भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2020-21/74
DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21 February 18, 2021

The Chairman/ Managing Director/ Chief Executive Officer
All Scheduled Commercial Banks excluding RRBs/
Small Finance Banks/Payments Banks/ Credit Card issuing NBFCs.

Madam/ Dear Sir,

Master Direction on Digital Payment Security Controls

Please refer to para II (7) of the Statement on Developmental and Regulatory Policies of the Bi-monthly Monetary Policy Statement for 2020-21 dated December 4, 2020 (extract given below). The Master Direction provides necessary guidelines for the regulated entities to set up a robust governance structure and implement common minimum standards of security controls for digital payment products and services.

Yours faithfully,

(T.K. Rajan)
Chief General Manager

Digital Payment Security Controls

Going by the pre-eminent role being played by digital payment systems in India, RBI gives highest importance to the security controls around it. Now it is proposed to issue Reserve Bank of India (Digital Payment Security Controls) Directions 2020, for regulated entities to set up a robust governance structure for such systems and implement common minimum standards of security controls for channels like internet, mobile banking, card payments, among others. While the guidelines will be technology and platform agnostic, it will create an enhanced and enabling environment for customers to use digital payment products in more safe and secure manner. Necessary guidelines will be issued separately.

Index

Master Direction on Digital Payment Security Controls

INTRODUCTION

In exercise of the powers conferred by the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934 and Payment and Settlement Systems Act, 2007, the Reserve Bank, being satisfied that it is necessary and expedient in the public interest so to do, hereby, issues the directions hereinafter specified.

CHAPTER – I

PRELIMINARY

1. **Short Title and Commencement**
   a. These directions shall be called the Reserve Bank of India (Digital Payment Security Controls) directions, 2021.

   b. These directions shall come into effect six months from the day they are placed on the official website of the Reserve Bank of India (RBI). However, in respect of instructions already issued either by Department of Payment and Settlement Systems (DPSS), Department of Regulation (DoR) or Department of Supervision (DoS) of RBI including those to select Regulated Entities (REs), by way of circular or advisory, the timeline would be with immediate effect or as per the timelines already prescribed.

2. **Applicability**

The provisions of these directions shall apply to the following Regulated Entities (REs):

a) Scheduled Commercial Banks (excluding Regional Rural Banks);
b) Small Finance Banks;
c) Payments Banks; and
d) Credit card issuing NBFCs.

3. **Definitions**

All expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, Reserve Bank of India Act, 1934, Payment and Settlement Systems Act, 2007 or Information Technology Act, 2000/ Information Technology (Amendment) Act, 2008 and Rules made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

CHAPTER – II

GENERAL CONTROLS

Governance and Management of Security Risks

4. REs shall formulate a policy for digital payment products and services with the approval of their Board. The contours of the policy, while discussing the parameters of any "new product" including its alignment with the overall business strategy and inherent risk of the product, risk management/ mitigation measures, compliance with regulatory instructions, customer experience, etc., should explicitly discuss about payment security requirements from Functionality, Security and Performance (FSP) angles such as:

   a) Necessary controls to protect the confidentiality of customer data and integrity of data and processes associated with the digital product/ services offered;
   b) Availability of requisite infrastructure e.g. human resources, technology, etc. with necessary back up;
   c) Assurance that the payment product is built in a secure manner offering robust performance ensuring safety, consistency and rolled out after necessary testing for achieving desired FSP;
   d) Capacity building and expansion with scalability (to meet the growth for efficient transaction processing);
   e) Minimal customer service disruption with high availability of systems/ channels (to have minimal technical declines);
   f) Efficient and effective dispute resolution mechanism and handling of customer grievance; and
   g) Adequate and appropriate review mechanism followed by swift corrective action, in case any one of the above requirements is hampered or having high potential to get hampered.

