**Security Checklist Sign Off**  **- BI SNAP OpenAPI Integration**

Doc version: 2.0

| Merchant Name |  | | |
| --- | --- | --- | --- |
| UAT Time Period |  | | |
| Document Objective | The objective of this document is to provide a comprehensive checklist for merchants to follow while integrating with OVO API, in order to ensure correct implementation and prevent the risk of data leaks and bugs in the future.  Additionally, it is important to note that merchants who have given their sign off on this checklist will be held responsible for any potential  risks of data leaks that may arise in the future due to incorrect implementation of the API | | |
| Step by step guides | 1. Run through the mandatory checklist and recommendation checklist provided in the integration guide thoroughly. 2. Implement the API correctly based on the guidelines in the checklist. 3. After completing the API integration, provide confirmation and sign off in this documents 4. Send this document back to OVO via email 5. Once the OVO team has received the document and the UAT is passed then OVO will share the production credentials   Please note that signing off on the checklist implies that you are taking full responsibility for any potential risks of data leaks that may arise in the future due to incorrect implementation of the API. Therefore, it is essential that you ensure correct implementation before giving your sign off. | | |
| Merchant Sign Off | **PICs** | **Name & Email** | **Sign Off** |
| Business |  |  |
| Product |  |  |
| Engineer |  |  |
|  | Others |  |  |

| **Mandatory Implementation** *Merchant* ***must*** *implement this checklist, if merchant does not implement the checklist then OVO will not give the production credentials*  *\* Customers = end user (for direct Partners), merchants & end user (for PG partners)* | | |
| --- | --- | --- |
| **No** | **Checklist** | **Merchant Confirmation** (IMPLEMENTED / NOT IMPLEMENTED) |
| 1 | [DATA HANDLING] The data 'ClientSecret' and 'PrivateKey' are extremely sensitive information. These should be well secured in Merchant's environment. This data should not be shared to anyone, including OVO.  NOTES:  - ClientSecret is provided by OVO during onboarding in encrypted format.  - PrivateKey (OVO as server) is generated by the Merchant and shares only the public key with OVO. |  |
| 2 | [DATA HANDLING] Following Request Headers for BI SNAP APIs should not be shared with customers\*, otherwise it could lead to compromised merchant account:  - X-Signature  - Authorization  NOTES :  - These Headers should be shared between OVO and merchant only. |  |
| 3 | [DATA HANDLING] Following request/response body parameter values sent by OVO to Merchant should NEVER be sent to the merchant's customers\*:  - AccessToken  - RefreshToken  - linkageToken  - authCode (used of refreshing and generating new accessTokens). Please note, a different 'authCode' used in OTP WebView redirection for binding, unbinding and payment are sent to users by OVO.  NOTES :  - These Request/Response Body parameters should be shared between OVO and merchant only.  - Authcodes are shared via webview URLs which are shared further between OVO and merchant and those requests include X-Signature and Authorization headers to ensure security and authenticity of the request. |  |
| 4 | [DATA HANDLING] Following parameters should be avoided to be sent to customers\*  - ILPid  - merchantId  NOTES:  - These values are for internal OVO and Merchant only. |  |
| 5 | [DATA HANDLING] Requests involving client/customer's PIN (OVO App) and OVO OTP should come ONLY to OVO. (This is a step where user is automatically redirected to OVO Webview). |  |
| 6 | [DATA HANDLING] There shall be NO API call from user to merchant directly which ask user to to send PIN or OTP info. |  |
| 7 | [DATA HANDLING] The algorithm generating the signatures/HMAC , which used in the APIs should NOT be shared/exposed to the customers\*. |  |
| 8 | [DATA HANDLING] Information obtained by Merchants from OVO about its customers\* should NOT be sent to its customers\*, unless there is an essential use case for customer\* to know that information. Recommended to consult internal GRC (Governance, Risk & Compliance) team and OVO team as needed in this regards.  NOTES:  - If data needs to be shared with customer\*, use masked data  Example of Customer's PII (Personally Identifiable Information) Data:  - Mobile Number  - KYC data |  |
| 9 | [API IMPLEMENTATION] Merchant's customers\* should not have any implementation where requests are made to OVO directly, EXCEPT for OTP and PIN validation |  |
| 10 | [API IMPLEMENTATION] Check the transaction status before taking further action. If the transactions is showing as pending do not process / replay the transaction. |  |
| 11 | [CYBERSECURITY MANDATE] Comply with the Region's Data Privacy Laws and Regulations while handling data. A GRC review is recommended. |  |
| 12 | [CYBERSECURITY MANDATE] Use encrypted communication (ex. HTTPS) only for all external communications (i.e. Between Merchant and OVO) |  |

| **Recommendation/ Best Practice** *Merchants are encouraged to implement the following best practices to minimize potential issues in the future, as they are not mandatory but highly recommended for a smoother integration process with OVO*  *\* Customers = end user (for direct Partners), merchants & end user (for PG partners)* | | |
| --- | --- | --- |
| **No** | **Checklist** | **Merchant Notes** |
| 1 | [DATA HANDLING] Transfer only necessary and relevant information to customer\* for completing the transaction. Any information which will not required by customer\* to process the transaction, should not be sent to the customer\*. |  |
| 2 | [API IMPLEMENTATION] Timeout of actions on merchant side should be aligning/complementing OVO's timeout. Mismatch may cause erroneous actions/transactions.  NOTES: - Example : Merchant side transaction timeout period if is less than OVO timeout period it might cause customer to do successful payment for timed out transactions. |  |
| 3 | [API IMPLEMENTATION] Implement user input validation before forwarding it to OVO. Before sending user inputs to OVO (via merchant's server), implement possible validation checks on the user input, and forward only the verified data to OVO.  NOTES:  Examples (but not limited to) :  - Check in invalid amounts (negative amount, extremely large amount, etc.)  - Transaction data not belonging to the same user (like Transaction ID of another user, ref. no. of another user, mobile no. of another user, etc.)  - Presence of unwanted characters / numbers |  |
| 4 | [API IMPLEMENTATION] New B2B token should be created close to expiry or after expiry of previous token.  - Expiry time of B2B token is 15 minutes (as per BI standards) |  |
| 5 | [API IMPLEMENTATION] As an added security check, an internal mechanism to validate expected payment amount against the actual transaction amount using the Direct Debit Inquiry Status API can be implemented. |  |
| 6 | [CYBERSECURITY RECOMMENDATION] Perform a security analysis (penetration testing / design review / architecture review) on the implementation. |  |
| 7 | [CYBERSECURITY RECOMMENDATION] Have Rate Limiting Controls implemented on the various APIs to avoid bot traffic. |  |
| 8 | [CYBERSECURITY RECOMMENDATION] Never trust user supplied data. Always have a server side check in place to check for all the data arriving from user to server, before processing the data. |  |
| 9 | [CYBERSECURITY RECOMMENDATION] Use encrypted communication (ex. HTTPS) only for all internal communications (i.e. Merchant Backend - Merchant Backend) |  |