**BMO Masterpass Wallet**

**Wallet Services API Specification**

Version 0.1

April 2017

Notices

Following are policies pertaining to proprietary rights and trademarks.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively “Mastercard”), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Customer Operations Services team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Table of Contents

[1 Introduction 11](#_Toc480329398)

[1.1 Overview 11](#_Toc480329399)

[1.2 Using This Document 11](#_Toc480329400)

[1.3 Revision History 11](#_Toc480329401)

[1.4 Document Conventions 11](#_Toc480329402)

[1.5 Acronyms 11](#_Toc480329403)

[1.6 References 12](#_Toc480329404)

[2 General 13](#_Toc480329405)

[2.1 API Overview 13](#_Toc480329406)

[2.2 API Design 13](#_Toc480329407)

[2.3 Message Envelope 14](#_Toc480329408)

[2.3.1 JWE Envelope 14](#_Toc480329409)

[2.4 API Security and Validations 18](#_Toc480329410)

[2.4.1 Message Confidentiality 18](#_Toc480329411)

[2.4.2 Message Replay Attack Detection and Mitigation 18](#_Toc480329412)

[2.4.3 JWE based Mobile API Security 19](#_Toc480329413)

[2.4.4 Authentication 19](#_Toc480329414)

[2.4.5 Session Control 19](#_Toc480329415)

[2.4.6 Input Validation 20](#_Toc480329416)

[2.4.7 Mobile App & Device Validations 20](#_Toc480329417)

[2.4.8 Business Validations 20](#_Toc480329418)

[2.5 URL Scheme 21](#_Toc480329419)

[2.5.1 URL Elements 21](#_Toc480329420)

[2.6 API Data Elements 22](#_Toc480329421)

[2.6.1 Date and Time Format 22](#_Toc480329422)

[2.6.2 UUID 22](#_Toc480329423)

[2.6.3 Response Code and Message 22](#_Toc480329424)

[3 Wallet Account Management Services 24](#_Toc480329425)

[3.1 Get Certificate Chain 24](#_Toc480329426)

[3.1.1 Overview 24](#_Toc480329427)

[3.1.2 API Relative URI 24](#_Toc480329428)

[3.1.3 HTTP Method 24](#_Toc480329429)

[3.1.4 Request Parameters 24](#_Toc480329430)

[3.1.5 Response Parameters 24](#_Toc480329431)

[3.1.6 Sample Request 24](#_Toc480329432)

[3.1.7 Sample Response 24](#_Toc480329433)

[3.1.8 Exceptions 24](#_Toc480329434)

[3.2 Get Public Key Certificate 25](#_Toc480329435)

[3.2.1 Overview 25](#_Toc480329436)

[3.2.2 API Relative URI 25](#_Toc480329437)

[3.2.3 HTTP Method 25](#_Toc480329438)

[3.2.4 Request Parameters 25](#_Toc480329439)

[3.2.5 Response Parameters 25](#_Toc480329440)

[3.2.6 Sample Request 25](#_Toc480329441)

[3.2.7 Sample Response 25](#_Toc480329442)

[3.2.8 Exceptions 25](#_Toc480329443)

[3.3 Check Device Eligibility 26](#_Toc480329444)

[3.3.1 Overview 26](#_Toc480329445)

[3.3.2 Relative API URI 26](#_Toc480329446)

[3.3.3 HTTP Method 26](#_Toc480329447)

[3.3.4 Request Parameters 26](#_Toc480329448)

[3.3.5 Response Parameters 26](#_Toc480329449)

[3.3.6 Sample Request 26](#_Toc480329450)

[3.3.7 Sample Response 26](#_Toc480329451)

[3.3.8 Exceptions 27](#_Toc480329452)

[3.4 Get Latest Legal Docs 28](#_Toc480329453)

[3.4.1 Overview 28](#_Toc480329454)

[3.4.2 Relative API URI 28](#_Toc480329455)

[3.4.3 HTTP Method 28](#_Toc480329456)

[3.4.4 Request Parameters 28](#_Toc480329457)

[3.4.5 Response Parameters 28](#_Toc480329458)

[3.4.6 Sample Request 28](#_Toc480329459)

[3.4.7 Sample Response 28](#_Toc480329460)

[3.4.8 Exceptions 28](#_Toc480329461)

[3.5 Register Wallet Account 29](#_Toc480329462)

[3.5.1 Overview 29](#_Toc480329463)

[3.5.2 Relative API URI 29](#_Toc480329464)

[3.5.3 HTTP Method 29](#_Toc480329465)

[3.5.4 Request Parameters 29](#_Toc480329466)

[3.5.5 Response Parameters 29](#_Toc480329467)

[3.5.6 Sample Request 29](#_Toc480329468)

[3.5.7 Sample Response 30](#_Toc480329469)

[3.5.8 Exceptions 30](#_Toc480329470)

[3.6 Retrieve User Profile 31](#_Toc480329471)

[3.6.1 Overview 31](#_Toc480329472)

[3.6.2 URL 31](#_Toc480329473)

[3.6.3 HTTP Method 31](#_Toc480329474)

[3.6.4 Request Parameters 31](#_Toc480329475)

[3.6.5 Response Parameters 31](#_Toc480329476)

[3.6.6 Sample Request 31](#_Toc480329477)

[3.6.7 Sample Response 31](#_Toc480329478)

[3.6.8 Exceptions 31](#_Toc480329479)

[3.7 Update User Accepted Legal Doc 32](#_Toc480329480)

[3.7.1 Overview 32](#_Toc480329481)

[3.7.2 API Relative URI 32](#_Toc480329482)

[3.7.3 HTTP Method 32](#_Toc480329483)

[3.7.4 Request Parameters 32](#_Toc480329484)

[3.7.5 Response Parameters 32](#_Toc480329485)

[3.7.6 Sample Request 32](#_Toc480329486)

[3.7.7 Sample Response 32](#_Toc480329487)

[3.7.8 Exceptions 32](#_Toc480329488)