   The Board and Senior Management shall be responsible for implementation of this policy. The policy shall be reviewed periodically, at least on a yearly basis. REs may formulate this policy separately for its different digital products or include the same as part of their overall product policy. Further, the policy document should require that every digital payment product/ services offered addresses the mechanics, clear definition of starting point, critical intermittent stages/ points and end point in the digital payment cycle, security aspects, validations till the digital payment is settled, clear pictorial representation of digital path and exception handling. In addition, signing off of the above requirements, mechanism for carrying out User Acceptance Tests (UAT) in multiple stages before roll out, sign off from multiple stakeholders (post UAT) and data archival requirements shall also be taken in to account. The need for an external assessment of the entire process including the logic, build and

security aspects of the application(s) supporting the digital product should be clearly articulated.

5. REs shall incorporate appropriate processes into their governance and risk management programs for identifying, analysing, monitoring and managing the specific risks, including compliance risk and fraud risk, associated with the portfolio of digital payment products and services on a continual basis and in a holistic manner. The Board/ Senior Management of REs shall have appropriate performance monitoring systems/ key performance indicators for assessing whether the product or service offered through digital payment channels meet operational and security norms.

6. As part of this process, the REs shall define product-level limits on the level of acceptable security risk, document specific security objectives and performance criteria including quantitative benchmarks for evaluating the success of the security built into the digital payment product or service, periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner and modify the business plan/ strategy involving the product, when appropriate, based on the security performance of the product or service.

7. REs shall have trained resources with necessary expertise to manage the digital payment infrastructure. Wherever the REs are dependent on third party service providers, adequate oversight and controls for monitoring the activities of the third party personnel, in line with RBI guidelines on outsourcing, shall be put in place.

8. REs shall conduct risk assessments with regard to the safety and security of digital payment products and associated processes and services as well as suitability and appropriateness of the same vis-a-vis the target users, both prior to establishing the service(s) and regularly thereafter. The risk assessment should take into account –

    a) The technology stack and solutions used;
    b) Known vulnerabilities at each of the touchpoints of the digital product and the remedial action taken by the entity;
    c) Dependence on third party service providers and oversight over such providers;
    d) Risk arising out of integration of digital payment platform with other systems both internal and external to the RE, including core systems and systems of payment systems operators, etc.;
    e) The customer experience, convenience and technology adoption required to use such products;
    f) Reconciliation process;
    g) Interoperability aspects;
    h) Data storage, security and privacy protection as per extant laws/ instructions;

i) Operational risk including fraud risk;
j) Business continuity and service availability;
k) Compliance with extant cyber security requirements; and
l) Compatibility aspects.

Such assessment shall cover the surrounding ecosystem as well. The assessment of risks shall address the need to protect and secure payment data[1] and evaluate the resilience of systems. The internal Risk and Control Self-Assessment (RCSA) exercise shall cover the risks (inherent) & controls vis-à-vis the probability and impact of threats to arrive at residual risk. In such an exercise, it is imperative for REs to maintain database of all systems and applications storing customer data in the payment ecosystem and compliance with applicable PCI standards in each of the systems (notwithstanding mandatory requirements of certification/ standard accreditation).

9. REs shall evaluate the risks associated with the chosen technology platforms, application architecture, both on the server and client side. Further, REs should undertake a review of the risk scenarios and existing security measures based on incidents affecting their services, before any major change to the infrastructure or procedures is made or, when, any new threats are identified through risk monitoring activities. Further, unused or unwanted features of the platform should be closely controlled to minimise risk.

10. REs shall develop sound internal control systems and take into account the operational risk before offering digital payment products and related services. This would include ensuring that adequate safeguards are in place to protect integrity of data, customer confidentiality and security of data.

11. REs shall ensure that the digital payment architecture is robust and scalable, commensurate with the transaction volumes and customer growth. The IT strategy of the RE shall ensure that a robust capacity management plan is in place to meet evolving demand. REs shall also put in place review mechanism of IT/ IT Security architecture and technology platform overhaul on a periodic basis based on Board-approved policy.

12. REs shall have necessary capacity, systems and procedures in place to periodically test the backed-up data, application pertaining to digital products to ensure recovery

[1] customer data; customer and beneficiary account details; payment credentials; transaction data;

without loss of transactions or audit-trails. These facilities should be tested at least on a half-yearly basis for digital payment products and services.

