LEXFO

Cible de sécurité CSPN

Réf. : LYF20170718-ANDROID V1.4

lyf pay

Lyf pay : le paiement mobile

Version Android

21/07/2020

TABLE DES MATIÈRES

1 PRESENTATION DE LA CIBLE DE SECURITE

1.1 VUE D'ENSEMBLE DE LA CIBLE DE SECURITE

Cette cible de sécurité a été élaborée dans le cadre du processus de certification CSPN mis en place par l'ANSSI. Le produit évalué est une application de porte-monnaie électronique et de commerce en ligne, ainsi que les infrastructures serveur permettant ces fonctionnalités.

Ce document décrit le produit évalué, précise les hypothèses relatives à son environnement d'utilisation, les menaces pouvant l'affecter et ses fonctions de sécurité.

1.2 IDENTIFICATION DU PRODUIT

Organisation éditrice	Lyf pay
Lien vers l'organisation	https://www.lyf.eu
Nom commercial du produit	Lyf pay : le paiement mobile
Numéro de la version évaluée	Applications Android : ▶ Lyf pay : le paiement mobile : 5.26.2 ▶ Lyf Pro Encaissement Mobile : 6.2.1 Web services : ▶ api.lyf.eu : 76 ▶ acceptance.lyf.eu : 76
Catégorie de produit	Divers

2 DESCRIPTION DE LA CIBLE D'EVALUATION

2.1 DESCRIPTION GENERALE DU PRODUIT

Les applications **Lyf pay** consistent en une combinaison d'un porte-monnaie électronique et d'une solution d'e-commerce. Les utilisateurs pourront effectuer des achats dans les magasins équipés grâce à leurs smartphones ou de manière transverse sur internet. Il est également possible d'effectuer des dons entre utilisateurs, ou au profit d'associations.

Les commerçants partenaires, en plus de pouvoir accepter des paiements provenant de la solution pourront entretenir une relation avec leur clientèle par le biais d'actualités, d'offres commerciales et des programmes de fidélité.

La solution est composée d'une application mobile cliente, **Lyf pay : le paiement mobile**, et d'une application destinée aux commerçants pour l'encaissement, **Lyf Pro Encaissement Mobile**. Un site commerçant permet la gestion pour les différents magasins.

