Mobile App Security Recommendations

Standardization Bureau, ITU

Arnold Kibuuka

Mobile Payment App Security Recommendations

DFS Security Recommendations

1. Mobile Application Security Best practices
2. Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling
3. Recommendations to mitigate SS7 vulnerabilities
4. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security

Mobile Payment App Security Best Practices

- Draws upon:
    - GSMA study on mobile money best practices,
    - ENISA smartphone security development guidelines,
    - State Bank of Pakistan mobile payment applications security framework
- Template can be used as input to an app security policy by DFS providers to provide minimum security baselines for app developers and DFS providers as well as setting criteria for verifying compliance of apps

Mobile Payment App Security Best Practices

Considerations:

i. device and application integrity.

ii. communication security and certificate handling.

iii. user authentication.

iv. secure data handling.

v. secure application development.

Mobile Application security best practices.

Le modèle pour la sécurité des applications propose les meilleures pratiques que les régulateurs des services financiers numériques qui pourraient être incluses dans un document de politique de sécurité des applications par les fournisseurs SFN. Le modèle prend strictement en compte l'application mobile sur l'appareil, sauf indication contraire, et les sous-sections décrivant les recommandations traitent de divers aspects de l'opération ou de la politique sous-jacente relative à l'application mobile. L'accent est principalement mis sur les applications Android compte tenu de leur part de marché importante, bien que de nombreuses recommandations soient applicables à tous les systèmes d'exploitation mobiles. Ce modèle est extrait de la section 9 de la Cadre de garantie de la sécurité des services financiers numériques.

1 Lignes directrices relatives aux bonnes pratiques en matière de sécurité des applications d'argent mobile

Nous présentons un modèle de cadre de sécurité pour les applications d'argent mobile, en nous concentrant sur de bonnes pratiques générales et non sur des technologies spécifiques, sauf lorsqu'elles sont explicitement mentionnées. Pour ce modèle, nous nous inspirons de travaux d'analyse récents sur les applications de SFN du point de vue des applications d'argent mobile. Ces travaux incluent l'étude de la Global System Mobile Association (GSMA) sur les bonnes pratiques en matière de sécurité des applications d'argent mobile[1], les lignes directrices de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour le développement sécurisé de smartphones[2], ainsi qu'un cadre de sécurité pour les applications de paiement mobiles élaboré par la Banque d'État du Pakistan[3]. Ce modèle peut également être utilisé par les fournisseurs de SFN pour étayer leur politique en matière de sécurité des applications.

Cette section vise à synthétiser les recommandations afin de fournir aux organismes de réglementation ou aux examinateurs de la sécurité applicative un point de départ pour leurs évaluations de la sécurité. Le modèle porte strictement sur l'application mobile installée sur l'appareil, sauf indication contraire, et les sous-sections décrivant les recommandations traitent de divers aspects de l'exploitation ou de la politique sous-jacente relative à l'application mobile. L'accent est principalement mis sur les applications Android étant donné leur part de marché importante, bien que de nombreuses recommandations s'appliquent à l'ensemble des systèmes d'exploitation mobiles. Bien que la confidentialité constitue également un facteur important, ces recommandations concernent avant tout la sécurité.

1.1 Intégrité des appareils et des applications

i. Les appareils les plus sûrs pour effectuer des transactions financières sont ceux qui n'ont jamais subi de débridage ou de rooting, car il peut être difficile, voire impossible, d'évaluer la sécurité du système d'exploitation sous-jacent s'il a été remplacé ou exploité. Les applications doivent donc utiliser les services de la plate-forme mobile pour déterminer que la plate-forme sous-jacente et elles-mêmes n'ont pas été modifiées.

https://www.sbp.org.pk/psd/2022/C1.htm#:~:text=In%20line%20with%20international%20standards%20and%20best%20practices%2C,payment%20applications%20for%20mobile%20c

بینک دولت پاکستان
State Bank of Pakistan

This plug-in isn't supported

MEDIA CENTRE | HELP DESK

Home | About SBP | Laws & Regulations | Circulars/Notifications | Monetary Policy | Financial Markets | Publications | Economic Data | Fi

Circulars/Notifications - Payment System Department

PSPOD Circular No 01 of 2022 **April 26, 2022**

The Presidents/CEOs
All Banks/ MFBs/ PSOs/ PSPs/ EMIs

Dear Sir/Madam,

Mobile Applications (Apps) Security Guidelines

Mobile payment applications (mobile apps) have become an alternate payment channel for a growing number of users. SBP regulated entities have been offering innovative products and services through mobile applications. Consequently, opportunities for the fraudsters to exploit vulnerabilities in mobile apps and defraud the customers have also increased manifold.

