**Security Checklist Sign Off**  **- BI SNAP QRIS MPM Integration**

Doc version: 1.0

| Merchant Name | *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* | | |
| --- | --- | --- | --- |
| UAT Time Period | *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* | | |
| Document Objective | The objective of this document is to provide a comprehensive checklist for partners / 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. | | |
| Partner / 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)* | | |
| --- | --- | --- |
| **S.No.** | **Checklist** | **Partner / Merchant Confirmation** (IMPLEMENTED / NOT IMPLEMENTED) + Comments |
| 1 | The data 'secret\_key' and 'private\_key' are extremely sensitive information. These should be well secured in Merchant/Partner's environment. This data should not be shared to anyone, including OVO (via API calls).  NOTES:  - secret\_key is provided by OVO during onboarding in encrypted format.  - private\_key (OVO as server) is generated by the Merchant/Partner and shares only the public key with OVO. |  |
| 2 | Following items SHOULD NOT TO BE SHARED WITH CUSTOMERS\* OR ANYONE, EXCEPT OVO:  1) accessToken  2) X-SIGNATURE (hmac generated during requests)  3) hmac generation algorithm |  |
| 3 | All the QRIS MPM APIs should be coming to OVO Backend from Merchant/Partner's Backend only (and not from any customer\*). |  |
| 4 | Use encrypted communication (ex. HTTPS) only for all external communications (i.e. Merchant/Partner to OVO). |  |
| 5 | Always check the transaction status before taking further action after calling Transactional API. If the transaction is showing as pending, do not process / replay the transaction, instead call the check status API as a mandate to get the final transaction status |  |
| 6 | In case of Timeout on transactional API, the transaction status should be regarded as suspect/unknown, and Check Status API should be called to confirm the status.  Timeout can be: 1. Client request timeout (no response after certain time threshold on client) 2. HTTP code 504 3. Any application response code indicating timeout |  |

| **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)* | | |
| --- | --- | --- |
| **S.No.** | **Checklist** | **Partner/Merchant Confirmation** (IMPLEMENTED / NOT IMPLEMENTED) + Comments |
| 1 | Do not share the QRIS MPM APIs and the data therein with Customers (End users). If any sensitive data needs to be shared please use masked values. |  |
| 2 | Timeout of actions on merchant/partner side should be aligning/complementing OVO's timeout. Mismatch may cause erroneous actions/transactions.  NOTES: - Example : Merchant/Partner side transaction timeout period if is less than OVO timeout period it might cause customer (end user) to do successful payment for timed out transactions. |  |
| 3 | Implement user input validation before forwarding any request to OVO with user supplied data. Before sending user inputs to OVO (via merchant's/partner'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 | New B2B token should be created close to expiry or after expiry of previous token.  NOTES: - Expiry time of B2B token is 15 minutes (as per BI standards) |  |
| 5 | Have Rate Limiting Controls implemented on the various APIs to avoid bot traffic. |  |
| 6 | Never trust user supplied data. Always have a server side check in place to for all the data arriving from user to server, before processing the data. |  |
| 7 | Use encrypted communication (ex. HTTPS) only for all internal communications (i.e. Merchant/Partner Backend to Merchant/Partner Backend within same environment). |  |
| 8 | Check the balance in Merchant's/Partner's account with OVO has sufficient balance before making the TOP UP API calls to ensure smooth process for top-ups for end customers. |  |