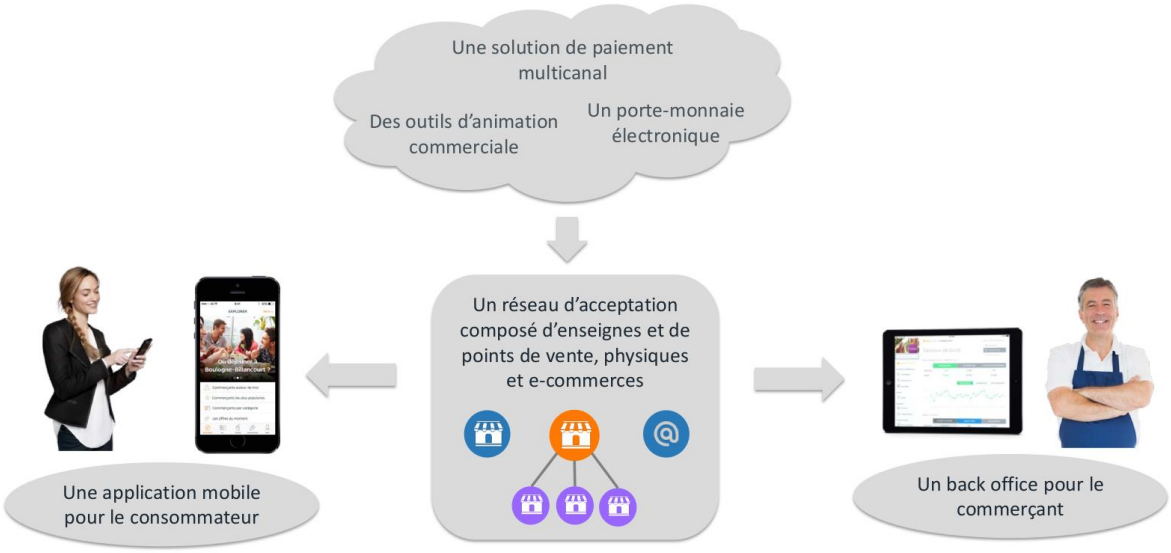

Figure 1 : présentation de la solution Lyf pay

2.2 DESCRIPTION DE L'UTILISATION DU PRODUIT

PARTIE CLIENT – APPLICATION MOBILE

L'application cliente est installée à l'initiative d'un utilisateur sur son smartphone ou sa tablette. L'application permet ensuite de s'inscrire sur le service, enregistrer une carte bancaire, et enfin consulter les magasins partenaires et effectuer des achats.

Les fonctionnalités principales de la solution sont les suivantes :

- **Inscription :** après la saisie des informations de l'utilisateur (e-mail, coordonnées, etc.), un SMS est envoyé au téléphone et contient un lien de validation permettant de finaliser l'inscription et ensuite de définir le code PIN. L'application est ensuite directement prête à l'emploi. Un mot de passe supplémentaire peut être défini afin de faciliter plus tard la reconnexion à l'application en cas de changement de téléphone par exemple ;
- **Utilisation** : deux types de sessions sont générées lors du login, une pour les opérations sensibles, qui expire en 5 minutes (ou à la fin de l'opération de paiement), et une pour les opérations de consultation qui a un temps d'expiration beaucoup plus long ;
  - Opérations non sensibles : l'utilisateur peut consulter la liste des magasins partenaires ainsi que leurs fiches détaillées, offres commerciales et programmes de fidélité ;
  - Opérations sensibles de gestion : l'utilisateur va pouvoir gérer son compte, associer une carte bancaire classique, privative ou dématérialisée, ou virer de l'argent sur son compte bancaire ;
  - Opérations sensibles de paiement : Les achats peuvent s'effectuer sur internet pour certains partenaires, mais surtout directement en magasin à partir de l'application mobile en présentant le QR Code généré par l'application au commerçant ou en lui indiquant le numéro de téléphone associé au compte. Après que le commerçant a lancé le processus de paiement en utilisant l'application pro, l'utilisateur doit valider ce paiement sur son mobile. Cette opération est également possible si l'application cliente n'a pas de connexion au réseau au moment de l'achat (pour des petits montants et un nombre limité de transactions).

PARTIE COMMERÇANT

L'application Pro permet au commerçant d'accepter des paiements, mais aussi de gérer son magasin : rédaction de notes d'actualité, offre commerciales et programmes de fidélité. Les opérations de gestion sont réalisées en passant par le site Pro (https://merchant.lyf.eu).

- **Inscription :** après le processus d'affiliation du commerçant, celui-ci peut télécharger l'application pro et l'initialiser à l'aide du code d'activation fourni par l'équipe commerciale **Lyf pay**. Elle est ensuite directement utilisable pour accepter des paiements ;
- **Utilisation :** l'application permet d'encaisser des paiements en scannant le QR Code généré par l'application du client, ou en entrant son numéro de téléphone. Le client valide le paiement, et l'encaissement est terminé. Le commerçant peut ensuite consulter sa liste de clients (anonymisée) et l'historique des paiements ;

- **Administration :** le commerçant va pouvoir créer ses actualités, offres commerciales et programmes de fidélité en passant par le site web dédié aux commerçants.

2.3 DESCRIPTION DE L'ENVIRONNEMENT D'UTILISATION PREVU

ENVIRONNEMENT SERVEUR

L'infrastructure serveur est hébergée par **Lyf pay** dans deux datacenters sécurisés (firewall applicatif, protection anti-DDoS). Les différents serveurs sont installés d'après des procédures établies sur la base de guides de sécurité fournis par des organismes reconnus tels que le NIST ou l'ANSSI. Ils sont mis à jour régulièrement, en particulier concernant les correctifs liés à la sécurité, et font également l'objet d'audits de sécurité réguliers.

ENVIRONNEMENT CLIENT

La solution est utilisable sur des terminaux Android d'une version supérieure ou égale à 5.0 pour l'application cliente, 4.4 pour l'application pro.