2. In line with international standards and best practices, SBP has developed comprehensive Mobile App Security Guidelines (the "Guidelines") providing baseline security requirements for app owners in order to ensure confidentiality and integrity of customer data and availability of app services in a secure manner, when developing payment applications for mobile or other smart devices.

3. App owners shall use these Guidelines for the architecture, design, development and deployment of mobile payment apps and associated environment that consumers use for digital financial services.

4. App owners shall ensure that their mobile apps and associated infrastructure are compliant with the requirements of these Guidelines latest by December 31, 2022.

Enclosure: Mobile Applications (Apps) Security Guidelines

Yours sincerely,

Sd/-

(Shoukat Bizinjo)
Additional Director

Mobile Application Security best practices

Device and Application Integrity

Use platform services for integrity checks;

remove extraneous code

maintain high-integrity state server-side.

Communication Security and Certificate Handling

Standardized cryptographic libraries; strong,

up-to-date TLS certificates; limit certificate lifetimes (825 days);

contingency for untrusted CA; secure TLS configuration;

certificate pinning; correct server certificate validation.

User Authentication

Disallow easily guessable credentials;

encourage multi-factor authentication;

prefer authenticator apps over SMS for OTPs;

secure storage of biometric information.

Secure Data Handling

Secure storage of confidential info;

trusted hardware for sensitive data;

avoid external storage;

clean caches/memory;

`fine-grained permissions for data sharing;

avoid hard-coding sensitive info;

validate client input for database storage.

Secure Application Development

Adhere to secure coding practices and standards;

provide secure application updates;

regular internal or external code reviews.

Mobile Application Security best practices

Device and Application Integrity

T1.2 Android:debuggable

`T1.4 Dangerous permissions

T8.1 The application should refuse to run on a rooted device

Communication Security and Certificate Handling

T3.1 Application should only use HTTPS connections

T3.2 Application should detect Machine-in-the-Middle attacks with untrusted certificates

T3.3 Application should detect Machine-in-the-Middle attacks with trusted certificates

T3.4 App manifest should not allow clear text traffic

T5.1 The app should not use unsafe crypto primitives

T5.2 The HTTPS connections should be configured according to best practices

T5.3 The app should encrypt sensitive data that is sent over HTTPS

User Authentication

T4.1 Authentication required before accessing sensitive information

T4.2 The application should have an inactivity timeout

T4.3 If a fingerprint is added, authentication with fingerprints should be disabled

T4.4 It should not be possible to replay intercepted requests

Secure Data Handling

T1.1 Android:allowBackup

T1.3 Android:installLocation

T2.1 Android.permission.WRITE_EXTERNAL_STORAGE

T2.2 Disabling screenshots

Secure Application Development

T9.1 The code of the app should be obfuscated

Mobile Application security best practices.

Le modèle pour la sécurité des applications propose les meilleures pratiques que les régulateurs des services financiers numériques qui pourraient être incluses dans un document de politique de sécurité des applications par les fournisseurs SFN. Le modèle prend strictement en compte l'application mobile sur l'appareil, sauf indication contraire, et les sous-sections décrivant les recommandations traitent de divers aspects de l'opération ou de la politique sous-jacente relative à l'application mobile. L'accent est principalement mis sur les applications Android compte tenu de leur part de marché importante, bien que de nombreuses recommandations soient applicables à tous les systèmes d'exploitation mobiles. Ce modèle est extrait de la section 9 de la Cadre de garantie de la sécurité des services financiers numériques.

