Mobile Applications (Apps) Security Guidelines

Issued vide PSP&OD Circular No. 01 of 2022

Payment Systems Policy & Oversight Department

Table of Contents

Acronyms

API: Application Programming Interface

EMI(s): Electronic Money Institutions

MFA: Multi Factor Authentication

MMS: Multimedia-Messaging Service

NFC: Near Field Communication

OS: Operating System

PA-DSS: Payment Application Data Security Standard

PCI-DSS: Payment Card Industry Data Security Standard

PII: Personally Identifiable Information

PSO/PSP: Payment Systems Operator/Payment Service Provider

RAM: Random Access Memory

SMS: Short Messaging Service

SRS: System Requirement Specification

SSL: Secure Socket Layer

TLS: Transport Layer Security

USSD: Unstructured Supplementary Services Data

1. Introduction

The prevalence of smartphones and the emergence of broadband internet services in the country has given rise to widespread use of mobile applications (mobile apps) by the end-users because of their intuitive user interface and ease of use. Financial institutions are increasingly offering various services through their mobile apps including payment services, account opening, third-party integrations etc. With the emergence of non-banking players in the payment services industry, the adoption and use of mobile apps is expected to grow manifold.

The convenience, availability and acceptance of mobile app based payment services has phenomenally increased the adoption of these apps by the customers. Data storage, inter-app communication, proper usage of cryptography, Application Programming Interfaces or APIs, and secure network communication are only some of the major areas to consider during mobile app development lifecycle.

The protection of sensitive data and payment transactional information is crucial to mobile app-based payment security. In line with international standards and best practices, SBP aims to provide baseline security requirements for the mobile apps broadly covering the areas of data storage, network communication with endpoints, authentication and authorizations, interaction with mobile platform, code quality and exploit mitigation and anti-tampering etc.

2. Objective

The objective of these "Guidelines" is to provide baseline security requirements for app owners in order to ensure confidentiality and integrity of customer data and availability of services in a secure manner when developing payment applications. App owners shall use these Guidelines for the architecture, design, development and deployment of mobile payment apps and their associated environment that consumers use for payment transactions.

3. Authority

These Guidelines are being issued in exercise of the powers conferred upon SBP under Section 3 and 15 of Payment Systems and Electronic Fund Transfers Act, 2007.

4. Definitions

Wherever used in these Guidelines, the following terms shall have the following meanings:

Account lockout is a method used to prevent password-guessing attacks by locking an account after a predefined number of invalid login attempts.

App Owners are SBP regulated entities; providing a mobile application for customers. App owners include but are not limited to all Financial Institution, authorized Payment Systems Operator/Payment Service Provider (PSO/PSP), Electronic Money Institutions (EMI) and any other licensed/authorized institutions, which are operating, facilitating, or providing digital financial services through mobile apps to consumers

Application Programming Interface (API) is a system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

Authentication is the act of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources.

Authorization is a mechanism to grant access privileges to a user, program, or process or the act of granting those privileges.

Availability is ensuring timely and reliable access to and use of information.
Code Obfuscation is the act of destroying data by cryptographic or other means to hide information.
Confidential customer information shall have the same meaning as defined in SBP's Framework for Risk Management in Outsourcing Arrangements by Financial Institutions as amended from time to time
Minification is the process of removing all unnecessary characters from source code without changing its functionality.
Mobile App is a self-contained computer program designed to execute on a mobile device. The term "app" refers to an application running on any mobile operating systems.
Personally Identifiable Information (PII) shall have the same meaning as defined in SBP's Framework for Risk Management in Outsourcing Arrangements by Financial Institutions as amended from time to time
Privilege Escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally be protected from an application or user.
Sensitive information is the information where the loss, misuse, or unauthorized access to or modification of could adversely affect the app owners or the consumers resulting in financial/data loss

5. Applicability

a) The requirements of these Guidelines shall be applicable on all Financial Institutions, authorized Payment Systems Operators/Payment Service Providers (PSOs/PSPs), Electronic Money Institutions (EMI) and any other SBP regulated/licensed/authorized institutions (hereinafter collectively referred to as 'App owners') which are developing, procuring, operating, facilitating, or providing digital financial services through mobile apps to end users.
b) The requirements of these Guidelines shall cover the entire mobile app ecosystem involved in capturing, storing, processing and transmitting financial/non-financial information, which includes but is not limited to mobile apps, web services, server-side databases, storage and network communications etc.
c) App owners shall be responsible to ensure that their mobile apps and associated infrastructure are aligned with these Guidelines latest by December 31, 2022.