[4 PIN Management API 33](#_Toc480329489)

[4.1 Authenticate Wallet 33](#_Toc480329490)

[4.1.1 Overview 33](#_Toc480329491)

[4.1.2 API Relative URI 33](#_Toc480329492)

[4.1.3 HTTP Method 33](#_Toc480329493)

[4.1.4 Request Parameters 33](#_Toc480329494)

[4.1.5 Response Parameters 33](#_Toc480329495)

[4.1.6 Sample Request 33](#_Toc480329496)

[4.1.7 Sample Response 33](#_Toc480329497)

[4.1.8 Exceptions 33](#_Toc480329498)

[5 Payment Card Management Services 34](#_Toc480329499)

[5.1 Retrieve Payment Cards 34](#_Toc480329500)

[5.1.1 Overview 34](#_Toc480329501)

[5.1.2 URL 34](#_Toc480329502)

[5.1.3 HTTP Method 34](#_Toc480329503)

[5.1.4 Request Parameters 34](#_Toc480329504)

[5.1.5 Response Parameters 35](#_Toc480329505)

[5.1.6 Sample Request 35](#_Toc480329506)

[5.1.7 Sample Response 35](#_Toc480329507)

[5.1.8 Exceptions 36](#_Toc480329508)

[5.2 Set Payment Card as Default 37](#_Toc480329509)

[5.2.1 Overview 37](#_Toc480329510)

[5.2.2 URL 37](#_Toc480329511)

[5.2.3 HTTP Method 37](#_Toc480329512)

[5.2.4 Request Parameters 37](#_Toc480329513)

[5.2.5 Response Parameters 37](#_Toc480329514)

[5.2.6 Sample Request 37](#_Toc480329515)

[5.2.7 Sample Response 37](#_Toc480329516)

[5.2.8 Exceptions 37](#_Toc480329517)

[5.3 Retrieve Payment Card Assets 38](#_Toc480329518)

[5.3.1 Overview 38](#_Toc480329519)

[5.3.2 URL 38](#_Toc480329520)

[5.3.3 HTTP Method 38](#_Toc480329521)

[5.3.4 Request Parameters 38](#_Toc480329522)

[5.3.5 Response Parameters 38](#_Toc480329523)

[5.3.6 Sample Request 38](#_Toc480329524)

[5.3.7 Sample Response 38](#_Toc480329525)

[5.3.8 Exceptions 39](#_Toc480329526)

[5.4 Activate Payment Card Token 40](#_Toc480329527)

[5.4.1 Overview 40](#_Toc480329528)

[5.4.2 URL 40](#_Toc480329529)

[5.4.3 HTTP Method 40](#_Toc480329530)

[5.4.4 Request Parameters 40](#_Toc480329531)

[5.4.5 Response Parameters 40](#_Toc480329532)

[5.4.6 Sample Request 40](#_Toc480329533)

[5.4.7 Sample Response 40](#_Toc480329534)

[5.4.8 Exceptions 41](#_Toc480329535)

[6 Shipping Address Management Services 42](#_Toc480329536)

[6.1 Add Shipping Addresses 42](#_Toc480329537)

[6.1.1 Overview 42](#_Toc480329538)

[6.1.2 URL 42](#_Toc480329539)

[6.1.3 HTTP Method 42](#_Toc480329540)

[6.1.4 Request Parameters 42](#_Toc480329541)

[6.1.5 Response Parameters 42](#_Toc480329542)

[6.1.6 Sample Request 43](#_Toc480329543)

[6.1.7 Sample Response 44](#_Toc480329544)

[6.1.8 Exceptions 44](#_Toc480329545)

[6.2 Update Shipping Address 45](#_Toc480329546)

[6.2.1 Overview 45](#_Toc480329547)

[6.2.2 URL 45](#_Toc480329548)

[6.2.3 HTTP Method 45](#_Toc480329549)

[6.2.4 Request Parameters 45](#_Toc480329550)

[6.2.5 Response Parameters 45](#_Toc480329551)

[6.2.6 Sample Request 45](#_Toc480329552)

[6.2.7 Sample Response 46](#_Toc480329553)

[6.2.8 Exceptions 46](#_Toc480329554)

[6.3 Retrieve Shipping Addresses 47](#_Toc480329555)

[6.3.1 Overview 47](#_Toc480329556)

[6.3.2 URL 47](#_Toc480329557)

[6.3.3 HTTP Method 47](#_Toc480329558)

[6.3.4 Request Parameters 47](#_Toc480329559)

[6.3.5 Response Parameters 47](#_Toc480329560)

[6.3.6 Sample Request 47](#_Toc480329561)

[6.3.7 Sample Response 47](#_Toc480329562)

[6.3.8 Exceptions 48](#_Toc480329563)

[6.4 Set Shipping Address as Default 49](#_Toc480329564)

[6.4.1 Overview 49](#_Toc480329565)

[6.4.2 URL 49](#_Toc480329566)

[6.4.3 HTTP Method 49](#_Toc480329567)

[6.4.4 Request Parameters 49](#_Toc480329568)

[6.4.5 Response Parameters 49](#_Toc480329569)

[6.4.6 Sample Request 49](#_Toc480329570)

[6.4.7 Sample Response 49](#_Toc480329571)

[6.4.8 Exceptions 49](#_Toc480329572)

[6.5 Delete Shipping Address 50](#_Toc480329573)

[6.5.1 Overview 50](#_Toc480329574)

[6.5.2 URL 50](#_Toc480329575)

[6.5.3 HTTP Method 50](#_Toc480329576)

[6.5.4 Request Parameters 50](#_Toc480329577)

[6.5.5 Response Parameters 50](#_Toc480329578)

[6.5.6 Sample Request 50](#_Toc480329579)

[6.5.7 Sample Response 50](#_Toc480329580)

[6.5.8 Exceptions 50](#_Toc480329581)

[7 Other Services 51](#_Toc480329582)

[7.1 Retrieve Countries 51](#_Toc480329583)

