Discovery Report

DR\_Vol\_4\_OTP\_SMS

Lotte Finance Vietnam

Version 0.1

Status: Draft

Date: 18.03.2021

Prepared by:

Author: Nguyen Tien Dat

Approved By: [Manager]

1. Table of Contents

[1. Table of Contents 2](#_Toc68076114)

[2. History of changes 4](#_Toc68076115)

[3. Introduction 6](#_Toc68076116)

[3.1. Notations 6](#_Toc68076117)

[4. Requirement List 7](#_Toc68076118)

[4.1. Các quy định chung của OTP 7](#_Toc68076119)

[4.1.1. Business Requirement 7](#_Toc68076120)

[4.1.2. Technical Detail 7](#_Toc68076121)

[- Mã OTP sinh ra, được ghi lại trong cơ sở dữ liệu, áp dụng băm với SHA1 và ghép OTP kèm chuỗi Pepper (tham số thiết lập cho môi trường). 7](#_Toc68076122)

[4.2. Xác minh số điện thoại đăng kí 8](#_Toc68076123)

[4.2.1. Business Requirement 8](#_Toc68076124)

[- Hệ thống Paylater tạo OTP xác thực thông tin số điện thoại 8](#_Toc68076125)

[- Hệ thống Paylater gửi thông tin OTP, số điện thoại tới gateway để gửi SMS tới số điện thoại khách hàng đăng ký. 8](#_Toc68076126)

[- Hệ thống Paylater có màn hình cho KH nhập thông tin OTP được LFVN gửi SMS tới số điện thoại. 8](#_Toc68076127)

[- Hệ thống Paylater xác thực OTP khách hàng nhập. 8](#_Toc68076128)

[4.2.2. Technical Detail 8](#_Toc68076129)

[Hệ thống tạo, gửi sms và verify mã OTP này sẽ thực hiện theo như phần yêu cầu chung 4.1. 8](#_Toc68076130)

[4.2.3. Testing and Sample 8](#_Toc68076131)

[4.2.4. Limitation 8](#_Toc68076132)

[4.3. OTP xác thực E-Signing 8](#_Toc68076133)

[4.3.1. Business Requirement 8](#_Toc68076134)

[- Hệ thống Paylater nhận OTP từ hệ thống E-Signing để gửi khách hàng. 8](#_Toc68076135)

[- Hệ thống Paylater có màn hình cho khách hàng nhập thông tin OTP được LFVN gửi SMS tới số điện thoại đăng ký. 8](#_Toc68076136)

[- Hệ hống Paylater gửi thông tin OTP mà khách hàng nhập sang hệ thống E-Singning để xác thực. 8](#_Toc68076137)

[- Hệ các giới hạn khác thì sẽ tuân theo hệ thống của E-Signing. 8](#_Toc68076138)

[4.3.2. Technical Detail 8](#_Toc68076139)

[4.3.3. Testing and Sample 9](#_Toc68076140)

[4.3.4. Limitation 9](#_Toc68076141)

[4.4. Xác thực giao dịch thanh toán 9](#_Toc68076142)

[4.4.1. Business Requirement 9](#_Toc68076143)

[- Hệ thống Paylater tạo OTP xác thực giao dịch thanh toán. 9](#_Toc68076144)

[- Hệ thống Paylater gửi thông tin OTP, số điện thoại tới gateway để gửi SMS tới số điện thoại khách hàng đã đăng ký trên hệ thống Paylater. 9](#_Toc68076145)

[- Hệ thống Paylater có màn hình cho KH nhập thông tin OTP được LFVN gửi SMS tới số điện thoại. 9](#_Toc68076146)

[- Hệ thống Paylater xác thực OTP khách hàng nhập. 9](#_Toc68076147)

[4.4.2. Technical Detail 9](#_Toc68076148)

[- Hệ thống tạo, gửi sms và verify mã OTP này sẽ thực hiện theo như phần yêu cầu chung 4.1. 9](#_Toc68076149)

[4.4.3. Testing and Sample 9](#_Toc68076150)

[4.4.4. Limitation 9](#_Toc68076151)

1. History of changes

|  |  |  |  |
| --- | --- | --- | --- |
| version | date | Description | author |
| 0.1 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Copyright**

© OpenWay Asia Limited 2021. All rights reserved.

