Guideline No. 01/2020

Guidelines on Minimum Compliance Standard for Payment Related Mobile Applications

These Guidelines are issued in terms of Section 44 of the Payment and Settlement Systems Act, No. 28 of 2005 (Act), to provide a minimum compliance standard to be adopted by any licensed commercial bank, licensed specialized bank, licensed finance company or licensed operator of a mobile phone based e-money system or any institution, all of which are operating or facilitating or providing payment services for mobile applications (hereinafter referred to as Payment Service Provider (PSP)).

These Guidelines shall cover the entire payment related mobile application eco system including but not limited to mobile applications, web services, server-side infrastructure and network communication. The Boards of Directors of PSPs shall be responsible for ensuring compliance to these Guidelines.

These Guidelines shall replace the Payment and Settlement Systems Guideline No. 01 of 2018 – Guidelines on Minimum Compliance Standard for Payment Related Mobile Applications and shall come into effect from 01.06.2020.

2 Definitions

Wherever used in these guidelines, the following terms shall have the following meanings.

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

Authentication: Authentication is the act of verifying the identity of a user and the user's eligibility to access computerized information.

Authorization: Authorization is the security mechanism used to determine user/client privileges or access levels related to system resources.

Availability: Availability is ensuring timely and reliable access to and use of information.

Certificate Authority: A certificate authority (CA) is a trusted entity that issues digital certificates that verify a digital entity's identity on the Internet.

Licensed Financial Acquirer: Any person who makes arrangements with third parties to accept payment cards of cardholders as a means of payment and reimburses those third parties with the value of the goods or services purchased by the cardholder, and/or who reimburses such third parties for cash advances obtained by the cardholders.

Minification: Minification is the process of removing all unnecessary characters from source code without changing its functionality.

Obfuscation: Obfuscation is the deliberate act of creating obfuscated code, i.e. source or machine code that is difficult for humans to understand.

Privilege Escalation: 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 data: Sensitive data in this context includes customer credentials, bank account numbers and payment card numbers and similar data fields.

Short-lived access token: When a client passes an access token to a server managing a resource, that server can use the information contained in the token to decide whether the client is authorized or not. These tokens have a short lifetime.

Stakeholders: Stakeholders in this context includes PSPs, software vendors, service providers, benefiting merchants and auditors.

Uniform Resource Locator (URL) Manipulation: URL manipulation is the process of altering the parameters in a URL.

3 Policy Formulation

3.1 PSPs shall develop a policy document governing all payment related mobile applications covering business objectives, standards, compliance, guidelines, controls, responsibilities, and liabilities. PSPs shall revise this policy document annually and as and when required.

3.2 This policy document shall be used as a framework when developing all payment related mobile applications and shall be clearly communicated to all stakeholders.

3.3 Policy document shall be approved by the board of directors of the PSP.

4 Documentation

4.1 PSPs shall ensure that all required documentation such as architecture diagram, System Requirement Specification (SRS) document, technical documentation, change management documents, functional and non-functional testing results, security testing, and user signoffs, and other user documentation prepared and maintained by all stakeholders are in accordance with the policy document developed under Section 3 above.

5 Device Registration

5.1 User accounts and mobile devices shall be registered with the PSP using mobile number and a unique device identifier pertaining to the device.

5.2 Devices with or without a mobile number may be allowed to register as secondary devices and these devices shall be authenticated by the primary device or by a call centre person or by a different verification method for which prior approval from the Central Bank of Sri Lanka (CBSL) shall be obtained.

5.3 Each payment related mobile application user account shall be allowed to be used only on mobile devices which are registered with the PSP.

5.4 A login authentication and a financial value-based transaction authentication shall be in place for each payment related mobile application user account.

5.5 Concurrent use of the same account shall not be allowed from multiple devices.

6 Authentication and Password Policy

Following minimum controls and password policies shall be implemented for authentication at the server-end.

6.1 Authentication shall be processed only at the backend except for authentication methods based on biometrics or chip-based authentication.

6.2 Short-lived access tokens shall be implemented to authenticate client requests without transmitting user credentials.

6.3 A suitable password policy shall be implemented in line with the policy document of the PSP.

6.4 Multi Factor Authentication (MFA) shall be implemented with mobile number, device identifier, Password/PIN and identifier specific to the payment related mobile application. Another device identifier shall be used in the place of mobile number in the case of secondary devices without mobile numbers.

6.5 A configurable account lockout function shall be implemented after multiple invalid login attempts. Unlocking of such accounts shall follow standard security procedure of the PSP.