Les logiciels doivent être installés depuis le « store » de l'environnement mobile.

2.4 DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Aucune hypothèse n'est faite sur la configuration des téléphones, mis à part la version minimum du système Android requise pour l'installation. En effet, certaines fonctionnalités de l'application cliente vérifient par exemple la présence d'un mot de passe sur le téléphone, une détection du root est effectuée (même si elle reste non bloquante), et les différents secrets sont protégés et n'apparaissent jamais en clair sur le système de fichier. Bien que souhaitables, les différents mécanismes de sécurité activables par l'utilisateur sur le téléphone (mot de passe, chiffrement) ne sont donc pas des prérequis.

La sécurité physique des serveurs distants est quant à elle considérée comme sûre.

D'un point de vue logique, il est considéré que les codes source des applications côté serveur ne sont pas disponibles.

D'un point de vue organisationnel, les administrateurs de la solution sont considérés comme non hostiles. Les applications mobiles et les mises à jour fournies par **Lyf pay** sont considérées comme sûres : les mécanismes de sécurité du store officiel garantissent l'intégrité et l'authenticité, et on considère qu'elles ne contiennent pas de code malveillant.

2.5 DESCRIPTION DES DEPENDANCES

Aucune dépendance particulière n'est requise sur la plateforme Android.

2.6 DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNES

Quatre groupes d'utilisateurs interviennent dans l'utilisation et la gestion de la solution :

- **administrateur(s) système**

En charge de la gestion des serveurs de l'infrastructure **Lyf pay**. Un administrateur système dispose de droits d'accès privilégiés sur le système d'exploitation hébergeant les applications serveur. Il s'assure du bon fonctionnement des serveurs et maintient leur niveau de sécurité.

- **administrateur(s) applicatif**

En charge de la gestion du produit. Un administrateur applicatif dispose de droits d'accès à l'interface d'administration de **Lyf pay**, qui n'est pas accessible publiquement.

- **utilisateurs finaux de la partie cliente**

En charge de l'installation du logiciel client sur leur smartphone. Les utilisateurs emploient les fonctionnalités de la solution pour gérer leur porte-monnaie électronique, consulter les différentes offres de commerçants, et effectuer leurs achats.

- **utilisateurs finaux de la partie commerçante**

En charge de l'installation du logiciel pro sur leur smartphone. Les utilisateurs emploient les fonctionnalités de la solution pour gérer les données en ligne de leur magasin, et encaisser les achats.

Seuls les cas d'utilisation des utilisateurs finaux (clients et commerçants) seront considérés dans cette évaluation.

2.7 DEFINITION DU PERIMETRE DE L'EVALUATION

Le périmètre de l'évaluation concerne les composants suivants :

- les applications Android fournies :
  - l'application cliente **Lyf pay : le paiement mobile** qui gère le porte-monnaie des utilisateurs, et permet d'effectuer des achats dans divers magasins ;
  - l'application **Lyf Pro Encaissement Mobile** qui gère l'encaissement et la consultation des transactions déjà effectuées ;
- les web services utilisés par les applications côté client et pro ;
- les différents échanges pouvant intervenir dans le cadre de l'utilisation des fonctionnalités de la solution **Lyf pay**.

Les éléments suivants ne font pas partie du périmètre d'évaluation :

- le plugin pour application mobile permettant l'intégration de **Lyf pay** dans l'application mobile d'un partenaire (SDK permettant d'intégrer les fonctionnalités de paiement **Lyf pay** dans une application tierce) ;
- les plugins web permettant d'intégrer le paiement **Lyf pay** dans des sites clients utilisant certains frameworks (magento, prestashop) ;

- le portail web client et le portail commerçant : dans le cadre de l'agrément de la solution par le **GIE-CB**, ces éléments sont déjà audités par un prestataire certifié PASSI. Ces sites seront utilisés pendant l'audit afin d'effectuer des modifications de configuration ou de la création de contenu, mais ils sont considérés comme sécurisés. Seuls les impacts des modifications dans l'application mobile ou le processus de paiement seront considérés ;
- L'utilisation de cartes de fidélité spécifiques à certains magasins.