6. General Requirements

a) App owners shall develop a policy governing mobile apps business objectives, standards, compliance, guidelines, controls, responsibilities, and liabilities. App owners may formulate this policy separately or include the same as part of their overall digital channels development policy. As a principle, the policy shall achieve a balance among security of apps, convenience and performance. The policy shall at least be revised annually and/or when a significant change is made in the environment.
b) App owners may develop mobile apps in-house, through outsourcing or by a combined approach. To manage mobile app development projects, app owners shall:
    i.) Put in place necessary app documentation including manuals on development, testing, trainings, production, operational administration, user guides and Service Level Agreements (SLAs).
    ii.) Carry out vulnerability assessment, penetration testing and performance assessment of mobile apps to ensure effective and smooth operation before deploying the same in production environment.

iii.) Carry out system and User Acceptance Testing (UAT) in an environment separate from the production environment.

iv.) Put in place an escrow arrangement in cases where third party vendors develop mobile apps but the source codes are not released to the app owners.

7. Mobile App Security Requirements

A. Mobile Application Architecture

i) App owners shall develop a standard architecture based on prescribed set of security principles, rules, techniques, processes, and patterns to design a secure mobile application.

ii) The entire development of mobile app shall revolve around the architecture principles, which can be updated based on the learnings during the course of development of application layers (or equivalent) and operational usage and consumer feedback.

iii) App owners shall ensure that the mobile payment app architecture is robust and scalable, commensurate with the transaction volumes and customer growth. For this purpose, a robust capacity management plan shall be put in place to meet evolving demand.

B. Device Binding/Registration

i) App owners shall ensure to implement a flexible device registration/binding functionality using multiple properties unique to the device (such as IP address, location, remote server, time of the day, device type, location, PIN code, Wi-Fi information, screen size, browser, etc.) so that only registered devices are allowed to access backend servers.

ii) The device registration/binding shall preferably be implemented using a combination of hardware, software and service information. In case, multiple devices are registered by a user:

a). the user must be notified of every new device registration on the registered mobile number, email or phone call and

b). App owners shall maintain record of all registered devices, providing the user a facility to disable a registered device.

C. User Authentication and Authorization

i) App owners shall ensure that explicit customer consent in a convenient manner is obtained before allowing registration of mobile app.

ii) A login authentication and a risk-based financial-value-based transaction authentication shall be in place.

iii) App owners shall ensure that the initiation of mobile payments, as well as access to sensitive payment and personal data is protected by strong customer authentication mechanism including:

a). Implementation of multi-factor authentication (MFA) for registration of mobile app user-account.

b). Strong and configurable PIN/password/pattern or a biometric credential such as face recognition or fingerprint recognition.

c). Time-based one-time passwords (TOTP) for authentication.

d). OTP auto-fetching functionality

e). Configure maximum number of failed authentication attempts after which access to the mobile payment service is blocked.

f). Define maximum duration for termination of inactive mobile payment service sessions.

g). Ensuring that user authentication shall be processed only at the app owner's server-end.

h). Ensure that authentication attempts are logged and monitored to detect login anomalies and possible breaches.

D. Protection of Sensitive Payment Data and Personal Data

i) App owners shall ensure that sensitive information is not stored in a shared store segment with other apps on mobile devices. It is recommended to utilize only the device internal storage, which is virtually sandboxed per app or preferably in a container app without meddling with other applications or security settings of the mobile devices.

ii) App owners shall ensure that confidential data is deleted from caches and memory after it is used and/or uninstalled. Further, app owners shall ensure that mobile app erase/expire all application-specific sensitive data stored in all temporary and permanent memories of the device during logoff or on unexpected termination of app instance.

iii) Customer credentials and transactional data shall be encrypted while in-transit and at rest using strong, internationally accepted and published standards for key length, algorithms, cipher suites, digital certificates and applicable protocols that are not deprecated/ demonstrated to be insecure/ vulnerable.

iv) Encryption keys shall only be stored with appropriate robust security controls and shall remain in a non-exportable form in a highly secure and standard key store. It may be bound to the secure hardware (e.g. Trusted Execution Environment, Secure Element for Android or its equivalent on any other platform). Further, Key Use Authorization shall be implemented, which should not be changed after generation of keys.

