**Functional / Technical Specifications**

Functional / Technical Specifications: The proposed Mobile Banking solution should have capability of performing the following functions:

|  |  |
| --- | --- |
| **Sr. No.** | **Features and Details** |
|  | **Mobile Banking application platform** |
| 1. | a) Android |
| 2. | b) Windows |
| 3. | c) iPhone/iOS |
| 4. | d) RIM (Blackberry) |
| 5. | e) JAVA (J2ME) |
| 6. | f) NUUP/USSD |
| 7. | g) WAP |
| 8. | h) Symbian |
| 9. | i) Brew |
| 10. | j) Low end handsets |
| 11. | k) Tablet |
| 12. | l) Any other platform to be specified |
|  | **Mode of communication** |
| 13. | a) GSM |
| 14. | b) SMS |
| 15. | c) CDMA |
|  | **Type of Mobile Banking** |
| 16. | a) Mobile Banking |
| 17. | b) SMS Banking |
| 18. | c) NUUP-USSD |
| 19. | d) WAP |
| 20. | e) Browser Based |
| 21. | f) Any other type to be specified |
|  | **Integration with existing systems** |
| 22. | a) Core Banking solution (Finacle, current version 7.0.25) |
| 23. | b) ATM switch (Base 24) |
| 24. | c) Internet Banking |
| 25. | d) SMS Gateway |
|  | **Mobile Banking Interface** |
| 26. | a) Message format ISO 8583 |
| 27. | b) Socket connection |
| 28. | c) Web services/XML over HTTP/HTTPS |
| 29. | d) SFTP, etc. |
|  | Integration with third party service  providers/software/middleware. |
| 30. | a) National Payments Corporation of India (NPCI) for  Immediate Payment Services (IMPS) transactions. |
| 31. | b) National Payments Corporation of India (NPCI) for  NUUP-USSD based mobile banking and transactions. |
| 32. | c) Tie-up with third party service providers for Utility bill  payment/m-commerce/value added services. |
| 33. | d) Integration with any other specified Regulatory /  Statutory bodies for data submission and monitoring. |
| 34. | e) Details of the third party software/middleware interfaced with the proposed application   Name and nature such third party software /  middleware interfaced   Type of interface and details of API’s to support  communication.   Techniques with which the third party application can be interfaced with the proposed solution. |
|  | Mobile Banking application functionality |
| 35. | Account information |
| 36. | a) Account Balance Enquiry |
| 37. | b) Statement of Account |
| 38. | c) Monitor Term deposit accounts |
| 39. | d) Access to loan account statement |
| 40. | e) Access to credit card statement |
| 41. | f) Mutual fund / Insurance statement |
| 42. | g) Access to Demat statement |
| 43. | Transaction |
| 44. | a) Fund transfer within Bank linked / third party account |
| 45. | b) IMPS fund transfer with MMID / Account & IFSC based  (P2A/P2P), P2M etc. |
| 46. | c) NEFT fund transfer |
| 47. | d) Mobile / DTH / Data Card Recharge |
| 48. | e) M-Commerce (Bill payment, Airline / Movie ticketing,  Restaurant reservation and Payment) |
| 49. | Support / Request Services |
| 50. | a) Creation of Recurring Deposit / Fixed Deposit |
| 51. | b) Request for ATM Debit card |
| 52. | c) Request for Internet Banking (Registration / Password  Re-generation) |
| 53. | d) Request for TDS statement |
| 54. | e) Purchase Gift card / Travel card |
| 55. | f) Status of Cheque |
| 56. | g) Request for Cheque book |
| 57. | h) Block debit card |
| 58. | i) ATM / Branch Search with map |
| 59. | j) E-lobby / Multi-Function kiosk search with map |
| 60. | k) Reminders on schedule bill payments |
| 61. | l) View status of fund transfer |
| 62. | m) Aadhar (UID) Seeding through the application / USSD  channel |
| 63. | Content based services |
| 64. | a) Geo-location based Push / Notification Services |
| 65. | b) Geo-location based services for Bank’s nearby service  outlet. |
| 66. | c) Application capability to allow customer to tag the  locations / preferences as per his/her preference. |
| 67. | d) Ability to push notifications for Merchant Discount  Offers/Redemption of Coupons |
| 68. | e) IFSC search / lookup |
| 69. | Personalization |
| 70. | a) Application support for customer preferred language |
| 71. | b) Application support for Theme / Skin personalization |
| 72. | c) Customer personalized date / time format |
| 73. | d) Customer personalized amount format |
| 74. | e) Color coding for debit and credit figures in statement. |
| 75. | f) Customer originated grouping of default transactions |
| 76. | g) Customer personalized default beneficiary list |
| 77. | h) Application support for multiple languages, primarily  multilingual and support advertisement of banking product within the mobile banking application. |
| 78. | i) Auto up-gradation of the Application as per OS version |
| 79. | j) Recharge using phone book numbers |
| 80. | k) Application capability to be refreshed to fetch details of  payees, billers account information, etc. |
| 81. | l) Capability to support campaign management of new  products and loyalty programs for customers. |
| 82. | Innovative offerings in a phased manner |
| 83. | a) Universal transaction abilities - Mobile wallet |
| 84. | b) Utility for Exchange market information |
| 85. | c) Integration with social media |
| 86. | d) Remote access to view queues in nearby Branch/ATM  before reaching the site |
| 87. | e) Communication enrichment though video calls. |
| 88. | f) Customer education through product demo to promote  adoption. |
| 89. | g) The product demo should be bilingual defining process  flow for application download, activation and usage of menu options and services. The demo should be process specific. |
| 90. | h) Send money from mobile to friend’s account (using nick  name, mail id or social media credentials etc.). |
| 91. | i) Remote account opening process through mobile |
| 92. | j) Call back facility to engage with interested customers  and provide data to CRM/Contact Centre system |
| 93. | k) Cash withdrawal though ATM, OTP/PIN based  authentication, allowing non-BOB customers to withdraw cash from any BOB ATM using mobile authentication/authorisation. |
| 94. | l) Support for m-Commerce through NFC transactions. |
| 95. | m) Supports customer to customize menus/icons, disable  menus which he would not like to use as per his choice at the application level. |
| 96. | n) Capability to push weather information and important  context sensitive news. |
| 97. | o) Notification through an alert for system down to  administrator/technical team. |
| 98. | p) Feature to provide M-Passbook through the application wherein the customer can download a copy of the same locally depending on the storage capacity of the  handset and facility to mark custom remarks on the transaction entries and categorize with an option to search later offline without internet connection. |
| 99. | q) Supports customer to set limit/capping on value and  volume of fund transfer per day/week/month at application level. |
| 100. | r) User defined option to enable and disable services. |
| 101. | s) Gamification features for listed services to provide an engaging experience to the user. |
| 102. | t) Vendor to propose any line items such as additional  mobile apps that enhances customer experience. |
|  | Registration and Download activity of mobile banking  application |
| 103. | Registration method |
| 104. | a) Branch |
| 105. | b) ATM |
| 106. | c) Internet Banking |
| 107. | d) SMS request for registration |
| 108. | e) Multi-function kiosk |
| 109. | f) Web portal |