Other Generic Security Controls

13. The communication protocol in the digital payment channels (especially over Internet) shall adhere to a secure standard. An appropriate level of encryption and security shall be implemented in the digital payment ecosystem.
14. Web applications providing the digital payment products and services should not store sensitive information in HTML hidden fields, cookies, or any other client-side storage to avoid any compromise in the integrity of the data.
15. REs shall implement Web Application Firewall (WAF) solution and DDoS mitigation techniques to secure the digital payment products and services offered over Internet.
16. The key length (for symmetric/ asymmetric encryption, hashing), algorithms (for encryption, signing, exchange of keys, creation of message digest, random number generators), cipher suites, digital certificates and applicable protocols used in transmission channels, processing of data, authentication purpose, shall be strong, adopting internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls are in general, compliant with extant instructions and the law of the land.
17. REs shall renew their digital certificates used in digital payment ecosystem well in time.
18. The mobile application[2] and internet banking application should have effective logging and monitoring capabilities to track user activity, security changes and identify anomalous behaviour and transactions.

Application Security Life Cycle (ASLC)

19. REs shall implement multi-tier application architecture, segregating application, database and presentation layer in the digital payment products and services.
20. REs shall follow a 'secure by design' approach in the development of digital payment products and services. REs shall ensure that digital payment applications are inherently more secure by embedding security within their development lifecycle.

[2] Mobile banking, mobile payment applications of the regulated entities

21. REs shall explicitly define security objectives (including protection of customer information/ data) during (a) requirements gathering, (b) designing, (c) development, (d) testing including source code review, (e) implementation, maintenance & monitoring and (f) decommissioning phases of the digital payment applications.

22. REs (including those partnering with other entities to co-brand/ co-develop applications) shall adopt and incorporate a threat modelling approach during application lifecycle management into their policies, processes, guidelines and procedures.

23. For digital payment applications that are licensed by a third party vendor, REs shall have an escrow arrangement for the source code for ensuring continuity of services in case the vendor defaults or is unable to provide services.

24. REs shall conduct security testing including review of source code, Vulnerability Assessment (VA) and Penetration Testing (PT) of their digital payment applications to assure that the application is secure for putting through transactions while preserving confidentiality and integrity of the data that is stored and transmitted. Such testing should invariably cover compliance with various standards like OWASP. If the source code is not owned by the RE, then, in such cases, the RE shall obtain a certificate from the application developer stating that the application is free of known vulnerabilities, malwares and any covert channels in the code. In this context,

    a) The VA shall be conducted at least on a half-yearly basis; PT shall be conducted at least on a yearly basis. In addition, VA/PT shall be conducted as and when any new IT Infrastructure or digital payment application is introduced or when any major change is performed in application or infrastructure;
    b) Testing related to review of source code/ certification shall be conducted/ obtained. This shall continue on a yearly basis, if changes/ upgrades have been made to the application during the year;
    c) Testing/ Certification should broadly address the objective that the product/ version/module(s) functions only in a manner that it is intended to do, is developed as per the best secure design/ coding practices and standards, addressing known flaws/threats due to insecure coding; and
    d) Penal provisions shall be included by the RE into third-party contractual arrangements for any non-compliance by the application provider.

25. REs may also run automated VA scanning tools to automatically scan all systems on the network that are critical, public facing or store customer sensitive data on a continuous/ more frequent basis.