[7.1.1 Overview 51](#_Toc480329584)

[7.1.2 URL 51](#_Toc480329585)

[7.1.3 HTTP Method 51](#_Toc480329586)

[7.1.4 Request Parameters 51](#_Toc480329587)

[7.1.5 Response Parameters 51](#_Toc480329588)

[7.1.6 Sample Request 51](#_Toc480329589)

[7.1.7 Sample Response 51](#_Toc480329590)

[7.1.8 Exceptions 51](#_Toc480329591)

[7.2 Retrieve field configuration 51](#_Toc480329592)

[7.2.1 Overview 51](#_Toc480329593)

[7.2.2 URL 52](#_Toc480329594)

[7.2.3 HTTP Method 52](#_Toc480329595)

[7.2.4 Request Parameters 52](#_Toc480329596)

[7.2.5 Response Parameters 52](#_Toc480329597)

[7.2.6 Sample Request 52](#_Toc480329598)

[7.2.7 Sample Response 52](#_Toc480329599)

[7.2.8 Exceptions 52](#_Toc480329600)

[8 Masterpass Checkout Services 53](#_Toc480329601)

[8.1 Initialize Checkout 53](#_Toc480329602)

[8.1.1 Overview 53](#_Toc480329603)

[8.1.2 URL 53](#_Toc480329604)

[8.1.3 HTTP Method 53](#_Toc480329605)

[8.1.4 Request Parameters 53](#_Toc480329606)

[8.1.5 Response Parameters 53](#_Toc480329607)

[8.1.6 Sample Request 53](#_Toc480329608)

[8.1.7 Sample Response 53](#_Toc480329609)

[8.1.8 Exceptions 53](#_Toc480329610)

[8.2 Authorize Checkout 54](#_Toc480329611)

[8.2.1 Overview 54](#_Toc480329612)

[8.2.2 URL 54](#_Toc480329613)

[8.2.3 HTTP Method 54](#_Toc480329614)

[8.2.4 Request Parameter 54](#_Toc480329615)

[8.2.5 Response Parameter 54](#_Toc480329616)

[8.2.6 Sample Request 55](#_Toc480329617)

[8.2.1 Sample Response 55](#_Toc480329618)

[8.2.2 Exceptions 56](#_Toc480329619)

[9 Generic Exceptions 57](#_Toc480329620)

[10 Push Notifications 59](#_Toc480329621)

[10.1 Description 59](#_Toc480329622)

[10.2 Notify Token Updated 59](#_Toc480329623)

[10.2.1 Message Parameter 59](#_Toc480329624)

[10.2.1 Sample Message 59](#_Toc480329625)

[11 Common Objects 60](#_Toc480329626)

[11.1 UserData 60](#_Toc480329627)

[11.2 MobileNumber 61](#_Toc480329628)

[11.3 RNSData 62](#_Toc480329629)

[11.4 SafetyNetData 62](#_Toc480329630)

[11.5 DeviceInstanceData 63](#_Toc480329631)

[11.6 DeviceProfileData 63](#_Toc480329632)

[11.7 ApplicationData 64](#_Toc480329633)

[11.8 DeviceEligibilityData 65](#_Toc480329634)

[11.9 PaymentCardData 66](#_Toc480329635)

[11.10 CardData 68](#_Toc480329636)

[11.11 AddressData 69](#_Toc480329637)

[11.12 CardBrandData 72](#_Toc480329638)

[11.13 CardTokenData 73](#_Toc480329639)

[11.14 AuthenticationMethod 74](#_Toc480329640)

[11.15 OSData 74](#_Toc480329641)

[11.16 ShippingAddressData 75](#_Toc480329642)

[11.17 LegalDocData 77](#_Toc480329643)

[11.18 LegalDocAcceptanceData 78](#_Toc480329644)

[11.19 CheckoutSelectionData 79](#_Toc480329645)

[11.20 DSRPData 80](#_Toc480329646)

[11.21 SessionKeySigningRequest 81](#_Toc480329647)

[11.22 SessionKeySigningResponse 82](#_Toc480329648)

[11.23 CountryData 83](#_Toc480329649)

[11.24 ProvinceData 84](#_Toc480329650)

[11.25 AccountVerificationData 84](#_Toc480329651)

[11.26 ErrorData 85](#_Toc480329652)

[11.27 FieldValidationConfig 86](#_Toc480329653)

[12 MDES Objects 88](#_Toc480329654)

[12.1 RegisterMobileAppRequest 88](#_Toc480329655)

[12.2 RegisterMobileAppResponse 88](#_Toc480329656)

[12.3 CheckEligibilityRequest 88](#_Toc480329657)

[12.4 CheckEligibilityResponse 88](#_Toc480329658)

[12.5 DigitizationRequest 89](#_Toc480329659)

[12.6 ActivateTokenRequest 89](#_Toc480329660)

[13 Appendix 90](#_Toc480329661)

[14 References 96](#_Toc480329662)

# Introduction

## Overview

This document is the API specification for Wallet services in BMO Masterpass Wallet. Wallet services specifically refer to services consumed by wallet client (either mobile wallet app or web wallet client).

Broadly it covers following APIs –

* Wallet account and lifecycle management API
* Mobile app instance and device management API
* Payment card setup with digitization, tokenization and lifecycle management API
* Masterpass checkout services API
* Address management API

## Using This Document

The document is a technical specification of the APIs. It is assumed that the reader is familiar with the high-level use cases supported by wallet product. Refer to the DRS document for more information.