|  |  |
| --- | --- |
| 110. | g) Contact Centre / IVR |
| 111. | h) Referral by active Mobile banking users |
| 112. | **Downloading mobile banking application** |
| 113. | a) Download URL sent in the SMS for successful  registration |
| 114. | b) Apple Store |
| 115. | c) Google Play Store |
| 116. | d) Windows App store |
| 117. | e) Blackberry App world |
| 118. | f) Link on Bank’s website |
|  | **Security** |
| 119. | a) Multi-factor authentication (Token / OTP / CAPTCHA / Security Question, etc.) Minimum two factor authentication |
| 120. | b) Data transmission with end to end encryption (Standard  encryption algorithms like 3DES, AES, RSA, PKI scheme, with minimum encryption strength of 256 bit) |
| 121. | c) Platform support for SSL transactions and external  certifying authority. |
| 122. | d) Support to store data in the platform database in  encrypted format. |
| 123. | e) MPIN for securing financial transactions. |
| 124. | f) Application PIN for accessing the application and non- financial transactions. |
| 125. | g) Ability to store access credentials in encrypted format in  the user’s handset. |
| 126. | h) Ability to lock the application due to incorrect MPIN  attempts, remotely block access, with auto activation  after 24 hours for accounts locked due to three incorrect attempts. |
| 127. | i) Terminate mobile banking session and automatic log off  application after lapse of defined period of inactivity. |
| 128. | j) Auto blocking/locking of account upon reaching  maximum limit of defined transactions. |
| 129. | k) Audit trails and logging features available in Application  server, Web server and Database. |
| 130. | l) Ability to deny access to handset that does not meet  industry standard. |
| 131. | m) Security alert on registered mobile number on account  of excessive activity in the account. |
| 132. | n) Transaction should be auditable and reliable-platform  to have intelligence to handle cases like:  **•** Call received while executing transactions  **•** Battery runs out while executing transactions  **•** Drop out in GPRS connection.  **•** Backend and host system down |
| 133. | o) Mention any other security feature supported by the  system with details and architecture of security components. |