26. REs shall compare the results from earlier vulnerability scans to verify/ ascertain that vulnerabilities are addressed either by patching, implementing a compensating control, or documenting and accepting the residual risk with necessary approval and that there is no recurrence of the known vulnerabilities. The identified vulnerabilities should be fixed in a time-bound manner.
27. REs shall ensure that all vulnerability scanning is performed in authenticated mode either with agents running locally on the system to analyse the security configuration or with remote scanners that are given administrative rights on the system being tested.[3]
28. REs shall verify and thoroughly test the functionality (to validate whether the system meets the functional requirements/ specifications) and security controls of payment products and services before its launch/ moving to the production environment.
29. REs shall institute a mechanism to actively monitor for the non-genuine/ unauthorised/ malicious applications (with similar name/ features) on popular app-stores and the Web and respond accordingly to bring them down.
30. The server at the RE's end should have adequate checks and balances to ensure that no transaction is carried out through non-genuine/ unauthorised digital payment products/ applications and the authentication process is robust, secure and centralised.
31. The security controls for digital payment applications must focus on how these applications handle, store and protect payment data. The APIs for secure data storage and communication have to be implemented and used correctly in order to be effective. REs shall refer to standards such as OWASP-MASVS, OWASP-ASVS and other relevant OWASP standards, security and data protection guidelines in ISO 12812, threat catalogues and guides developed by NIST (including for Bluetooth and LTE security), for application security and other protection measures. Such testing has to necessarily verify for vulnerabilities including, but not limited to OWASP/ OWASP Mobile Top 10, application security guidelines/ requirements developed/ shared by operating system providers/ OEMs.
32. REs shall redact/ mask customer information such as account numbers/ card numbers/ other sensitive information when transmitted via SMS/ e-mails.

[3] SANS Critical Security Controls

Authentication Framework

33. In view of the proliferation of cyber-attacks and their potential consequences, REs should implement, except where explicitly permitted/ relaxed, multi-factor authentication for payments through electronic modes and fund transfers, including cash withdrawals from ATMs/ micro-ATMs/ business correspondents, through digital payment applications. At least one of the authentication methodologies should be generally dynamic or non-replicable. [e.g., Use of One Time Password, mobile devices (device binding and SIM), biometric/ PKI/ hardware tokens, EMV chip card (for Card Present Transactions) with server-side verification could be termed either in dynamic or non-replicable methodologies.].

34. REs may also adopt adaptive authentication to select the right authentication factors depending on risk assessment, user risk profile and behaviour. Properly designed and implemented multi-factor authentication methods are more reliable and stronger fraud deterrents and are more difficult to compromise. The key objectives of multi-factor authentication are to protect the confidentiality of payment data as well as enhance confidence in digital payment by combating various cyber-attack mechanisms like phishing, keylogging, spyware/ malware and other internet-based frauds targeted at REs and their customers. In this regard,

    a) The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the RE's digital payment products and services. The risk should be evaluated in light of the type of customer (e.g., retail/ corporate/ commercial); the customer transactional requirements/ pattern (e.g., bill payment, fund transfer), the sensitivity of customer information and the volume, value of transactions involved.

    b) Beyond the technology factor, the success of a particular authentication method depends on appropriate policies, procedures, and controls. An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, customer profile, location, transaction, etc., and interoperability with other systems.

    c) To enhance online processing security, multi factor authentication and alerts (like SMS, e-mail, etc.) should be applied in respect of all payment transactions (including debits and credits), creation of new account linkages (addition/ modification/ deletion of beneficiaries), changing account details or revision to fund transfer limits. In devising these security features, REs should take into account their efficacy and differing customer preferences for additional online protection.

    d) The alerts and OTPs received by the customer for online transactions shall identify the merchant name, wherever applicable, rather than the payment aggregator through which the transaction was effected.

e) As an integral part of the multi factor authentication architecture, REs should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack. This is to ensure, among other things, that the data in transit is secured and the transactions are authenticated only by genuine/ authorised source/ process.

f) An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference or in case the customer closes the application, the session should be terminated, and the affected transactions resolved or reversed out. The customer should be promptly notified about the status of the transaction by email, SMS or through other means.

35. REs should set down the maximum number of failed log-in or authentication attempts after which access to the digital payment product/ service is blocked. They should have a secure procedure in place to re-activate the access to blocked product/ service. The customer shall be notified for failed log-in or authentication attempts.

Fraud Risk Management

36. The REs shall document and implement the configuration aspects for identifying suspicious transactional behaviour in respect of rules, preventive, detective types of controls, mechanism to alert the customers in case of failed authentication, time frame for the same, etc.