The intended audience includes

* Wallet design and implementation team
* Product management team adding enhancements and modifications to the product.
* IT teams including hosting, production support and web engineering to understand the integration dependencies

## Revision History

| Date | Version | Author | Change Log |
| --- | --- | --- | --- |
|  |  |  |  |

## Document Conventions

| Convention | Description |
| --- | --- |
| Arial | General Description |
| Courier New | Example of Communication message format |

## Acronyms

| Acronym | Description |
| --- | --- |
| WS | Wallet Server |
| WC | Wallet Client |
| MDES | Mastercard Digital Enablement Service |
| JOSE | JSON Object Signing & Encryption |
| JWE | JSON Web Encryption |
| ECDH | Elliptic Curve Diffie–Hellman |
| PBES2 | Password-Based Encryption Scheme |
| OWASP | Open Web Application Security Project |
| API | Application Programming Interface |
| RPC | Remote Procedure Call |
| MPA | Mobile Payment Application |
| TSP | Token Service Provider |

## References

| Document Name | Publisher |
| --- | --- |
| DRS | BMO |

# General

## API Overview

Wallet Services API is a set of standard APIs that allows wallet clients to perform the below operations communicating with wallet server or related backend application –

* Wallet account and lifecycle management
* Mobile app instance and device management
* Payment card setup with digitization, tokenization and lifecycle management
* Masterpass checkout services
* Address management

Generally APIs are designed to be multi-channel and hence can be consumed by types of wallet clients with configurations related to Message envelope and related security features. Please refer Message envelope section for further details.

Certain APIs may be specific to a wallet client channel and hence is optimized accordingly.

## API Design

Wallet Services API are RPC style stateless APIs.

## Message Envelope

Message envelope refers to the message payload structure that is exchanged between wallet client and server during API calls.

Generally APIs are designed to be multi-channel and hence can be consumed by types of wallet clients with configurations related to Message envelope and related security features. There are client channel specific optimization specifically related to message level security and hence message envelope varies as per client channel.

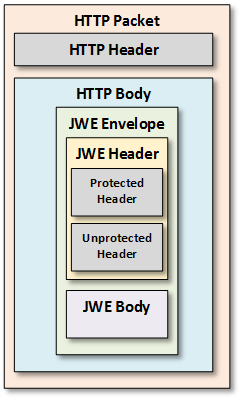
Below section describes various message envelope types

### JWE Envelope

JWE envelope serves as the message envelope exchanged over HTTP/TLS. Logically, JWE envelope is divided into two parts – header and body.

Generally header part will contain service agnostic parameters and body part will contain service specific parameters.

Below is the pictorial representation of JWE envelope.



Below table explain each of the part of above-mentioned envelope. It also provides guidelines on which data should be placed in which part of the envelope.

| Envelope Component | Guideline for placing Data |
| --- | --- |
| HTTP Header | Service agnostic or generic parameters, which are, require prior to processing of JWE envelope should be placed here. It is secured by HTTP/TLS for data confidentiality. |
| HTTP Body | Actual payload resides here in form of JWE compliant message envelope. It is secured by HTTP/TLS for data confidentiality. |
| JWE Protected Header | For sensitive header values, this header must be used. On top of HTTP/TLS security measures, these header values are signed at application level to verify data integrity for it |
| JWE Unprotected Header | These header values are only secured by HTTP/TLS and should be used to carry non-sensitive or critical header level values. |
| JWE Body | Service specific message body is to be placed here. |

#### HTTP Headers

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| tenantId | String | Y | 25 | Unique identifier of a tenant i.e. wallet provider or issuer |
| locale | String | N | 10 | Device locale set by application on top of Accept-Language header value following BCP 47. |
| messageId | String | Y | 64 | Unique message identifier generated by client for each request to detect and prevent message replay attacks. |
| OCIF\_ID | String | O | 13 | BMO BOK Customer ID from OCIF System. This header will be injected by ISAM after a Customer is signed in to BMO Mobile Banking or Online Banking System |

#### JWE Protected Headers

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| appInstanceId | String | Conditional | 36 | Unique identifier of the Wallet Application instance consuming the service. Present in request as protected header  All the requests made by wallet client prior to registration and login (adding new mobile app into existing account scenario) will not have this field. |
| walletId | String | Conditional | 36 | Unique identifier of the Wallet Account to which Wallet Application instance is associated with.  All the requests made by wallet client prior to registration & login will not have this field. |
| rootedDeviceInfo | String | Y | 32 | Indicator whether the device has been rooted or not. Based on the value server will take appropriate action. |
| deviceFingerprint | String | Y | 256 | This field uniquely identifies the device. There are different algorithms for generating device fingerprint for Android and iOS. |
| applicationData | [ApplicationData](#_ApplicationDetails_1) | Y | N/A | Application information. Please refer [ApplicationDetails](#_ApplicationDetails) object structure for more details. |
| osData | [OSData](#_OSData) | Y | N/A | Operating system information refer [OSDetails](#_OSDetails) object structure for more details. |
| serverTimestamp | String | Y | 50 | This number (long) timestamp will be used to prevent “Replay Transmitted Data”. |
| safetyNetData | [SafetyNetData](#_SafetyNetData) | Conditional | N/A | Google SafetyNet JWS Payload for verification. Please refer [SafetyNetData](#_SafetyNetData) object structure for more details.  Only following set of APIs request needs to have safety net details   * Check Device Eligibility * Wallet Registration |

#### JWE Unprotected Headers

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |

## API Security and Validations

### Message Confidentiality

All API interactions between wallet client and services are protected and authenticated using TLS. Hence all request and response data are passed within HTTP header or body and not supported in URL as query string parameters.

For custom dedicated deployments, TLS 1+ version is strongly recommended.

### Message Replay Attack Detection and Mitigation

API provides a mechanism to detect and mitigate message replay attack scenarios. It expects a nonce as unique message identifier to be provided by client for each API invocation. API preserves and remembers the message identifier for a configured amount of time in replay cache during which message with previous message identifier won’t be accepted and entertained. Such message with recurring ID will be treated as replayed message.

### JWE based Mobile API Security

This API security scheme is applicable for mobile app channels and is a client server scheme to ensure end to end message level security including message integrity, authentication. The scheme aligns with JWE and JWK standards for protecting JSON messages.

JWK is leveraged for sharing the public key from services application (wallet server or similar) to mobile consumer apps.