|  |  |
| --- | --- |
|  | **Scalability and Availability** |
| 134. | a) No. of concurrent users the platform can support and  handle requests in a second. |
| 135. | b) Total time for a typical fund transfer transaction  execution. |
| 136. | c) Mention whether the scalability is dependent upon  software / hardware. |
| 137. | d) Impact on performance and functionality if additional  hardware is added. |
| 138. | e) Restart or recovery process inbuilt in the application in  the event of transaction or process failure. |
| 139. | f) Control features within the application to ensure  integrity of data (input and update, maintained totals, audit trails, error reports, etc.) |
| 140. | g) Mention details regarding the interoperability of the  product and the components which can be used by  other applications. |
| 141. | h) Mention the support available for load balancing  circumstances. |
| 142. | i) Application scalability to meet the future up gradations to and all new handset/platform coming in the industry. |
| 143. | j) Application support to work on 2G/3G/4G environment  / platform. |
| 144. | k) Application capability to work on encrypted/non-  encrypted mode as per the requirement of the Bank. |
| 145. | l) Application platform support for native, hybrid-web,  hybrid combination (hybrid with additional native UI  and code capability) and mobile web app. |
| 146. | m) Support for Contact Centre log-in or API to integrate  with Bank’s CRM/Contact Centre for various activities such as:  **•** View customer registration and activation details  **•** Block stolen handset number  **•** Regenerate access credentials  **•** Change mobile number / handset |
| 147. | n) Application should support simulator environment for  testing of new features across all devices and respective  OS. |
| 148. | o) Capability of the proposed solution to push new  changes over the air without frequent uploading on App store of various platforms. |
| 149. | p) Solution capability to provide Force Update / Upgrade. |
|  | **Reports / MIS, Reconciliation and Monitoring** |
| 150. | a) Administrator Web portal for reports/MIS, monitoring  and reconciliation reports. |
| 151. | b) Compliance of web portal with OWASP (Open Web  Application Security Project) standards/guidelines. |
| 152. | c) Provision to assign specific rights / privileges to platform  administrators for secure and restricted access. |
| 153. | d) Provision to create different user groups with different  sets of rights and permission. |
| 154. | e) Administrator Web portal capability for-  i. Search customer record |

|  |  |
| --- | --- |
|  | ii. Approving user creation  iii. Register and De-register users for mobile banking application  iv. Terminate the users.  v. Maintenance of activation requests  vi. Change of Handset / Mobile number of users.  vii. All administrator activities logged to indicate the creation, modification and deletion of data.  viii. The web portal support to work on maker and checker concept for any addition, deletion, modification request made by the authorized users.  ix. Support bulk upload for creation of users  x. Handle concurrent uses of the same user ID.  xi. Set thresholds, frequency limits (daily, weekly and monthly) etc. |
| 155. | f) Transaction log reports |
| 156. | g) Session log reports |
| 157. | h) Transaction wise report (with various filters such as type  of transaction / Mode of transaction / Amount wise / Branch wise / Group wise / Financial / Non-Financial) |
| 158. | i) Channel based report |
| 159. | j) User activity based report |
| 160. | k) Dynamic report generation with query builder features. |
| 161. | l) Access to database for ad hoc report generation |
| 162. | m) An audit trail of all the registrations done with details of  the mode of request, activation type, date, time, etc. stored in the database. |
| 163. | n) Web portal support to generate reports, logs, audit  trails regarding each and every transaction. |
| 164. | o) Provision to download reports in standard formats  namely txt, xls, csv, xml, pdf, etc. |
| 165. | p) Provision for settling limits for each user / group. The limits include per day/week/month/year limit, maximum and minimum amount per transaction depending on the type of transactions. |
| 166. | q) Web portal support for configuration of NEFT on  Sundays/Holidays/Weekdays/Saturdays with timing. |
| 167. | r) Web portal support for configuration of access method,  menu items, authentication for financial / Non-financial transactions, etc. |
| 168. | s) Web portal support for various types of alerts, 1) SMS campaign, Emailer’s / Bank product / Bank advertisement to be displayed in the downloaded mobile banking application, 2) Offers on fund transfer / M-Commerce transactions, 3) System down alerts. |
| 169. | t) Web portal support to include an alert and monitoring  system to report the system down alert. The number of hours the system remained down with time period during the day/week/month/year. |
| 170. | u) Availability of Report for system uptime during the day/week/month/year. |