37. System alerts shall be parameterised and monitored in terms of various applicable parameters. Such parameters, as applicable could be: transaction velocity (e.g., fund transfers, cash withdrawals, payments through electronic modes, adding new beneficiaries, etc.) in a short period, more so in the accounts of customers who've never used mobile app/ internet banking/ card ever (depending upon the type of payment channel), high risk merchant category codes (MCC) parameters, counterfeit card parameters (String of Invalid CVV/ PINs indicates an account generation attack), new account parameters (excessive activity on a new account), time zones, geo-locations, IP address origin (in respect of unusual patterns, prohibited zones/ rogue IPs), behavioural biometrics, transaction origination from point of compromise, transactions to mobile wallets/ mobile numbers/ VPAs on whom vishing fraud or other types of fraud is/are registered/ recorded, declined transactions, transactions with no approval code, etc.

38. Fraud analysis shall be conducted to identify the reason for fraud occurrence and determine mechanism to prevent such frauds.

39. The staff, especially in the fraud control function, shall be educated about frauds and trained in the following skills and areas of expertise:

    a) Fraud control tools and their usage;
    b) Investigative techniques and procedures;
    c) Cardholder and merchant education techniques to prevent fraud;
    d) Scheme/ Card operating regulations;
    e) Data processing and analysis and liaising or communicating with law enforcement agencies; and
    f) The requisite skills required to (i) set and update appropriate rules, (ii) monitor the exceptions thrown based on the rules on a continuous basis and take necessary actions promptly, (iii) communicate/ escalate wherever required to appropriate authorities, and (iv) differentiate false positives from the rest.

40. REs shall maintain updated contact details of service providers, intermediaries, external agencies and other stakeholders (including other REs) for coordination in incident response. REs shall put in place a mechanism with the stakeholders to update and verify such contact details. REs shall also formulate specific SOPs to handle incidents related to payment ecosystem to mitigate the loss either to the customer or RE.

Reconciliation Mechanism

41. A real time/ near-real time (not later than 24 hours from the time of receipt of settlement file(s)) reconciliation framework for all digital payment transactions between RE and all other stakeholders such as payment system operators, business correspondents, card networks, payment system processors, payment aggregators, payment gateways, third party technology service providers, other participants, etc., shall be put in place for better detection and prevention of suspicious transactions. A mechanism shall be introduced to monitor the implementation and effectiveness of such framework.

Customer Protection, Awareness and Grievance Redressal Mechanism

42. REs shall incorporate secure, safe and responsible usage guidelines and training materials for end users within the digital payment applications. They shall also make it mandatory (i.e. not providing any option to circumvent/ avoid the material) for the consumer to go through secure usage guidelines (even in the consumer's preferred language) while obtaining and recording confirmation during the on-boarding

procedure in the first instance and first use after each update of the digital payment application or after major updates to secure and safe usage guidelines.

43. REs shall mention/ incorporate a section on the digital payment application clearly specifying the process and procedure (with forms/ contact information, etc.) to lodge consumer grievances. A mechanism to keep this information periodically updated shall also be put in place. The reporting facility on the application shall provide an option for registering a grievance. Customer dispute handling, reporting and resolution procedures, including the expected timelines for the RE's response should be clearly defined.

44. REs shall adhere to extant instructions[4], updated from time to time, to put in place system/s for online dispute resolution for resolving disputes and grievances of customers pertaining to digital payments.

45. REs shall educate customers about the need to maintain the physical and logical security of their devices accessing digital payment products and services including recommending secure/ regular installation of operating system and application updates, downloading applications only from authorised sources, having anti-malware/ anti-virus applications on devices, etc.

46. REs shall ensure that its customers are provided information about the risks, benefits and liabilities of using digital payment products and its related services before they subscribe to them. Customers shall also be informed clearly and precisely on their rights, obligations and responsibilities on matters relating to digital payments, and, any problems that may arise from its service unavailability, processing errors and security breaches. The terms and conditions including customer privacy and security policy applying to digital payment products and services shall be readily available to customers within the product. All digital channels are to be offered on express willingness of customers and shall not be bundled without their knowledge.

47. Whenever new operating features or functions, particularly those relating to security, integrity and authentication, are introduced to online delivery channels,

[4] RBI/2020-21/21 DPSS.CO.PD No.116/02.12.004/2020-21 circular dated August 6, 2020 on 'Online Dispute Resolution (ODR) System for Digital Payments'

clear and effective communication followed by sufficient instructions to properly utilise such new features should be provided to the customers.