6.6 Authentication attempts shall be logged and monitored to detect login anomalies and possible attacks in real-time. All transactions shall also be monitored for anomalies. Both types of anomalies shall be notified to the user.

6.7 Access to any internal resource shall be properly authenticated.

7 Authorization

Following minimum controls shall be implemented on authorisation.

7.1 Principle of Least Privilege (PoLP) shall always be followed.

7.2 Privilege escalation controls and URL manipulation controls shall be implemented.

8 Session Handling

Following minimum controls shall be implemented on session handling.

8.1 Session ID shall be randomized.

8.2 Payment related mobile application shall have automatic user log off functionality after an idle time period.

8.3 An easy to use and clearly visible log off method shall be implemented.

8.4 During the log off, all application specific sensitive data stored in all temporary and permanent memories of the mobile device shall be erased or marked expired.

8.5 A procedure shall be implemented at the server-side to detect and communicate simultaneous login attempts to the user.

8.6 A procedure shall be implemented to centrally disable the access to the payment related mobile application server from a device reported lost or stolen.

9 Entering and Storing Data

9.1 Payment Card data capturing/storing shall take place only in a Licensed Financial Acquirer's domain or in a mobile application where the mobile application ecosystem is PA-DSS (Payment Application Data Security Standard) and PCI-DSS (Payment Card Industry Data Security Standard) certified.

9.2 Payment related sensitive data except payment card data shall only be captured/stored in an ecosystem approved and regulated by CBSL.

9.3 Sensitive information such as account numbers and customer credentials in temporary storages (E.g. Random Access Memory (RAM), temp files, cache) of the device shall be secured appropriately."

9.4 Sensitive information shall not be stored in the mobile device/s subject to 8.4.

9.5 Data shall be validated and sanitized before being recorded in the databases. Payment related mobile application databases shall be hardened for server-side and client-side.

10 Offline Transactions

10.1 Payment related mobile applications shall not allow offline authorization of transactions and storing transaction data on the device for later transmission unless permitted by CBSL.

11 Cryptography

The following properties shall be used when designing and using cryptographic algorithms in payment related mobile applications.

11.1 Payment related mobile application shall use cryptographic algorithms and iteration counts that are currently not identified as vulnerable, industry-tested and accepted by institutions including but not limited to Federal Financial Institutions Examination Council (FFIEC), American National Standards Institute (ANSI) and National Institute of Standards and Technology (NIST).

11.2 Sensitive data shall be encrypted while in transit and at rest. Payment related mobile application shall use a Salt when generating hashes from passwords.

11.3 Encryption keys shall not be stored in the mobile device without appropriate security controls.

12 Transport Layer Protection

12.1 Transport layer encryption shall be implemented for all communications

12.2 Payment related mobile application shall use valid SSL certificates issued by a trusted certificate authority.

12.3 Certificate pinning shall be properly implemented and used with proper exception handling.

12.4 Controls to mitigate bypassing of certificate pinning shall be implemented.

12.5 Payment related mobile application shall cease operations until SSL certification errors are properly addressed and certification errors shall not be ignored.

12.6 Sensitive data shall be transmitted only through letters, in-app notifications, or email. Only One Time Password (OTP) shall be transmitted using alternate channels such as USSD, SMS, MMS, or other notification channels.

13 Reverse Engineering and Debugging

13.1 Payment related mobile application shall not allow any third-party to debug the application during runtime.

13.2 Minification and source code obfuscation techniques shall be used in the payment related mobile application.

14 Tampering Detection

14.1 The following checks shall be implemented in the server-side to verify the integrity and to detect any manipulation of the client application. These checks can be executed at the start of the payment related mobile application or as appropriate. If any of these checks fail, payment related mobile application shall be disabled.

14.1.1 Hash values/checksums of code blocks, classes, or the whole program.
14.1.2 Validate the size of certain system files or the file modification timestamps.
14.1.3 Verify the signature of the package file at the run time.

14.2 Payment related mobile applications shall not be allowed to be executed on rooted/jail broken devices.

14.3 Debugger detection and emulator detection shall be implemented, and payment related mobile application shall not be allowed to run inside a debugger/emulator.

15 Payment related Mobile Application Permissions

15.1 Payment related mobile application shall acquire only minimum Operating System (OS) permissions required for the application to function properly.

16 Secure Coding

PSPs shall ensure that the following practices are adopted.

16.1 Developers shall adhere to secure coding practices and standards, that are inherent to the coding language used.

16.2 Payment related mobile application shall not use vulnerable/deprecated components, protocols, libraries, scripts etc.

