Guideline No. : 01/2018

Guidelines on Minimum Compliance Standards 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, finance company or licensed operator of 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 databases, storage and network communication. PSPs shall obtain approval from the Central Bank of Sri Lanka for all payment related mobile applications. These Guidelines shall come in to effect from 18 January 2018.

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.

Certificate Pinning : The client makes a connection to the server and the server responds with its SSL (Secure Socket Layer) certificate. If that certificate was issued by a Certificate Authority that is trusted by the mobile application, then the connection is allowed.

Licensed Financial Acquirer: Any person licensed under the Payment Cards and Mobile Payment Systems Regulations No. 1 of 2013 to make 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.

Sandbox : Sandbox is a security mechanism for separating running programs. It is often used to execute untested or untrusted programs or code.

Sensitive data : Sensitive data in this context includes customer credentials, bank account numbers and payment card numbers and similar 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 may revise this 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.

4. Documentation

4.1. PSPs shall ensure that all required documentation such as architecture diagram, System Requirement Specification (SRS) document, technical documentation 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 regi:tered with the PSP using mobile SIM number and device identifier details including Media Access Control (MAC) address or International Mobile Equipment Identity (IMEI) number.

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

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

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 server end.

6.2. Short-Lived Access Tokens shall be implemented to authenticate client requests without transmitting user credentials.

6.3. Multi Factor Authentication (MFA) shall be implemented with mobile SIM number, device identifier and Password/PIN and identifier specific to the payment related mobile application.

6.4. A configurable strong password policy shall be implemented.

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.

6.7. Access to any internal resource shall be properly authenticated.

7. Authorization

Following minimum controls shall be implemented on authorization;

7.1 Principle of Least Privilege (PoLP) shall be followed at all times.

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 a configurable 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/ expired.

8.5. A procedure shall be implemented to centrally disable the access to the payment related mobile application server from the device reported lost or stolen. A procedure shall be implemented at the server side to detect simultaneous login attempts and communicate it to the user.

9. Entering and Storing Data

9.1. Payment Card data capturing shall be taken 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 shall not be stored in the mobile device.

9.4. Sensitive information in the Random Access Memory (RAM) of the device shall be secured appropriately.

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 it is a paymen made using a stored value card or for transactions 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 Financial industry accepted cryptographic algorithms and cryptographic modes.

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. Hash iteration count shall be in accordance with the financial industry standards.

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

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

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

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

12.6. Sensitive data except One Time Password shall not be transmitted using alternate channels such as USSD, SMS, MMS and notifications.

13. Reverse Engineering and debugging

13.1. Payment related mobile application shall not allow any third-party to debug the application during the 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 are failed 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 time stamps.

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 detections 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 adopt following practices;

16.1. Developers adhere to industry accepted secure coding practices and standards.

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

16.3. Implementation of components/ protocols/ libraries/ scripts do not lead to any vulnerability.

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

16.5. Sensitive information 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 sensitive information.

17.3 Controls shall be implemented to disable the clipboard/ copy-paste function for sensitive data.

18. Error and Exception Handling

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

18.2. Sensitive information and/or hints shall not be disclosed in error/warni ıg 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 payment related mobile application crash logs shall not be stored in the mobi.e device.

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

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

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. Server and the ecosystem logs shall be available for audits.

20.6. Logs shall be retained for a period of six years at a minimum. 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.

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

22. Use of Third-party app stores and hosting at business websites

22.1. The payment related mobile application shall be hosted only at the relevant platform store such as Google Play Store, Apple Store and Windows Store, and shall not be hosted for downloading at PSP website or the vendor website or any other third party website.

22.2. PSPs shall ensure that all users are informed by the payment related mobile application owner that the payment related mobile application is not hosted in third party stores.

23. Business Continuity and Change Management

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

23.2. If third party software is used. the PSP preferably ensures that the payment related mobile application owner has an escrow arrangement for all revised versions of the source code.

23.3. PSPs shall maintain appropriate redundancy and disaster recovery systems.

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

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

24. Audit

24.1. An information system audit and information security audit shall be conducted for the entire payment related mobile application eco-system including web services, the server side databases and storage and network communication by an independent, reputed third-party auditor, who possess adequate capacity for auditing information systems.

24.2. The scope for audit may include, but not limited to, static and dynamic security analysis. source code review, production and testing environment reviews, vulnerability assessments and penetration reviews.

24.3. Information security audit requirements and compliance to these guidelines shall be met for each release of the payment related mobile application before live implementation and shall include all relevant patches and updates.

24.4. All composed audit reports shall contain the details of all members of the audit team including experience. academic and professional qualifications of each audit team member.

C.J.P. Siriwardena
Deputy Governor