JWE standard is leveraged for message authentication and integrity. On top of leveraging JWE, the scheme provides variations for message security based on availability and applicability of the secure credentials like PIN or token. This is described as below –

### Authentication

**Authentication Initialization**

* For API interaction where Mobile App PIN or token (Wallet PIN or similar) is not setup or available, PKI is leveraged for secure keys sharing. In this scheme, both sender and recipient use key pair to provide an ECDH or RSA based secret key sharing and encryption scheme to protect the messages.
* API examples include Registration, Reset Credentials like Reset PIN etc.

**Authenticated Access**

* For cases where Mobile App PIN or token (Wallet PIN or similar) is setup or available, it is leveraged to generate shared secret further used to protect the messages.
* API examples include post login services and transactions.

**Device based Authentication**

* **Device Fingerprint Validation** - If user is using Wallet Client from a mobile device, Wallet Server compares device fingerprint received in request with the one stored in DB. If they do not match, Authorization will be failed.
* **SafetyNet Attestation** - The SafetyNet API from Google Inc. is designed to check whether a device has been tampered with or not. If user is using Wallet Client from a mobile device, Wallet Server verifies SafetyNet attestation response received from Google API and assesses various error scenarios.

### Session Control

Wallet Server follow REST like architecture style and hence all APIs exposed are stateless and there is no session management for mobile device users. This stateless nature of requires mobile wallet client & wallet server to implement message expiry validation which is described below.

* **Message Expiry Validation**

Due to stateless nature of wallet service APIs, irrespective of user logged in or logged out of mobile wallet application, as long as “Message ID” (which is passed to prevent message replay detection & prevention) present in request is valid, wallet server has no reason to consider request as a threat. And hence, wallet server is vulnerable to network attacks in which valid data transmission is fraudulently repeated after “Message ID” expiry period.

To eliminate the risk, wallet server (in co-ordination with wallet mobile app) implement message expiry validation using wallet server and mobile device timestamp values.

### Input Validation

Following input validations are performed for every API invocation –

* **Request validation** per API for syntax & possible values validations
* **SQL and XSS Injection Checks** - API service validates the input data based on the black listed character set and it will decline the request if the validation fails.
  + API checks following regular expression for whitelisting -
    - ([A-Za-z0-9,\\(\\)\\[\\]\\{\\}\\?\\-\\+\\=\\@\\%\\:.\\/\_\\s])\*
  + API checks following regular expression for whitelisting -
    - ^(.\*?(\\+\\+).\*?)$

### Mobile App & Device Validations

Following checks will be performed by Wallet Server to validate integrity of wallet mobile application and mobile device

* **App (Certificate) Checksum check** –whether mobile app binary istempered or not. Application should not run if it has been altered and signed with an illegal signing certificate, which is detected by comparing the App Certificate Checksum shared by the App/Wallet Provider with the App Certificate Checksum generated on Wallet Server using the stored App Certificate.
* **Rooted Device check** – whether mobile device is rooted or not

### Business Validations

All API request are validated against existing wallet state to ensure it is not impacting data integrity and consistency. Following cross cutting checks are performed –

* **Wallet provider status check** – whether wallet provider is in active state or not.
* **Wallet account availability check** – whether account is available and is not in suspended or terminated state
* **Wallet app instance and device check**
  + Device is not blacklisted and is supported
  + Device Fingerprint based validations
  + Wallet app instance account status checks for validity

As per business needs, specific or custom validation may be applied for certain API calls.

## URL Scheme

This section describes overall API specification URL scheme.

Wallet service APIs for both web and mobile app wallet channels has API version associated with it. This API version reflects the API specification version that outlines and describes those APIs. API version is specified as part of API URL.

General API URL scheme is as follows -

scheme://host[:port]/contextRoot/{channel}/{apiType}/api/{majorVerion}/{minorVersion}/\*

### URL Elements

| **URL Element** | **Description** |
| --- | --- |
| **scheme** | http(s) |
| **host:[port]** | Host name and optional port number of wallet server |
| **contextRoot** | Context root to identify the individual component services or application. In general, below conventions is recommended   * Wallet Services - /wallet * Admin Console Services - /wallet/admin * Wallet CSR Services - /wallet/csr |
| **channel** | * web * mobile |
| **apiType** | Please refer below description for details. Possible values:   * public * private * resource |
| **majorVersion** | Major version of API |
| **minorVersion** | Minor version of API reflecting changes related to bug fixes, patches etc. |
| **api\_relative\_uri** | Relative API URI that identifies and invoke a specific API |

With some hosting environment, there is a need to differentiate within APIs consumed by web clients to specify which API specifically needs authentication/authorization and validation checks by some external identity propagation & validation infrastructure. The configurations related to this need are made in identity propagation & validation infrastructure and it needs a mechanism in API URL to identify itself as a public or private API. Please refer table for API types and description –

| **Web API Type** | **Description** |
| --- | --- |
| **Public API** | API, which doesn’t, need any session control based authentication and authorization. |
| **Private API** | API which can only be accessed post session authentication and initialization. |
| **Static Resource API** | This is the API that doesn’t require any authentication and authorization. Also data exchanged using these APIs are in plain. Typically all the images and static content retrieval APIs are such kind of APIs. |

## API Data Elements

### Date and Time Format

Format of date and time used in APIs follows ISO 8601 format i.e. YYYY-MM-DDThh:mm:ssZ format. Note that UTC time zone will be followed for date and time. Details are as below -

* YYYY = four-digits year
* MM = two digits month (01 = January etc.)
* DD = two digits day of month (01 through 31)
* T = Indicates beginning of time element
* hh = two digits of hour (00 through 23) (am/pm NOT allowed)
* mm = two digits of minute (00 through 59)
* ss = two digits of second (00 through 59)
* Z = Denotes UTC time zone

Example Date: 1997-07-16T19:20:30Z

### UUID

All unique IDs provided by APIs specifically entity IDs including Wallet ID, Payment Card ID etc. are 16 byte or 36 character strings. ID generation is compliant with RFC 4122.