The Copyright of this complete document and every part it belongs to OpenWay Asia Limited. Proprietary material, brand or product names of other parties or trademarks remain with their respective owners. You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system. Any sample data used in examples below are completely fictitious unless otherwise noted.

**Disclaimer**

This document and the OpenWay Asia software it describes are furnished by OpenWay Asia Limited under a Software Licensing Agreement, Consultancy Agreement, Variation Request or Confidentiality Agreement, and may be used or copied only in accordance with the terms of such Agreement. Neither this document nor the OpenWay Asia software it describes may be used, sold, transferred, copied, translated, reproduced, or transmitted in any form or by any means, electronic or mechanical, for any purpose, in whole or in part, other than in accordance with the terms of such Agreement, or otherwise without prior written consent of OpenWay Asia Limited.

This document describes a generic product or service and should be read in conjunction with other documents relevant to the configuration of any specific system. The licensee of OpenWay software or user of OpenWay Asia services is responsible for ensuring that the product or service described herein meets its own requirements.

**Confidentiality**

The information contained in this Document is the property of OpenWay Asia Ltd and contains CONFIDENTIAL information that is produced solely for the benefit of the receiving party named on the front page of this document. The recipient should keep this document and all its information confidential. On no account should this document, in whole or in part, be used, sold, transferred, copied, translated, reproduced, or transmitted in any form or by any means, electronic or mechanical, or disclosed or disseminated to any third party, without the express written permission of OpenWay Asia Ltd.

1. Introduction
   1. Notations

Notations used in this document are listed in the table below.

***Table 1. Notations***

| Notation | Description |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. Requirement List
   1. REQV4\_1 - Các quy định chung của OTP

### Business Requirement

* Mã OTP có độ dài : 6 kí tự.
* Khách hàng chỉ có thể chọn gửi mã OTP tối đa 3 lần / phiên và 2 phiên / ngày , nghĩa là phiên thứ N chỉ tạo được sau 24h kể từ lần gửi tin đầu tiên của phiên số 1 (chỉ tính các phiên không xác thực OTP thành công lần nào). Số phiên không thành công và thời gian 24h có thể được thay đổi (chưa thực hiện trong gian đoạn này).
* Mã OTP sẽ được sinh ngẫu nhiên, là số có 6 chữ số (gồm cả số 0 ở đầu) và sẽ được lưu lại trong cơ sở dữ liệu và có bảo vệ (chi tiết do kỹ thuật quyết định).
* Mỗi mã OTP chỉ được kiểm tra sai không quá 3 lần/mỗi lần gửi, nếu sai quá số lần phải gửi lại và chỉ cho phép gửi lại cũng không quá 3 lần như quy tắc trên.
* Thời gian hiệu lực của mã OTP là 3 phút. Thời gian mỗi lần gửi lại mã OTP sẽ dãn cách nhau tối thiểu 1 phút. Lưu ý: thời gian 1 phút và 3 phút có thể tham số hóa nhưng chưa thực hiện trong gian đoạn này.
* Có tính năng để hệ thống Customer support hỗ trợ reset lại các thông số trên khi khách hàng cần hỗ trợ.
* Về phần verify mã OTP : Khi khách hàng nhập mã OTP thì hệ thống sẽ thực hiện xác thực mã (Mã OTP lấy được sẽ kèm theo sessionID).