1 Lignes directrices relatives aux bonnes pratiques en matière de sécurité des applications d'argent mobile

Nous présentons un modèle de cadre de sécurité pour les applications d'argent mobile, en nous concentrant sur de bonnes pratiques générales et non sur des technologies spécifiques, sauf lorsqu'elles sont explicitement mentionnées. Pour ce modèle, nous nous inspirons de travaux d'analyse récents sur les applications de SFN du point de vue des applications d'argent mobile. Ces travaux incluent l'étude de la Global System Mobile Association (GSMA) sur les bonnes pratiques en matière de sécurité des applications d'argent mobile[1], les lignes directrices de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour le développement sécurisé de smartphones[2], ainsi qu'un cadre de sécurité pour les applications de paiement mobiles élaboré par la Banque d'État du Pakistan[3]. Ce modèle peut également être utilisé par les fournisseurs de SFN pour étayer leur politique en matière de sécurité des applications.

Cette section vise à synthétiser les recommandations afin de fournir aux organismes de réglementation ou aux examinateurs de la sécurité applicative un point de départ pour leurs évaluations de la sécurité. Le modèle porte strictement sur l'application mobile installée sur l'appareil, sauf indication contraire, et les sous-sections décrivant les recommandations traitent de divers aspects de l'exploitation ou de la politique sous-jacente relative à l'application mobile. L'accent est principalement mis sur les applications Android étant donné leur part de marché importante, bien que de nombreuses recommandations s'appliquent à l'ensemble des systèmes d'exploitation mobiles. Bien que la confidentialité constitue également un facteur important, ces recommandations concernent avant tout la sécurité.

1.1 Intégrité des appareils et des applications

i. Les appareils les plus sûrs pour effectuer des transactions financières sont ceux qui n'ont jamais subi de débridage ou de rooting, car il peut être difficile, voire impossible, d'évaluer la sécurité du système d'exploitation sous-jacent s'il a été remplacé ou exploité. Les applications doivent donc utiliser les services de la plate-forme mobile pour déterminer que la plate-forme sous-jacente et elles-mêmes n'ont pas été modifiées.

Il convient de supprimer tout code superflu éventuellement ajouté à l'application pendant le développement, comme les fonctionnalités qui ne sont pas conçues pour les plates-formes d'appareils sur lesquelles l'application sera déployée ou les fonctionnalités de développement/débogage, afin de réduire la surface d'attaque du code de production déployé. Côté serveur, il convient de déterminer si l'application s'exécute dans un état d'intégrité élevée grâce à la validation de signature, au hachage sur l'application ou à certains blocs de fonction du programme.

Sécurité des communications et gestion des certificats

Les applications doivent utiliser des bibliothèques cryptographiques normalisées. Pour la communication avec les services internes, elles doivent également appliquer un chiffrement de bout en bout en bout en utilisant des protocoles normalisés, en particulier TLS. La version minimale recommandée du protocole TLS est la version 1.2.
Les certificats TLS ne doivent pas être expirés et doivent présenter des suites de chiffrement robustes, notamment le chiffrement AES-128 et SHA-256 pour le hachage. Nous recommandons l'utilisation de modes d'opération de chiffrement authentifiés tels que le Galois/Counter Mode (GCM).
Il faut limiter la durée de vie des certificats émis à 825 jours, conformément aux bonnes pratiques préconisées par le Certification Authority Browser Forum.
Il convient de vérifier la fiabilité de l'autorité de certification et de prévoir un plan d'urgence si celle-ci n'est plus fiable.
La configuration de TLS doit être effectuée de manière sécurisée et des mesures doivent être prises pour éviter les problèmes de configuration qui pourraient entraîner l'échec de l'authentification ou une mauvaise sélection de l'algorithme.
L'épinglage des certificats est recommandé pour empêcher leur remplacement.
Il convient de s'assurer que les certificats de serveur sont validés correctement au niveau des appareils côté client.

Authentification des utilisateurs

Country level Adoption

- CRASA
- EACO – Now implementation in the member states
- SBS Peru
- State Bank of Pakistan
- Uganda – Drafting stage
- Tanzania – Drafting stage

Countries that have setup the DFS security lab

- Tanzania
- Uganda
- Peru
- Zimbabwe, Rwanda, The Gambia – In Progress

Questions

Contact: dfssecuritylab@itu.int