### Response Code and Message

In general, API response will have HTTP status code as per the API invocation result. Some of the common HTTP status codes are as below –

* 200 – OK
* 500 – Internal Server Error

Additionally all API level error or exception (HTTP response status code 200) will be reported via **errors** object in response containing API specific **responseCode** and **responseDescription.** Please refer [ErrorData](#_ErrorData_1) object for details.

**Sample**

{

"errors": [{

"responseDescription”: "",

"responseCode": "",

"inputField": ""

}]

}

# Wallet Account Management Services

## Get Certificate Chain

### Overview

This public API is used to download the public key certificate which is used to enable PKI key agreement based communication security for APIs calls from mobile clients.

This API does not requires JOSE based communication security.

### API Relative URI

/device/certificate/jwk

### HTTP Method

GET

### Request Parameters

No specific attributes required in request.

### Response Parameters

Response data contains a file of MIME type "application/pkix-cert"

### Sample Request

N/A

### Sample Response

N/A

### Exceptions

No API specific exceptions will be thrown.

## Get Public Key Certificate

### Overview

This public API is used to download the public key certificate which is used to wrap the randomly-generated key (RGK) during the MDES MPA registration process.

This API does not requires JOSE based communication security.

### API Relative URI

/device/certificate/mpa

### HTTP Method

GET

### Request Parameters

No specific attributes required in request.

### Response Parameters

Response data contains a file of MIME type "application/pkix-cert"

### Sample Request

N/A

### Sample Response

N/A

### Exceptions

No service specific exceptions will be thrown.

## Check Device Eligibility

### Overview

This public API check and determine whether the device from which request has been originated is whitelisted on wallet server or not. In case device is not configured as whitelist device or is being blacklisted, API returns appropriate error. Mobile App will pass OS details in JWE protected headers.

Mobile App will invoke this API on first lunch using ECDH based JOSE communication.

### Relative API URI

/device/eligibility/check

### HTTP Method

**POST**

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| deviceEligibilityData | [DeviceEligibilityData](#_DeviceEligibilityDetails) | Yes | N/A | Device Eligibility Rules Configuration Details |

### Response Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| result | Boolean | Yes | N/A | Device Eligibility Result. |
| salt | String | Yes | 256 | Base 64 encoded salt for hashing wallet PIN |

### Sample Request

TBD

### Sample Response

TBD

### Exceptions

| Response Code | Response Message | Description |
| --- | --- | --- |
| OS\_NOT\_SUPPORTED | Operating System is not supported by Wallet Provider | OS is not whitelisted as per Wallet Provider hence wallet app cannot be used. |
| OS\_VER\_NOT\_SUPPORTED | Operating System Version is not supported by Wallet Provider | OS is blacklisted as per Wallet Provider hence wallet app cannot be used. |
| OEM\_NOT\_SUPPORTED | Original Equipment Manufacturer is not supported by Wallet Provider | OEM is not whitelisted as per Wallet Provider hence wallet app cannot be used. |
| MODEL\_NOT\_SUPPORTED | Device Model is not supported by Wallet Provider | Device Model is not whitelisted as per Wallet Provider hence wallet app cannot be used. |

## Get Latest Legal Docs

### Overview

This public API is responsible for retrieving wallet provider’s latest legal documents metadata. Legal document’s metadata can then further be used by client to download legal documents contents.

Mobile App will invoke this API using ECDH based JOSE communication.

### Relative API URI

/legaldoc/retrieve

### HTTP Method

**POST**

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| locale | String | Yes | 5 | Locale in which legal documents should be provided |

### Response Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| legalDocs | Array[[LegalDocData](#_LegalDocDetails)] | Yes | N/A | Latest legal document details |

### Sample Request

N/A

### Sample Response

TBD

### Exceptions

No service specific exceptions will be thrown.

## Register Wallet Account

### Overview

This public API is responsible for initializing wallet account and/or wallet instance (mobile app instance) record into the wallet server. In addition, this API may also initialize user record.

Mobile App will invoke this API using ECDH based JOSE communication.

### Relative API URI

/wallet/account/register

### HTTP Method

**POST**

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| userData | [UserData](#_UserDetails_1) | Mandatory | N/A | User details. |
| rnsData | [RNSData](#_AppInstanceDetails) | Mandatory – If request is originated from mobile wallet. | N/A | Remote notification service registration details |
| deviceInstanceData | [DeviceInstanceData](#_ApplicationDetails) | Mandatory – If request is originated from mobile wallet. | N/A | Device Instance details |
| deviceProfileData | [DeviceProfileData](#_DeviceProfileDetails) | Mandatory – If request is originated from mobile wallet. | N/A | Device Profile details |

### Response Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| walletAccountId | String | Yes | 36 | Wallet Account Unique Identifier |
| appInstanceId | String | Mandatory – If request was originated from mobile wallet | 36 | App Instance Unique Identifier |
| paymentAppInstanceId | String | Mandatory – If request was originated from mobile wallet | 48 | Payment App Instance ID generated by server as per MDES specifications |

### Sample Request

TBD

### Sample Response

TBD

### Exceptions

| Response Code | Response Message | Description |
| --- | --- | --- |
| USER\_ALREADY\_EXIST | User already exists | User with given email address or mobile number is already registered. |

## Retrieve User Profile

### Overview

This private API is responsible for retrieve user profile associated with wallet account.

Mobile App will invoke this API using PBES based JOSE communication.

### URL

/wallet/account/profile/retrieve

### HTTP Method

**POST**

### Request Parameters

No specific attributes required in request.

### Response Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| userData | [UserData](#_UserDetails_1) | Yes | N/A | User details associated with wallet account. Only following parameters will be returned to wallet client.   * firstName * lastName * email * mobileNumber |

### Sample Request

TBD

### Sample Response

TBD

### Exceptions

No specific exceptions will be thrown.

## 

## Update User Accepted Legal Doc

### Overview

This private API is for updating user accepted legal doc details (versions & their respective timestamps) in wallet account.

Mobile App will invoke this API using PBES based JOSE communication.