### Technical Detail

* Mã OTP sẽ được sinh ngẫu nhiên bằng hàm java.util.Random (với tham số seed lấy từ SecureRandom nhưng gắn với /dev/urandom để đảm bảo tốc độ), là số integer có 6 chữ số tối đa (gắn số 0 ở đầu nếu số nhỏ 100000).
* Mã OTP sinh ra, được ghi lại trong cơ sở dữ liệu, áp dụng băm với SHA1 và ghép OTP kèm chuỗi Pepper (tham số thiết lập cho môi trường).
* Số lần sai và thời gian giữ phiên có thể reset được bằng hàm API hoặc User Portal (thực hiện ở pha kế tiếp).
* Về phần gửi sms : Hệ thống sẽ gọi Api bên phía FPT do LFVN hợp tác để lấy token. Token này sẽ được lưu vào cache (để tránh trường hợp lấy token nhiều lần). Sẽ có 2 trường hợp đó là sẽ lưu token vào cơ sở dữ liệu (nếu token time dài và yêu cầu chỉ lấy 1 token duy nhất) hoặc sẽ được lưu vào trong 1 directory chỉ định (nếu token time ngắn và có thể tạo nhiều token). Sau khi đã lấy được token thì hệ thống sẽ tiếp tục gọi vào Api brandname phía OTP để thực hiện gửi sms mã OTP cho khách hàng (nội dung tin nhắn sẽ được mã hóa base 64 theo đặc tả của nhà cung cấp API).

### Testing and Sample

Cung cấp sau.

### Technical Detail

Cung cấp sau.

* 1. REQV4\_2 - Xác minh số điện thoại đăng kí

### Business Requirement

* Hệ thống Paylater tạo OTP xác thực thông tin số điện thoại
* Hệ thống Paylater gửi thông tin OTP, số điện thoại tới gateway để gửi SMS tới số điện thoại khách hàng đăng ký.
* Hệ thống Paylater có màn hình cho KH nhập thông tin OTP được LFVN gửi SMS tới số điện thoại.
* Hệ thống Paylater xác thực OTP khách hàng nhập.

### Technical Detail

Hệ thống sẽ tự động tạo mã OTP, gọi hàm gửi tin nhắn theo mẫu tin nhắn định trước tới số điện thoại khách hàng nhập. Sau khi khách hàng nhập vào form thì hệ thống sẽ tiến hành verify mã OTP xác nhận. Số lần tạo và gửi tin nhắn sẽ giới hạn như yêu cầu chung 4.1.

### Testing and Sample

### Limitation

* 1. REQV4\_3 - OTP xác thực E-Signing

### Business Requirement

* Hệ thống Paylater nhận OTP từ hệ thống E-Signing để gửi khách hàng.
* Hệ thống Paylater có màn hình cho khách hàng nhập thông tin OTP được LFVN gửi SMS tới số điện thoại đăng ký.
* Hệ hống Paylater gửi thông tin OTP mà khách hàng nhập sang hệ thống E-Singning để xác thực.
* Các giới hạn khác thì sẽ tuân theo hệ thống của E-Signing.
* Có tính năng để hệ thống Customer support hỗ trợ reset lại các thông số trên thì tuân theo hệ thống E-Signing.

### Technical Detail

Phía Paylater sẽ gọi vào api để lấy mã OTP từ bên phía E-Signing và gửi cho khách hàng. Sau khi khách hàng nhập mã OTP thì phía Paylater sẽ gửi lại mã OTP này cho phía E-Signing để thực hiện verify mã OTP và sẽ trả lại kết quả cho phía Paylater xem mã OTP khách hàng nhập có chính xác không.

### Testing and Sample

Cung cấp sau.

### Limitation

Tuỳ thuộc khả năng của dịch vụ E-Signing.

* 1. REQV4\_4 - Xác thực giao dịch thanh toán (khi sử dụng tài khoản Paylater)

### Business Requirement

* Hệ thống Paylater tạo OTP xác thực giao dịch thanh toán.
* Hệ thống Paylater gửi thông tin OTP, số điện thoại tới gateway để gửi SMS tới số điện thoại khách hàng đã đăng ký trên hệ thống Paylater.
* Hệ thống Paylater có màn hình cho KH nhập thông tin OTP được LFVN gửi SMS tới số điện thoại.
* Hệ thống Paylater xác thực OTP khách hàng nhập.
* Phần generate OTP và gửi sms này cũng sẽ giới hạn như phần yêu cầu chung 4.1
* Có tính năng để hệ thống Customer support hỗ trợ reset lại các thông số trên khi khách hàng cần hỗ trợ. Việc reset này chỉ áp dụng cho khách hàng cụ thể.

### Technical Detail

Hệ thống tạo, gửi sms và verify mã OTP này sẽ được thực hiện tương tự như phần xác minh số điện thoại đăng kí 4.2

### Testing and Sample

### Limitation