E. Network and Interfacing Security

i) App owners shall ensure to enforce secure communication during the session establishment, exchange of data among apps and backend services (including micro-services).

ii) Transport layer encryption shall be implemented for all communications between the mobile app and app servers.

iii) App owners shall setup their own Trust Manager to avoid accepting every unknown certificate. Mobile apps shall use valid certificates issued by a trusted certificate authority.

iv) Mobile apps shall have inbuilt controls to mitigate bypassing of certificate pinning.

v) Mobile apps shall cease operations until certification errors are properly addressed.

vi) App owners shall ensure that mobile apps must be able to identify new network connections or connections from unsecured networks like unsecured Wi-Fi connections. Appropriate controls shall be implemented for performing transactions under those circumstances.

F. Session Management

i) App owners shall ensure that mobile apps have automatic user-logoff functionality after a configurable idle time-period.

ii) App owners shall ensure that mobile apps have an easy to use and clearly visible logoff method.

iii) App owners shall ensure that mobile app erase/expire all application specific sensitive data stored in all temporary and permanent memories of the device during logoff or on termination of app instance.

iv) App owners shall implement a procedure to centrally disable access to the mobile app servers from devices that are reported lost or stolen. For this purpose, app owners shall put in place a well-defined procedure for customers to report lost or stolen devices.

v) App owners shall ensure that a procedure is in place to detect multiple simultaneous login attempts and immediately communicate it to the concerned user through alternate channels such as callback, SMS, email etc.

G. Tampering Detection

i) App owners shall implement necessary checks on the server-side to verify mobile app integrity and to detect any manipulation.

ii) App owners shall ensure that installation of mobile apps is not allowed on rooted/jail broken devices.

iii) App owners shall ensure that mobile apps are not allowed to run inside a debugger/emulator. For this purpose, mobile apps shall have debugger/emulator detections in place. Further, app owners shall not allow any third party to debug the application during runtime.

H. App Permissions

i) App owners shall ensure to restrict data shared with other applications on the device through fine-grained permissions.

ii) App owners shall ensure to minimize the number of permissions requested by the app and ensure that the permissions correlate to functionality required for the app to work. Mobile app shall defer or relinquish permissions when the same are no longer needed.

iii) Unless for a specific business requirement in accordance with the security architecture principles, app owners shall not allow users to navigate to other apps, sites or view objects that are not trusted and outside of app environment.

I. Secure Coding

i) App owners shall ensure that their mobile app developers adhere to industry accepted secure coding practices and standards.

ii) App owners shall ensure that security libraries offered by mobile operating systems are correctly designed and implemented and that the cipher suites they support are sufficiently strong. Accordingly, app owners shall only use necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.

iii) App owners shall document all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the payment application.

iv) App owners shall have knowledge of all off-the-shelf libraries/modules/components utilized in the development of mobile app.

v) App owners shall ensure that code signing is used for the mobile app to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.

vi) App owners shall ensure that private key used for code signing is generated, securely stored and appropriately backed-up.

vii) App owners shall ensure that minification and source code obfuscation techniques are used in the mobile apps.

viii) App owners shall ensure to review application code prior to release to customers after any significant change, to identify any potential coding vulnerabilities.

ix) App owners shall verify that apps are not vulnerable to common coding vulnerabilities by performing manual or automated penetration testing that specifically attempts to exploit injection flaws, buffer overflow, insecure cryptographic storage, insecure communications and improper error handling etc.

J. Input and Output Handling

i) App owners shall ensure that any input coming from the client that is to be stored in databases is properly validated to avoid SQL injection attacks.
ii) App owners shall ensure that input and output data is properly sanitized and validated at the server and at the client-end.
iii) Auto-complete feature shall be disabled for sensitive information such as login IDs and passwords.
iv) Clipboard/ copy-paste function shall be disabled for sensitive data. App owners may also use in-app keypad/ keyboard to capture the input from users.