16.3 Implementations of components/protocols/libraries/scripts shall not lead to any vulnerability.

16.4 Payment related mobile application shall be properly patched if any vulnerability is identified.

16.5 Sensitive information such as configuration details shall not be hardcoded in the source code.

17 Input and Output Handling

17.1 All input and output data shall be properly sanitized and validated at the server and at the client.

17.2 Auto complete feature shall be disabled for password/PIN.

18 Error and Exception Handling

18.1 Proper error and exception handling shall be implemented throughout the application.

18.2 Sensitive information and/or hints shall not be disclosed in error/warning messages and notifications.

18.3 Payment related mobile application errors shall be logged in the server.

19 Server-side Infrastructure

19.1 Servers and web services with which the payment related mobile application communicates shall be properly hardened.

19.2 Server access controls and audit logs shall be maintained at the server level.

19.3 Ports and services which are not used by the payment related mobile application shall be disabled.

20 Logs and Data Leakage

Detailed transaction logs shall be maintained in accordance with the following.

20.1 The logs shall be stored in a log server which is segregated from the application/database servers and protected with appropriate access controls.

20.2 The payment related mobile application crash logs shall not be permanently stored in the mobile device and shall be flushed during log in and/or log out processes.

20.3 The payment related mobile application logs shall not contain any sensitive data.

20.4 Security safeguards shall be implemented to protect the logs from unauthorized modification or destruction and only authorized officers shall be provided with access to the logs.

20.5 All related server and ecosystem logs shall be available for audits.

20.6 Logs shall be retained for a certain time period in accordance with the prevailing legal requirements. Adequate measures shall be implemented for the protection of transaction details against any loss or damage.

21 Code Signing of Payment Related Mobile Application

21.1 PSP shall ensure that code signing is used for the payment related mobile application to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.

21.2 The private key used for code signing shall be generated, securely stored, and backed up by the PSP and/or mobile application owner.

21.3 Signing certificate shall be prepared with a strong private key.

22 Hosting

22.1 The payment related mobile application shall be hosted only at the relevant platform and/or store (Google Play Store, Apple App Store, Microsoft Store, Galaxy Store, etc.) and shall not be hosted for downloading at PSP website, the vendor website or any other third party website.

22.2 PSPs shall ensure that all current/potential users are informed by the payment related mobile application owner that the payment related mobile application is only hosted at relevant platform and/or store.

23 Business Continuity Planning

23.1 If third-party vendor/software is used for development, the PSP/mobile application owner shall ensure business continuity through, an escrow arrangement for all versions of the source code or relevant agreements with stakeholders.

23.2 PSPs shall have proper business continuity planning and disaster recovery arrangements to ensure business continuity and agreements with relevant parties for this purpose.

23.3 PSPs shall maintain recovery time objectives (RTO) and recovery point objectives (RPO) for all its payment related mobile application and these mobile applications shall be tested/operated during BCP drills.

24 Change Management

24.1 Details of the system including the Software Development Life Cycle (SDLC) shall be documented properly with change management.

24.2 Payment related mobile application version controlling shall be maintained and documented.

24.3 Change Requests/Change Management procedures shall be followed for all changes in the payment related mobile application.

25 Compliance

25.1 Each PSP shall submit a Compliance Report with the approval of the Board of Directors of PSP to Director, Payments and Settlements Department, CBSL certifying compliance to the Guidelines for each payment related mobile application for which payment services are provided by the PSP prior to the commercial launch of the mobile application. In case of foreign banks, the Head of the Office supervising operations in Sri Lanka shall act in place of the Board of Directors.

25.2 In order to ensure compliance, an information system audit and information security audit for the entire payment related mobile application eco-system including web services, server-side infrastructure and network communication shall be conducted. It is strongly recommended to carry out the audit by an independent third-party auditor, who possesses an adequate capacity for auditing information systems. This audit shall be conducted prior to the commercial launch of the mobile application and thereafter, may be conducted as and when decided by the board of directors of the PSP.

25.3 The scope for audit shall include, but not be limited to, static and dynamic security analysis, source code review for secure controls, backdoors, hardcoded sensitive information, contradictory code etc., production and testing environment reviews and vulnerability assessments and penetration testing reviews.

25.4 Each PSP shall submit a report for the preceding year before 31st January of each year, on payment related mobile applications for which the PSP has provided payment services. This report shall be certified by the board of directors of PSP and shall cover any new versions, patches or updates. In case of foreign banks, the Head of the Office supervising operations in Sri Lanka shall act in place of the Board of Directors.

26 User Awareness

26.1 PSPs shall provide usage and awareness materials for users of payment related mobile applications which may include videos and operational procedural diagrams.

ඩී.ඒ. වි. 29/5/2020

Deputy Governor