3 DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

3.1 MATERIEL COMPATIBLE OU DEDIE

Les smartphones Android doivent disposer d'une version du système d'exploitation supérieure ou égale à 5.0 pour l'application cliente, et 4.4 pour l'application pro.

Aucune contrainte matérielle particulière n'est présente. Aussi, un équipement classique de type smartphone est retenu pour l'évaluation, possédant un système d'exploitation récent (Android supérieur ou égal à 6). Concernant la partie serveur, l'évaluation reposera sur l'utilisation de l'infrastructure mise en place par **Lyf Pay**.

3.2 ENVIRONNEMENT SYSTEME RETENU

L'environnement de test prévu concernant cette évaluation comprend deux smartphones (Samsung Galaxy S10), possédant le système d'exploitation Android dans une version supérieure ou égale à 9.

Deux smartphones sont nécessaires afin de tester le processus de paiement où l'application pro scanne le QR Code généré par l'application cliente.

4 DESCRIPTION DES BIENS SENSIBLES

Les différents biens que la solution doit protéger sont les suivants :

- **B1 : Données d'authentification client**

Les identifiants (login et PIN/mot de passe) employés par les utilisateurs de la solution doivent être protégés en confidentialité et en intégrité.

Toutes les clés cryptographiques et tokens utilisés dans le cadre de l'authentification (clé de session SRP, clé de HMAC, clés permettant de générer les OTP, tokens Oauth2, token pour l'authentification biométrique, etc.) doivent également être protégées en confidentialité et en intégrité.

- **B2 : Données d'authentification commerçant**

Les identifiants employés par les commerçants, ainsi que les valeurs qui en sont dérivées (clé de HMAC par exemple) doivent être protégés en confidentialité et en intégrité.

- **B3 : Interactions client/serveur**

Les données transmises (données personnelles, bancaires, authentification, etc.) entre l'équipement mobile et les serveurs de **Lyf pay** doivent être protégées en confidentialité, intégrité et disponibilité. Ces connexions ont été établies suite à une authentification préalable.

- **B4 : Données utilisateurs**

Les données stockées sur l'appareil mobile et les serveurs de la solution doivent être protégées (ex. configuration de l'application, données bancaires, etc.). Ces données doivent rester confidentielles et intègres.

5 DESCRIPTION DES MENACES

Par hypothèse, les administrateurs ne sont pas considérés comme des attaquants potentiels.

Les menaces suivantes ont été identifiées :

- **M1 : Vol de smartphone**

Le smartphone de l'utilisateur a été perdu ou volé. Dans cette configuration, on peut avoir affaire à deux cas distincts : le smartphone est verrouillé ou ne l'est pas. Le but est d'accéder aux informations enregistrées par l'application.

- **M2 : Compromission du smartphone**

Une application malveillante est présente sur le smartphone de l'utilisateur. Celle-ci va tenter d'obtenir les informations stockées par l'application, ainsi que le contenu des échanges effectués lors de son utilisation. Elle va en particulier tenter de récupérer des informations bancaires ou effectuer des paiements frauduleux.

Une récupération des données stockées par l'application pourraient également permettre de cloner toutes les données utilisées sur un autre téléphone afin d'usurper l'identité d'un utilisateur légitime.

- **M3 : Attaque de l'infrastructure**

Un attaquant ayant connaissance de l'infrastructure **Lyf pay** cible les services et les applications web accessibles sur Internet pour impacter le bon fonctionnement de la solution (attaques de type DoS), compromettre ou récupérer des données (informations bancaires ou personnelles) ou encore obtenir un accès aux comptes d'autres utilisateurs ou commerçants, voire même compromettre les serveurs.

- **M4 : Man in the Middle**

Un attaquant situé sur le même réseau qu'un utilisateur effectue une attaque Man-in-the-Middle sur la connexion. Le but est de capturer les informations sensibles (ex. : identifiants, informations bancaires), d'intercepter ou de modifier les données échangées entre l'application mobile et l'infrastructure serveur.