K. Error and Exception Handling

i) Mobile apps shall have a proper error-handling mechanism and all errors shall be logged in the server.
ii) Sensitive information and/or hints shall not be disclosed in error/warning messages and notifications.

L. Monitoring, Logs and Data Leakage

i) App owners shall ensure that the app usage behavior is maintained and monitored through automated mechanism and deploy tools to identify any anomaly in the usage and behavior. The mechanism shall integrate with complete process of customer support for verification to clear the anomaly for consumer protection.
ii) App owners shall ensure that mobile app logs does not contain any sensitive data and where essentially required should be masked such that it no longer remains directly constructible in its complete form by collating components.
iii) The logs shall be stored separately from the application/database servers and protected with appropriate access controls.
iv) App owners shall implement appropriate security safeguards to protect the logs from unauthorized modification or destruction.
v) App owners shall ensure that all mobile payments server and the ecosystem logs are available for audits.
vi) App owners shall implement appropriate control to protect transactional data/information against any loss or damage.
vii) Server access controls and audit logs shall be maintained at the server level as per data retention policy or as may be determined by SBP.

M. App Vulnerability Assessment, Patching and Updating

i) App owners shall ensure that the apps have passed through extensive and recursive vulnerability assessment, scan and intrusion tests to identify weaknesses in app through both internal and independent assessors.
ii) App owners shall ensure that the vulnerabilities identified during assessment scans, usage of the app or through independent identifier sources are fixed and updated to respective platform stores.
iii) App owners shall ensure notifying users about update and enforce it within a grace period depending upon the criticality of fixes. The information about fixes shall be published in app release notes.

N. Application Programming Interface (APIs)

In order to establish adequate safeguards to manage the development and provision of APIs for secure delivery of third party provided services through mobile apps, App owners shall implement following measures:

i) Establish security standards for designing and developing secure APIs including measures to protect the API keys or access tokens, which are used to authorize access to APIs to exchange confidential data. App owners shall define and enforce a reasonable timeframe for access token expiry to reduce the risk of unauthorized access.

ii) A well-defined vetting process shall be put in place for assessing the appropriateness of third parties in connecting to the mobile app via APIs, as well as governing third party API access. The vetting criteria shall take into account third party's nature of business, security policy, industry reputation and track record amongst others.

iii) Perform risk assessment before allowing third parties to connect to their systems via APIs, and ensure the security implementation for each API is commensurate with the sensitivity and business criticality of the data being exchanged.

iv) Strong authentication and access control mechanism to authorize and control access to designated API services in order to safeguard customer information

v) Strong encryption standards and key management controls to secure transmission of sensitive data through APIs.

vi) The app owners shall have the ability to log the access sessions by the third party (ies), such as the identity of the third party making the API connections, and the data being accessed by them. App owners shall ensure to perform a robust security screening and testing of the API between the app owners and third party before going live.

vii) Deploy real-time monitoring and alerting capabilities to ensure visibility of the usage and performance of APIs and detect suspicious activities. In the event of a breach, measures shall be in place to promptly revoke API keys or access tokens.

viii) Take steps to handle high volumes of API call requests by legitimate applications, and implement measures to mitigate denial-of-service attacks while ensuring that these measures are commensurate with the criticality and availability requirements of the app.

O. Customer Awareness

i) The app shall have a visible section/tab/module containing necessary legal, regulatory and compliance related information with required disclaimers and acknowledgment of facts (such as relating to the extent of collection, storage, and disposal of data), rights, responsibilities and liabilities of both the customers and provider of the App.

ii) App owners shall ensure to educate and inform customers clearly about how to access, download, securely use and cease to use payment apps within the App interface as well as through official application release channels in order to mitigate the risk of running malware-infected apps.

iii) App owners shall ensure that a robust remedial process of customer support and complaint resolution is defined and implemented to address any security incidence albeit targeted, sectoral or global related to mobile App user(s) or their back end infrastructure.

iv) App owners shall ensure that mobile apps are hosted only at the relevant app platform and shall not be hosted for downloading at app owner's website or the vendor website or any other third-party website.

v) App owners shall undertake active awareness campaigns to educate customer and internal staff about malicious messages, phishing attacks, and spoofing.
vi) All of the above information should be in a structured, clear and understandable form at least both in English and Urdu languages.

***** End *****