48. REs may continuously create public awareness on the types of threats and attacks used against the consumers while using digital payment products and precautionary measures to safeguard against the same. Customers shall be cautioned against commonly known threats in recent times like phishing, vishing, reverse-phishing, remote access of mobile devices and educated to secure and safeguard their account details, credentials, PIN, card details, devices, etc.

49. REs shall provide digital payment products and services, to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions.

50. REs should provide a mechanism on their mobile and internet banking application for their customers to, with necessary authentication, identify/ mark a transaction as fraudulent for seamless and immediate notification to his RE. On such notification by the customer, the REs may endeavour to build the capability for seamless/ instant reporting of fraudulent transactions to the corresponding beneficiary/ counterparty's RE; vice-versa have mechanism to receive such fraudulent transactions reported from other REs. The objective of this mechanism is to accelerate early detection and enable the banking/ payment system to trace the transaction trail and mitigate the loss to the defrauded customer at the earliest possible time.

Chapter III

INTERNET BANKING SECURITY CONTROLS

In addition to the controls prescribed in Chapter II, the following instructions are applicable to REs offering/ intending to offer internet banking facility to their customers:

51. Internet banking websites are vulnerable to authentication related brute force attacks/ application layer Denial of Service (DoS) attacks. Based on the RE's individual risk/ vulnerability assessment on authentication-related attacks such as brute force/ DoS attacks, REs shall implement additional levels of authentication to internet banking website such as adaptive authentication, strong CAPTCHA (preferably with anti-bot features) with server-side validation, etc., in order to plug this vulnerability and prevent its exploitation. Appropriate measures shall be taken to prevent DNS cache poisoning attacks and for secure handling of cookies. Virtual keyboard option should be made available.

52. An online session shall be automatically terminated after a fixed period of inactivity.

53. Secure delivery of password for login purpose shall be ensured. The password generated and dispatched by the RE should be valid for a limited period from the date of its creation. If the password is generated and dispatched by the RE, then, the user shall be compulsorily required to change the password, on the first login.

54. When the internet banking application is accessed through external websites (eg: in case of payment of taxes, e-commerce transactions, etc.), the procedure for authentication and the appearance/ look and feel of the RE's internet banking site should be made uniform as far as possible.

Chapter IV

MOBILE PAYMENTS APPLICATION SECURITY CONTROLS

In addition to the controls prescribed in Chapter II, the following instructions are applicable to the REs offering/ intending to offer mobile banking/ mobile payments facility to their customers through mobile application:

55. On detection of any anomalies or exceptions for which the mobile application was not programmed, the customer shall be directed to remove the current copy/ instance of the application and proceed with installation of a new copy/ instance of the application. REs shall be able to verify the version of the mobile application before the transactions are enabled.

56. Specific Controls for mobile applications include:

    a) Device policy enforcement (allowing app installation/ execution after baseline requirements are met);
    b) Application secure download/ install;
    c) Deactivating older application versions in a phased but time bound manner (not exceeding six months from the date of release of newer version) i.e., maintaining only one version (excluding the overlap period while phasing out older version) of the mobile application on a platform/ operating system;
    d) Storage of customer data;
    e) Device or application encryption;
    f) Ensuring minimal data collection/ app permissions;
    g) Application sandbox/ containerisation;
    h) Ability to identify remote access applications (to the extent possible) and prohibit login access to the mobile application, as a matter of precaution; and
    i) Code obfuscation.

57. REs may consider to perform validation on the security and compatibility condition of the device/ operating system and the mobile application to ensure that activities relating to the account are put through the mobile application in a safe and secure manner.

58. REs may explore the feasibility of implementing a code that checks if the device is rooted/ jailbroken prior to the installation of the mobile application and disallow the mobile application to install/ function if the phone is rooted/ jailbroken.

59. Checksum of current active version of application shall be hosted on public platform so that users can verify the same.

60. REs shall ensure device binding of mobile application[5].

61. Considering that the additional factor of authentication and mobile application may reside on the same mobile device in the case of mobile banking, mobile payments, REs may consider implementing alternatives to SMS-based OTP authentication mechanisms.