### API Relative URI

/wallet/account/legaldoc/update

### HTTP Method

**POST**

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| legalDocAcceptanceData | Array[[LegalDocAcceptanceData](#_LegalDocAcceptanceDetails)] | Y | N/A | User Accepted Legal Doc Details |

### Response Parameters

No API specific response parameters will be returned. In case of any error, API will return error(s) object.

### Sample Request

TBD

### Sample Response

TBD

### Exceptions

No specific exceptions will be thrown.

# PIN Management API

This section describes services manage PIN of mobile wallet app

## Authenticate Wallet

### Overview

This public API is responsible to authenticate mobile app instance using wallet pin.

Mobile App will invoke this API using ECDH based JOSE communication.

### API Relative URI

/wallet/appinstance/authenticate

### HTTP Method

**POST**

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| walletPIN | String | Yes | N/A | User selected/entered hashed value of PIN |

### Response Parameters

No service specific parameters will be returned.

### Sample Request

TBD

### Sample Response

TBD

### Exceptions

No specific exceptions will be thrown.

# Payment Card Management Services

This section describes services used to add and manage Payment Cards.

## Retrieve Payment Cards

### Overview

This private API is responsible for retrieving a payment card(s), their billing address and associated token details from wallet server. If paymentCardId is not provided in the request then all the payment cards of a particular wallet (identified by wallet mobile app instance identifier) account will be returned.

* If paymentCardId does not exists with wallet server or no payment cards added in wallet account, empty response will be returned
* If request is from mobile app, tokens which are specific to app instance identified by appInstanceId header parameter will be returned.

Mobile App will invoke this service using PBES2 based JOSE communication.

### URL

/paymentcard/retrieve

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| paymentCardId | String | Conditional – if not provided, all payment card of a wallet account will be returned | 36 | Unique identifier of payment card in Wallet Server. |
| includeCardTokens | Boolean | N | N/A | Indicate if payment card tokens needs to be retrieve along with payment card details.  Default value: TRUE |
| includeBillingAddress | Boolean | N | N/A | Indicates if billing address need to be retrieved along with payment card details. Default value: TRUE |
| includeOnlyActive | Boolean | N | N/A | Indicates if only active cards need to be retrieved.  Default value: TRUE |

### Response Parameters

| Attributes | | Type | | Mandatory | Max Length | | Description |
| --- | --- | --- | --- | --- | --- | --- | --- |
| paymentCards | | Array[[PaymentCardData](#_PaymentCardInfo)] | Y | | N/A | Payment Card Object. | |

### Sample Request

{  
   "paymentCardId": "9586b69a-c2b7-4f3b-b31a-937c0c60d550",  
   "includeCardTokens": true,  
   "includeOnlyActive": true,  
   "includeBillingAddress": true  
}

### Sample Response

{  
   "paymentCards": [  
      {  
         "paymentCardId": "9586b69a-c2b7-4f3b-b31a-937c0c60d550",  
         "status": "ACTIVE",  
         "isPreferred": true,  
         "accountPANSuffix": "â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢7844",  
         "expiryMonth": "10",  
         "expiryYear": "2019",  
         "cardBrandData": {  
            "name": "master",  
            "code": "master"  
         },  
         "billingAddressData": {  
            "line1": "100 1st Street",  
            "line2": "test@321",  
            "line3": "123",  
            "city": "St. Louis",  
            "province": "CA",  
            "countryCode": "USA",  
            "postalCode": "61000",  
            "recepientName": "RECNAMEYCK",  
            "mobileNumber": {  
               "number": "1481362805",  
               "countryCode": "+91"  
            }  
         },  
         "cardTokenData": [  
            {  
               "tokenUniqueReference": "DGENMC0000000001c04efef2798b4d90b29b849022954f6b",  
               "tokenPANSuffix": "6923"  
            }  
         ],  
         "panUniqueReference": "FGENMC00000000014e103afb84ad4df38c88a3b4f11a7b11"  
      }  
   ]  
}

### Exceptions

No specific exceptions will be thrown.

## Set Payment Card as Default

### Overview

This private API is responsible for setting a payment card as default. Before marking payment card in request as default, preferred flag on any existing payment card in wallet account will be set to false.

Mobile App will invoke this service using PBES2 based JOSE communication.

### URL

/paymentcard/setdefault

### HTTP Method

POST

### Request Parameters

| Attributes | | Type | | Mandatory | | Max Length | | Description | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| paymentCardId | | String | | Y | | 36 | | Unique identifier of payment card in Wallet Server. | |

### Response Parameters

No specific response parameters will be returned. In case of any error, API will return error(s) object.

### Sample Request

TBA

### Sample Response

TBA

### Exceptions

| Response Code | | Response Message | | Description | |
| --- | --- | --- | --- | --- | --- |
| PAYMENT\_CARD\_NOT\_FOUND | | Payment Card not found | | Payment Card not found | |
| PAYMENT\_CARD\_NOT\_ACTIVE | | Payment card is not in active state. | | Payment card is not in active state. | |

## Retrieve Payment Card Assets

### Overview

This private API is responsible for retrieving asset from Wallet Server based on an asset identifier provided by token service provider.

### URL

/paymentcard/asset

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| assetId | String | Y | 64 | Asset identifier provided by TSP |
| cardBrandCode | String | Y | 64 | Card brand code. For possible values, please refer [CardBrandData](#_PaymentCardBrandDetails) object code field description. |

### Response Parameters

Response will contain requested asset data. HTTP header parameter “Content-type” & “Content-length” should be used by client to identify content type & content length

### Sample Request

{    
   "assetId":"1978cc5b-df15-437d-b23e-9ba4c4d0a603",  
   "cardBrandCode":"master"  
}

### Sample Response

{    
   "mediaContents":[    
      {    
         "type":"image/png",  
         "height":"375",  
         "width":"375",  
         "data":"iVBORw0KGgoAAAANSUhEUgAAAXcAAAF3CAIAAADRopypAAAABGdBTUEAANbY1E9YMgAAAAlwSFlzAAAASAAAAEgARslrPgAAGtNJREFUeNrt3W9oW+"  
      }  
   ]  
}

### Exceptions

No service specific exception will be returned.

