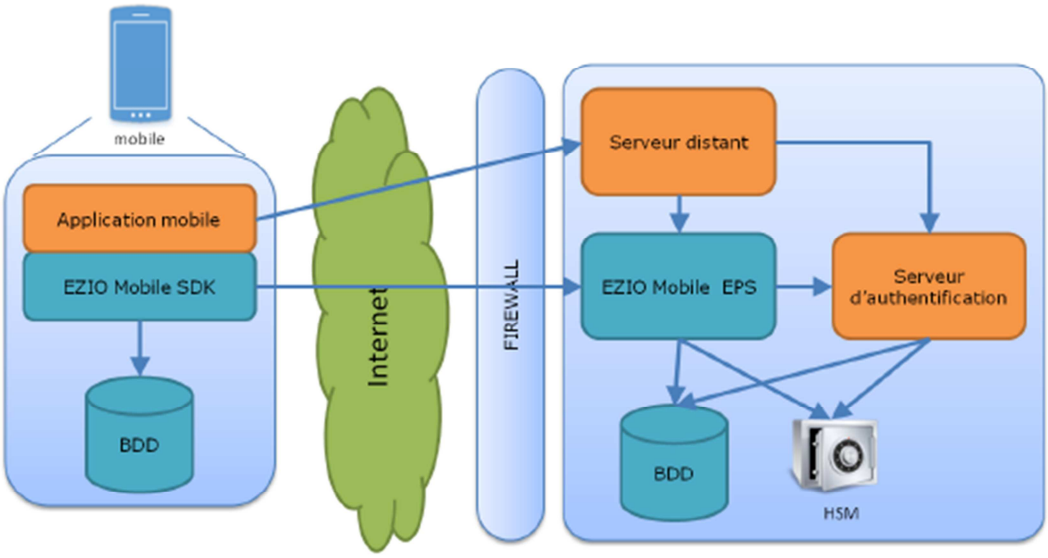

Figure 1 - Architecture du système EZIO.

La figure suivante illustre la phase d'enrôlement d'un utilisateur et de mise à disposition de la clé secrète (*provisioning*) :

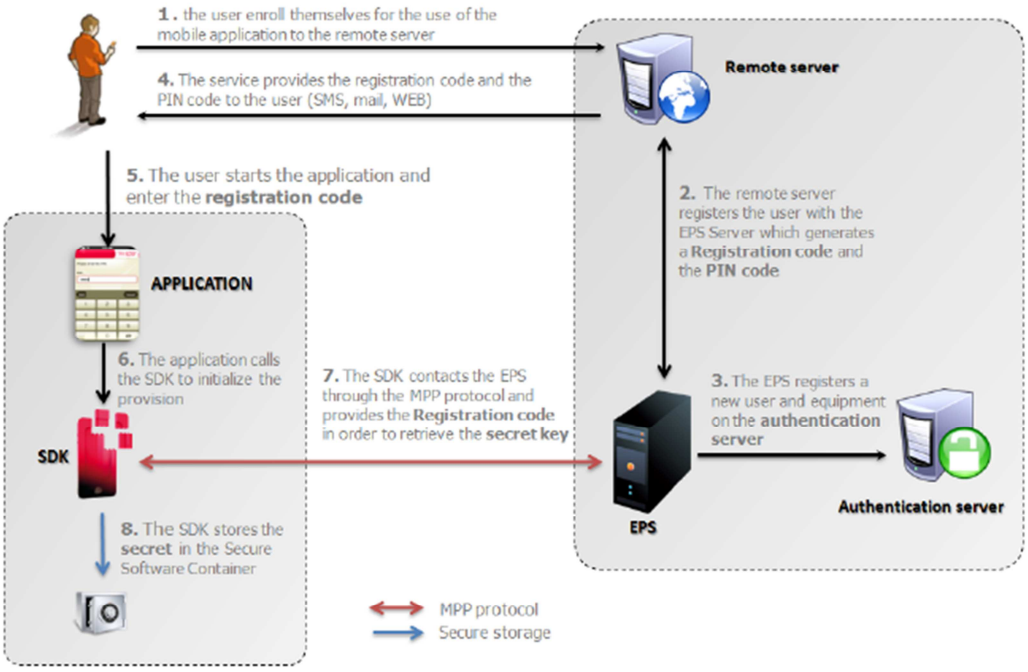

Figure 2 - Phase d'enrôlement et de *provisioning*

Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.1.1. Catégorie du produit

☐ 1 – détection d'intrusions
☐ 2 – anti-virus, protection contre les codes malicieux
☐ 3 – pare-feu
☐ 4 – effacement de données
☐ 5 – administration et supervision de la sécurité
☒ **6 – identification, authentification et contrôle d'accès**
☐ 7 – communication sécurisée
☐ 8 – messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 – environnement d'exécution sécurisé
☐ 11 – terminal de réception numérique (*Set top box*, STB)
☐ 12 –matériel et logiciel embarqué
☐ 13 – automate programmable industriel
☐ 14 – autre