62. The mobile application should require re-authentication whenever the device or application remains unused for a designated period and each time the user launches the application. Applications must be able to identify new network connections or connections from unsecured networks like unsecured Wi-Fi connections and must implement appropriate authentication/ checks/ measures to perform transactions under those circumstances.

63. The mobile application should not store/ retain sensitive personal/ consumer authentication information such as user IDs, passwords, keys, hashes, hard coded references on the device and the application should securely wipe any sensitive customer information from memory when the customer/ user exits the application.

64. REs shall ensure that their mobile application limit the writing of sensitive information into 'temp' files. The sensitive information written in such files must be suitably encrypted/ masked/ hashed and stored securely.

65. REs may consider designing anti-malware capabilities into their mobile applications.

66. REs shall ensure that the usage of raw (visible) SQL queries in mobile applications to fetch or update data from databases is avoided. Mobile applications should be secured from SQL injection type of vulnerabilities. Sensitive information should be written to the database in an encrypted form. Web content, as part of the mobile application's layout, should not be loaded if errors are detected during SSL/ TLS negotiation. Certificate errors on account of the certificate not being signed by a recognised certificate authority; expiry/ revocation of the certificate must be displayed to the user.

[5] The device binding should be preferably implemented through a combination of hardware, software and service information. In case, the RE allows multiple devices to be registered, then, (a) the user must be notified of every new device registration on multiple channels such as registered mobile number, email or phone call and (b) in relation to the mobile application, RE must maintain a record of all registered devices, providing the user a facility to disable a registered device.

Chapter V

CARD PAYMENTS SECURITY

In addition to the controls prescribed in Chapter II, the following instructions are applicable to the REs offering/ intending to issue cards (credit/ debit/ prepaid) (physical or virtual) to their customers:

67. REs shall follow various payment card standards (over and above PCI-DSS and PA-DSS[6]) as per Payment Card Industry (PCI) prescriptions for comprehensive payment card security as per applicability/ readiness of updated versions of the standards such as –

    a) PCI-PIN (secure management, processing, and transmission of personal identification number (PIN) data);
    b) PCI-PTS (security approval framework addresses the logical and/ or physical protection of cardholder and other sensitive data at point of interaction (POI) devices and hardware security modules (HSMs);
    c) PCI-HSM (securing cardholder-authentication applications and processes including key generation, key injection, PIN verification, secure encryption algorithm, etc.); and
    d) PCI-P2PE (security standard that requires payment card information to be encrypted instantly upon its initial swipe and then securely transferred directly to the payment processor).

68. REs should ensure that terminals installed at the merchants for capturing card details for payments or otherwise are validated against the PCI-P2PE program to use PCI-approved P2PE solutions; PoS terminals with PIN entry installed at the merchants for capturing card payments (including the double swipe terminals) are approved by the PCI-PTS program.

69. Acquirers shall secure their card payment infrastructure (Unique Key Per Terminal – UKPT or Derived Unique Key Per Transaction – DUKPT/ Terminal Line Encryption – TLE).

70. The security controls to be implemented at HSM are:

    a) The HSMs should have logging enabled, the logs must themselves be tamper proof;
    b) HSM can become a single point of failure. This needs to be mitigated by 'clustering' for high availability and ensure secure backups;
    c) Access to the HSM should be controlled through Access Control Lists (ACLs);
    d) Separate ACLs should be maintained for each individual application to ensure application level isolation;
    e) All access to HSM should be managed and monitored using a robust Privileged Identity and Access Management solution;
    f) Decryption and validation of keys, PIN should be done at HSM;

[6] PCI Secure Software Standard, a PCI standard within PCI Software Security Framework (SSF) will replace PA-DSS as the primary standard for securing payment software in 2022. (ref: PCI security standards website)

g) Card PIN generation and printing should be directly at system connected HSM;
h) CVV generation and validation should be done at HSM;
i) Ensure HSM is implemented with secure PIN block format with controls to disable outputting PIN block in weaker format;
j) Secure key management for HSMs (such as LMKs, etc.); and
k) Security of the physical keys of the HSM device should be properly maintained.

