**Security Checklist Sign Off**  **- Push to Pay Integration**

Doc version: 2.0

| Merchant Name | *Family Coffee* | | |
| --- | --- | --- | --- |
| UAT | *14 April 2023* | | |
| 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 | *John Mayer*  [*john.mayer@familycoffee.com*](mailto:john.mayer@familycoffee.com) |  |
| 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* | | |
| --- | --- | --- |
| **No** | **Checklist** | **Merchant Confirmation** (IMPLEMENTED / NOT IMPLEMENTED) |
| 1 | Following items SHOULD NOT TO BE SHARED WITH CUSTOMERS OR ANYONE, EXCEPT OVO:  1) Key  2) HMAC  3) HMAC generation algorithm |  |
| 2 | No PTP API call should be made from Customers (end users) to OVO (except PIN/OTP challenge). All the PTP APIs and data involved therein is to be used between Merchant Backend and OVO Backend only. |  |
| 3 | The PIN/OTP challenge should only involve OVO and the Customer (End User). Any request involving the PIN should NOT route through the Merchant. |  |
| 4 | In the Inquiry, VOID and Reversal PTP APIs, ensure to use the actual transaction value only. Any incorrect amount mentioned may give an incorrect response. |  |
| 5 | Ensure that after the settlement process of the transactions the final amount is tallied from the merchant records for any discrepancies. |  |
| 6 | Use encrypted communication (ex. HTTPS) only for all communications (external) |  |

| **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* | | |
| --- | --- | --- |
| **No** | **Checklist** | **Merchant Notes** |
| 1 | Do not share the PTP APIs data with Customers (End users). If any sensitive information is shared please use masked values. | *We have implemented this, no sensitive information shared to user* |
| 2 | Timeout of actions on the merchant side should be aligning/complementing OVO's timeout. Mismatch may cause erroneous actions/transactions.  Note: OVO timeout is 60 Seconds |  |
| 3 | Use encrypted communication (ex. HTTPS) only for all communications (internal communication between merchant Backend to merchant backend) |  |
| 4 | Have Rate Limiting Controls implemented on the various APIs to avoid bot traffic. |  |
| 5 | If the payment status is showing as pending/ merchant doesn’t receive any response from OVO after 60 seconds, merchant can call API Check Payment Status to get the latest status |  |
| 6 | Merchants show a clear guidance to users about how to complete their transaction after they input their phone number and show the countdown of time left.  Key points in the guidance of how to complete transaction:   1. Segera selesaikan pembayaran di aplikasi OVO 2. Klik notifikasi yang dikirimkan oleh OVO lalu klik tombol **“Bayar”** 3. Atau buka aplikasi OVO, lalu klik menu **Inbox** 4. Klik notifikasi konfirmasi pembayaran 5. Klik tombol **“Bayar”** 6. Selesaikan pembayaran sebelum kadaluarsa |  |
| 7 | 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.  Example:   1. When user need to input OVO phone number, merchants has a validation to only allow user to input integer value 2. When users need to input an OVO phone number, merchants validate the format phone number first if it’s the right phone number format or not. If user input 123456789 then merchant will not send the request to OVO |  |
| 8 | Merchant show a clear error message to user so user understand if their transaction is fail  Example:   1. Users input a phone number that is not registered in OVO, then OVO responds with RC14 (Invalid phone number). Merchant should explain to user that their phone number is not registered in OVO 2. Users input a phone number that is registered in OVO but OVO responds with RC26 (fails to send notification). Merchant should explain to the user that their transaction is fail so user can retry 3. Users input a phone number that is registered in OVO but the user then the payment fails due to any reasons. Merchants should show the information that the payment is fail |  |
| 9 | Never trust user supplied data. Always have a server side check in place for all the data arriving from user to server, before processing the data. |  |