1.1.2. Identification du produit

Nom du produit	Serveur EZIO EPS
Numéro de la version évaluée	2.6.1

La version certifiée du produit peut être identifiée à l'aide de l'API de statut du serveur EPS, en se connectant à l'adresse suivante :

```
https://<IP_serveur>:3443/enroller/api/status
```

1.1.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- le blocage du PIN,
- la protection en confidentialité des clés stockées,
- la protection de la clé secrète,
- la protection en confidentialité de la clé secrète pendant sa mise à disposition,
- la protection en intégrité des biens sensibles.

1.1.4. Configuration évaluée

Le produit a été livré par le développeur sur un serveur physique IBM x3650 Series M4 au format rack, identique à celui illustré sur la figure suivante :

Figure 3 - Serveur IBM x3650 Series M4

Le serveur embarque un système d'exploitation Linux *Red Hat Enterprise*, sur lequel sont installés les logiciels suivants nécessaires au fonctionnement du serveur EPS :

- *Java Development Toolkit* (version 1.7.0.13),
- *Apache Tomcat* (version 6.0.32),
- *MariaDB* (version 5.5.31),
- le serveur d'authentification DS3 (version 2.2.1-SP).

Le développeur a également mis à disposition de l'évaluateur un *HSM* Thales payShield 9000.

Une configuration *debug* d'EPS été installée sur le serveur fourni, afin de permettre à l'évaluateur d'effectuer les tests nécessaires, y compris ceux nécessitant l'usage de mécanismes faibles (connexions non sécurisées, *SSM*[1] etc.) non utilisables en configuration nominale durcie.

[1] *Software Security Module*, ou module de sécurité logiciel.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, menaces, utilisateurs et fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Sans objet.

2.3.1.2. Description de l'installation et des non-conformités éventuelles

Le produit a été livré préinstallé. La configuration a été faite à l'aide d'une carte à puce préalablement programmée sur un PC à l'aide de l'outil *Ops Control Centre*. Les étapes de la configuration du serveur sont correctement documentées dans le guide *Hand's on* (voir [GUIDES]).

2.3.1.3. Durée de l'installation

L'installation a été rapide et n'a pas soulevé de problème particulier.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une installation et une prise en main efficace du produit.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source et estime que le code est clairement organisé et correctement documenté.
La maintenabilité du code est assurée par l'utilisation de fonctions clairement définies.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Le produit dans sa version évaluée offre des mécanismes globalement robustes et à l'état de l'art.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Toutes les fonctions de sécurité ont fait l'objet d'une analyse et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2. Recommandations pour une utilisation sûre du produit

L'utilisateur du produit doit avoir une compréhension claire du fonctionnement de la solution, en particulier de l'architecture des communications et de l'utilisation qui est faite des données. Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis, en particulier les guides d'administration et d'intégration.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur disposant de notions de base en cryptographie et en administration de serveurs.

2.3.8.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas de vulnérabilité exploitable dans le contexte d'emploi visé.

2.5. Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé, il se base sur une graine générée par le HSM qui fait l'objet d'un retraitement de nature algorithmique et est jugé conforme au [RGS]. Aucune vulnérabilité exploitable liée à l'utilisation de ce générateur n'a été identifiée.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Serveur EZIO EPS, version 2.6.1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 0 du présent rapport de certification.
L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN EZIO Mobile EPS* Référence : *GEMALTO-EZIO-EPS-ST v1.3* ; Version : 1.3 ; Date : *29 avril 2016*
[RTE]	*CSPN Evaluation EZIO EPS 2.6.1* Référence : *U12.ESEC.PRO2016.101-CSPN-EZIO-EPS2.6-ETR* ; Version : 1.0 ; Date : *13 juin 2016*
[SPEC-CRY]	Ezio_Mobile_EPS-Cryptographic_Mechanisms Référence : -- ; Version : -- ; Date : *26 novembre 2016*
[GUIDES]	*Administration Guide for Ezio Server EPS* Référence : -- ; Version : -- ; Date : *28 janvier 2016* *Ezio Server EPS Integration Guide* Référence : -- ; Version : 0.10 ; Date : *21 avril 2016* *Administration Guide for Ezio Server AS* Référence : -- ; Version : -- ; Date : *22 avril 2016* *DS3 Hand's On* Référence : -- ; Version : -- ; Date : *22 avril 2016*

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr/
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.