|  |  |
| --- | --- |
| 171. | v) Web portal support to generate daily settlement  reports for Mobile recharge and other M-Commerce transactions with bifurcation on Bank’s commission and amount payable. |
| 172. | w) Provision to generate reports for registration and  activation failure. |
| 173. | x) Provision to generate report for transactions monthly /  quarterly / half-yearly /yearly. |
| 174. | y) Generate usage statistics for Incentivisation. |
| 175. | z) Reports on service wise usage. |
| 176. | aa) Provision to provide an additional software package for reconciliation of IMPS transactions, Fund transfer transactions and M-Commerce (Mobile Recharge/Bill Payment/DTH Recharge, etc.) transactions. |
| 177. | bb) Bank expects to reach a volume of daily 1,00,000 IMPS  transactions, 50,000 Fund transfer transactions and  20,000 M-Commerce transactions within the initial six months and then upgrade as per the requirement of the Bank. |
| 178. | cc) Reporting Dashboard with Ability to gauge the services  as per usage. |
| 179. | dd) The predefined pages of the web portal should handle  web application security threats like Cross-site scripting, SQL injection flaws, Malicious file execution,  Information leakage, Improper error handling, Broken  authentication and session management, Insecure Cryptographic storage, Failure to restrict URL access. Separate Document to be submitted for the same. |
| 180. | ee) Web pages in the portal to solely communicate via SSL. |
|  | **Migration from existing mobile banking solution** |
| 181. | a) Proposed migration plan for Bank’s registered customer base of 26+ lakh customers. |
| 182. | b) Road map for migration of existing customer database  to the new platform. |
| 183. | c) Road map including features of export/import of mobile  app for easier migration. |
| 184. | d) Availability of an export feature to backup App  configuration data. |
| 185. | e) Arrangement for content creation and advertisement  for publicizing Bank’s Mobile Banking solution to the  customers. |
| 186. | f) Proposed role of vendor in enhancement of the services  and desirable features. |
|  | **Support and maintenance** |
| 187. | a) Provision to inform System downtime activity to the  bank 48 hours before the schedule maintenance activity through email. |
| 188. | b) Provision to send prior notification to Bank through  email and telephone, In case of exigency, if any unscheduled system maintenance activity that needs to be carried out to keep the system up. |
| 189. | c) Ability to provide a 365 X 24 X 7 telephone number and |

|  |  |
| --- | --- |
|  | email ID to be used for reporting issues and problem  resolution.  Escalation matrix with email ID and problem classification with time period for resolution. |
| 190. | d) Availability of an experienced support team for quick  problem resolution and corrective measures. |
| 191. | e) Provision for Push notification of system down to  customers through the application over the air, if required by Bank. |
|  | **Statutory and regulatory requirements / enhancements** |
| 192. | a) Ability of the solution offered to comply with all the  Operative Guidelines for Mobile Banking Transactions in India issued by RBI with any further guidelines and mandates issued by RBI for Mobile Banking  Transactions. |
| 193. | b) Ability to propose a version update plan with new  enhanced features with scheduled timelines of deployment. |
|  | **Standards for Mobile Banking application** |
| 194. | Mandatory compliance of the mobile banking application with  the PA-DSS guidelines/standards. |
| 195. | The proposed mobile banking solution should offer protection  against the following specified risks:  **Privacy**   Protecting customer’s sensitive information from exposure  to unintended third parties.   Preventing identity impersonation from lost or stolen mobile devices or device credentials.   Preventing account takeover or identity impersonation from credentials harvested via key loggers or other malware.  **Fraud**   Prevent money laundering from the use of compromised accounts.   Prevent smurfing (splitting of large financial transactions into smaller transactions)   Prevent the disguise of mobile transaction totals, origin and destination.  **Compliance**   The mobile banking solution should comply with the security principles and practices for authentication of mobile banking transactions as stated by The Reserve Bank of India.  **Application**   OS Security check up. Application should have capability to detect if the application is running on a jail-broken/rooted  /malware infected device.   Capability of the Application to read SIM serial no. and IMEI (International Mobile Equipment Identity) no.   Application must prevent hackers from accessing the app in a case where the device is rooted or jail-broken.   Blacklisting/Blocking of older versions of the Application on the back end, if there is a security breach.   Security logging where all security events that happen inside the application should be logged and sent to the back-end server. |

|  |  |
| --- | --- |
| 196. | For mobile payment transactions, the application should have  inbuilt security mechanism to:   Prevent account data from being intercepted when entered into a mobile device,   Prevent account data from compromise while processed or stored within the mobile device,   Prevent account data from interception upon transmission out of the mobile device |
| 197. | **Compliance to Usability Audit - Best design practices to**  **benchmark**   Branding, positioning and persuasion   Home screen / Layout and landing screens   Navigation   Information architecture   Graphics and Animation / Text   System User Dialogue and Forms   Accessibility   Task efficiency   Language   Visual Clarity   Control and Feedback   Functionality and Features   Errors |
|  | **Implementation plan** |
| 198. | List the key phases of application implementation and  Deployment.  Provide a detailed implementation plan/schedule that identifies the various activities, timeframe for implementation of each activity, interdependence between activities, key milestones, etc. |
| 199. | Provide plans for initial installation of proposed system.  Details of resources required during the implementation phase and implementation services available on site / off site. |