71. REs shall implement the following for improving the security posture of the ATM:

a) Implement security measures such as BIOS password, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other softwares, terminal security solution, time-based admin access, etc;
b) Implement anti-skimming and whitelisting solution; and
c) Upgrade all the ATMs with supported versions of operating system. Use of ATMs that have unsupported operating systems shall be prohibited.

72. REs shall ensure robust surveillance/ monitoring of card transactions (especially overseas cash withdrawals) and setting up of rules and limits commensurate with their risk appetites. REs shall take up with the card network and/ or ATM network as the case may be, to put in place transaction limits at Card, BIN as well as at the RE level. Such limits shall be mandatorily set at the card network switch itself. Limits could be mandated both for domestic as well as international transactions separately. REs shall put in place transaction control mechanisms with necessary caps (restrictions on transactions), if any of the limits set as per the above requirement is breached. A periodic review mechanism of such limits set as per the risk appetite of the RE shall be put in place as per the Board-approved policy. REs shall institute a mechanism to monitor breaches, if any, on a 24x7 basis, including weekends, long holidays and put in place a robust incident response mechanism to mitigate the fraud loss, on account of suspicious transactions, if any. REs shall ensure that card details of the customers are not stored in plain text at the RE and its vendor(s) locations, systems and applications. REs shall also ensure that the processing of card details in readable format is performed in a secure manner to strictly avoid data leakage of sensitive customer information.

73. REs that use card data scanning tools to identify unencrypted (clear text) payments card data in their ecosystem especially during audits shall adhere to the following safety measures:

a) Any tool (procured by/ from a third-party) for the purpose of scanning of unencrypted card data should first be tested in a test environment to understand the scope and impact of the tool’s capabilities;
b) The scanning tool should be installed only in the RE's premises on their devices;
c) Card data scanning should not be done remotely;

d) The discovered data, if any, must preferably reside in the scanning tool. Exportable card data must be appropriately masked. (No data, even masked, must be taken out of the RE's premises/ infrastructure); and
e) Limited access to service providers to conduct the scan or analyse the data, if at all, must be provided only on the RE's devices.

Acronyms

ACL	Access Control List
ASLC	Application Security Life Cycle
ATM	Automated Teller Machine
BIN	Bank Identification Number
BIOS	Basic Input/ Output System
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CVV	Card Verification Value
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DoR	Department of Regulation
DoS	Department of Supervision
DPSS	Department of Payment and Settlement Systems
DUKPT	Derived Unique Key per Transaction
EMV	Europay, Mastercard, and Visa
FSP	Functionality, Security and Performance
HSM	Hardware Security Module
HTML	HyperText Markup Language
IP	Internet Protocol
IT	Information Technology
IVR	Interactive Voice Response
LMK	Local Master Key
MCC	Merchant Category Code
MITB	Man-in-The Browser attack
MITM	Man-In-the-Middle attack
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OTP	One Time Password
OWASP	Open Web Application Security Project
OWASP-ASVS	Open Web Application Security Project – Application Security Verification Standard
OWASP-MASVS	Open Web Application Security Project – Mobile Application Security Verification Standard
PA-DSS	Payment Application Data Security Standard

PCI	Payment Card Industry
PCI-DSS	Payment Card Industry-Data Security Standard
PCI-HSM	Payment Card Industry-Hardware Security Module
PCI-P2PE	Payment Card Industry-Point to Point Encryption
PCI-PTS	Payment Card Industry-PIN Transaction Security
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PoS	Point of Sale
PT	Penetration Testing
RBI	Reserve Bank of India
RCSA	Risk Control Self-Assessment
REs	Regulated Entities
SIM	Subscriber Identification Module
SOP	Standard Operating Procedure
SQL	Structured Query Language
SSL	Secure Socket Layer
TLE	Terminal Line Encryption
TLS	Transport Layer Security
UAT	User Acceptance Test
UKPT	Unique Key Per terminal
USB	Universal Serial Bus
VA	Vulnerability Assessment
VPA	Virtual Payment Address
WAF	Web Application Firewall