- **M5 : Analyse de l'application par Rétro-ingénierie**

Un attaquant ayant téléchargé l'application peut analyser celle-ci par rétro-ingénierie. Cela pourrait lui permettre d'approfondir ses connaissances sur le fonctionnement de l'application et ainsi de trouver des vulnérabilités ou des cibles intéressantes (par exemple des web services ou fonctionnalités non documentés), et potentiellement de découvrir des secrets stockés en dur dans l'application.

6 DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

Les fonctions de sécurité implémentées au sein de la solution **Lyf pay** sont les suivantes :

- **F1 - Authentification**

Différentes authentifications sont utilisées par la solution :

- **Oauth2** : opérations non sensibles sur les web services utilisés par l'application cliente **Lyf pay** (https://api.lyf.eu/). Cette authentification est réalisée en utilisant le protocole Oauth2. Cette authentification est réalisée lors de l'inscription au service. La durée du token d'authentification est de 3 mois, mais des tokens de renouvellement sont utilisés afin de renouveler automatiquement cette authentification. Dans le cadre d'une utilisation normale de l'application, cette authentification ne nécessite donc pas d'intervention utilisateur après l'inscription au service. Les tokens d'authentification (accesstoken et refreshtoken) sont stockés de manière sûre en utilisant le keystore du système Android ;

- **Reconnexion** : en cas de suppression de l'application ou de changement de téléphone, le client doit se reconnecter à l'application **Lyf pay**. Cette nouvelle authentification utilise un mot de passe configuré préalablement par l'utilisateur, ainsi qu'un challenge envoyé par SMS. Si l'utilisateur a oublié son mot de passe, un lien « mot de passe oublié » est disponible afin de le réinitialiser. Par ailleurs, cette réauthentification, afin d'éviter toute fraude, va nécessiter de recréer un nouveau PIN pour les opérations sensibles, et va également supprimer tous les moyens de paiement préalablement enregistrés ;

- **Secure Remote Password (SRP)** : les opérations sensibles, comme le paiement ou l'ajout d'une carte, nécessitent la saisie d'un mot de passe. Ce mot de passe (qui est en fait un PIN numérique sur 4 caractères) est créé lors de l'inscription au service, ou lors d'une reconnexion (voir ci-dessus). Le protocole SRP utilise différents mécanismes cryptographiques permettant d'empêcher les attaques par bruteforce même si un attaquant a pu capturer l'échange de clés. Les sessions SRP sont de courte durée : 5 minutes. Pour les opérations de paiement, la session est limitée à l'opération en cours et ne pourra pas être réutilisée pour une autre opération. La session est invalidée lors de la fermeture de l'application ou de sa mise en arrière-plan ;

- **Authentification biométrique** : cette authentification utilise également le protocole SRP, et génère un PIN aléatoirement qui sera stocké de manière sécurisée dans le Keystore, et accessible uniquement suite à une authentification biométrique. Cette authentification biométrique est facultative, et désactivable côté serveur si nécessaire ;

- **HMAC** : La partie commerçant utilise un système de HMAC initialisé par le code d'initialisation fourni par **Lyf pay** lors de l'affiliation. Cette authentification est valable uniquement pour l'encaissement, les autres actions comme le remboursement ou la modification du profil passent par le site commerçant. La clé utilisée est stockée de manière sécurisée, chiffrée à l'aide d'une clé stockée dans le keystore du système Android ;

- **QR Code** : afin d'effectuer un paiement, un QR Code est généré par l'application cliente. Ce QR Code est ensuite scanné par l'application pro et envoyé aux serveurs de **Lyf Pay** afin de réaliser le paiement.

  Trois modes de paiement sont possibles : le paiement offline, le paiement court, et le paiement normal. Dans tous les cas, le QR Code contient un OTP qui va permettre de valider l'authenticité de la transaction. Cet OTP est calculé en utilisant l'algorithme décrit dans la RFC 4226 (il s'agit d'une version étendue à 10 chiffres alors que l'algorithme original en contient 8).

  Dans le cadre du paiement offline, l'OTP est calculé à partir d'une clé récupérée lors de l'inscription (offline shared key) et stockée de manière chiffrée (le PIN de l'utilisateur est nécessaire pour le déchiffrement). Le paiement offline permet donc de payer sans avoir de connexion à internet côté client, il ne nécessite pas d'établir une session avec le serveur, une connexion côté commerçant est suffisante.

  Dans le cadre d'un paiement normal, l'OTP est calculé également à partir d'une clé récupérée lors de l'inscription (online shared key) et nécessite d'établir une session avec le serveur, et donc de saisir le PIN.

  Pour le paiement court, qui est utilisable uniquement pour des montants inférieurs à un certain seuil et un nombre limité de transactions, et uniquement si le téléphone est protégé par un mot de passe, l'OTP est calculé en utilisant les shared keys mentionnées précédemment et sans nécessiter la saisie du PIN de l'utilisateur.

  Dans les trois cas, les QR Codes générés ne sont valables que pour une durée limitée suite à leur émission ;

- **Bruteforce** : le produit inclut des protections empêchant les attaques de type brute force. En cas d'échecs répétés de l'authentification (4 tentatives erronées), un captcha devra être rempli par l'utilisateur. Si le PIN est toujours erroné après la saisie du captcha, le compte sera bloqué.

F2 - Protection des échanges

L'ensemble des transmissions est chiffré, qu'il s'agisse des connexions au site client, au site marchand, ou aux web services. Ce chiffrement est géré par le protocole HTTPS utilisé lors de ces communications. Ce protocole permet également de garantir l'intégrité des transactions.

De plus, lors d'une transaction sensible dans l'application cliente suite à l'authentification en utilisant le protocole SRP, une clé de chiffrement supplémentaire est dérivée de la clé de session SRP et va permettre de chiffrer le trafic à l'intérieur du tunnel TLS avec l'algorithme AES.

Un HMAC permet également de garantir l'intégrité des échanges lors d'une transaction sensible, ainsi que pour toutes les requêtes d'encaissement dans l'application pro.

F3 - Protection des données

Côté client, toutes les informations de session sont stockées de manière chiffrée sur le mobile. Ce chiffrement est réalisé en utilisant les fonctionnalités prévues à cet effet par l'OS (keystore). De plus, aucune information bancaire n'est stockée sur le téléphone, et toute information à caractère personnel n'est accessible que par l'application et stockée de manière sécurisée.

Côté serveur, les données utilisateur et techniques sont protégées par les différents mécanismes d'authentification et de transport (confidentialité et intégrité). Les serveurs gérant les transactions bancaires sont certifiés PCI-DSS.

- **F4 - Protection contre le clonage**

L'application cliente est protégée contre le clonage. Une simple copie de tous les fichiers de l'application sur un autre téléphone ne permettra pas d'usurper l'identité de l'utilisateur.

Dans un tel cas, l'application ne sera plus loguée (Oauth2), et l'utilisateur devra effectuer un processus de reconnexion (décrit dans la partie authentification), et tous les moyens de paiement seront supprimés du compte.

- **F5 - Défense en profondeur**

Afin de limiter l'impact d'une éventuelle attaque, plusieurs mesures sont implémentées dans l'application :

- Détection du root : l'application cliente détecte si le téléphone a été rooté ;
- Protection du code : des mesures sont en place pour compliquer l'analyse du logiciel par reverse engineering ;
- Plusieurs couches de protection pour les données sensibles : les données sensibles sont chiffrées même à l'intérieur des communications SSL/TLS afin de les protéger même en cas d'attaque man in the middle réussie ;
- L'application ne logue aucune information sensible, n'est pas en mode debug, et ne contient pas de fonctionnalités cachées comme des fonctionnalités de test par exemple.

7 MATRICES DE COUVERTURE

Biens sensibles / Menaces	Vol	Malware	Attaque de l'infrastructure	MitM	Rétro-ingénierie
Données d'authentification client	X	X	X	X	X
Données d'auth commerçant	X	X	X	X	X
Interactions client/serveur		X	X	X	
Données utilisateur	X	X	X	X	

Fonctions de sécurité / Menaces	Vol	Malware	Attaque de l'infrastructure	MitM	Rétro-ingénierie
F1 - Authentification	X	X	X	X	
F2 - Protection des échanges		X	X	X	
F3 - Protection des données	X	X	X	X	
F4 - Protection contre le clonage	X	X			
F5 - Défense en profondeur	X	X		X	X