## Activate Payment Card Token

### Overview

This private API is responsible to activate token either using authentication code or using tokenization authentication value with TSP. If verification is successful, token will be activated.

Mobile App will invoke this service using PBES2 based JOSE communication.

### URL

/paymentcard/token/activate

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| activateTokenRequest | [ActivateTokenRequest](#_ActivateTokenRequest) | Y | N/A | Please refer ActivateTokenRequest for details |

### Response Parameters

No specific response parameters will be returned. In case of any error, API will return error(s) object.

### Sample Request

{    
   "tokenUniqueReference":"DGENMC000000000135fe076fa7164f9d88ec831fb04d6bf7",  
   "authenticationCode":"1234"  
}

### Sample Response

{}

### Exceptions

| Response Code | Response Message | Description |
| --- | --- | --- |
| INVALID\_TUR | Invalid TUR | Invalid TUR |
| INVALID\_TOKEN\_STATUS | Token is not in desired state | Token is not in desired state |
| INCORRECT\_CODE | Authentication Code was incorrect and rejected. Retries permitted | Authentication Code was incorrect and rejected. Retries permitted |
| INCORRECT\_CODE\_RETRIES\_EXCEEDED | Authentication Code was incorrect and the maximum number of retries now exceeded. | Authentication Code was incorrect and the maximum number of retries now exceeded. |
| EXPIRED\_CODE | Authentication Code has expired or was invalidated. | Authentication Code has expired or was invalidated. |
| INCORRECT\_TAV | Tokenization Authentication Value was incorrect and rejected. | Tokenization Authentication Value was incorrect and rejected. |
| EXPIRED\_SESSION | The Token cannot be activated because the digitization session has expired. The caller must delete any artifacts relating to the Token and restart the process from the beginning. | The Token cannot be activated because the digitization session has expired. The caller must delete any artifacts relating to the Token and restart the process from the beginning. |

# Shipping Address Management Services

This section describes APIs used to manage shipping addresses.

## Add Shipping Addresses

### Overview

This private API is responsible to add shipping addresses into wallet account. Client can provider more than one shipping address details, **maximum five**, in request.

Mobile App will invoke this service using PBES2 based JOSE communication.

### URL

/shippingaddress/add

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| addresses | Array[AddAddressRequest] | Y | N/A | Please refer below table for add address request structure. |

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| addressRecordId | String | Conditional – required only if more than one shipping address details provided in request | 50 | Unique shipping address record (in request) identifier generated by client. Same identifier will be return in response to map request with response details. |
| addressData | [AddressData](#_CheckEligibilityData) | Yes | N/A | Address details. |

### Response Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| response | Array[AddAddressResponse] | Y | N/A | Please refer below table for add address response structure. |

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| addressRecordId | String | Conditional – required only if more than one shipping address details provided in request | 50 | Shipping address record identifier provided by client in request. |
| addressId | String | Conditional – required only if address data successfully added in wallet | 36 | Unique identifier of shipping address assigned by Wallet Server. |
| errors | Array[[ErrorData](#_ErrorData)] | Conditional – required only in case of error while processing request | N/A | Error Object. |

### Sample Request

{

"addresses": [

{

"addressRecordId": "1",

"addressData": {

"alias": "Sam",

"firstName": "Sam1",

"lastName": "user",

"line1": "address1",

"line2": "address2",

"line3": "address3",

"city": "US",

"province": "usgov",

"countryCode": "91",

"postalCode": "5555555555",

"mobileNumber": "8989898989",

"recepientName": "user1"

}

},

{

"addressRecordId": "2",

"addressData": {

"alias": "Sam",

"firstName": "Sam1",

"lastName": "user",

"line1": "address1",

"line2": "address2",

"line3": "address3",

"city": "US",

"province": "usgov",

"countryCode": "91",

"postalCode": "5555555555",

"mobileNumber": "8989898989",

"recepientName": "user1"

}

}

]

}

### Sample Response

{

"response": [

{

"addressRecordId": "123456",

"addressId": "0095ad3b-e66a-4987-929f-436e3b8513cf"

},

{

"addressRecordId": "123457",

"addressId": "e7dddd76-0bca-49d7-a3e6-cd0f4ce1a3eb"

}

]

}

### Exceptions

No service specific exception will be returned.

## Update Shipping Address

### Overview

This private API is responsible for updating shipping address.

Mobile App will invoke this service using PBES2 based JOSE communication.

### URL

/shippingaddress/update

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| addressId | String | Y | 36 | Unique identifier of address in Wallet Server. |
| addressData | [AddressData](#_CheckEligibilityData) | Yes | N/A | Address details. |

### Response Parameters

No specific response parameters will be returned. In case of any error, API will return error(s) object.

### Sample Request

{

"addressId" : "f30b40b5-02ec-4a71-bdbb-944deee52fc7",

"addressData" : {

"alias" : "test",

"firstName" : "John1",

"lastName" : "Chalie",

"line1" : "Apex avenue",

"line2" : "123 sid",

"line3" : "dsf main",

"city" : "st charles",

"province" : "MO",

"countryCode" : "USA",

"postalCode" : "3078530785",

"mobileNumber" : {

"number" : "1485514385",

"countryCode" : "+91"

},

"recepientName" : "FNAMEYCK"

}

}

### Sample Response

{ }

### Exceptions

| Response Code | | Response Message | | Description | |
| --- | --- | --- | --- | --- | --- |
| SHIPPING\_ADDRESS\_NOT\_FOUND | | Shipping address not found | | Shipping address not found | |

## Retrieve Shipping Addresses

### Overview

This service is responsible to retrieve address based on address identifier. If addressId is not provided in the request then all the shipping addresses of a particular wallet account will be returned. If addressId does not exists with wallet server or no shipping addresses added in wallet account, empty response will be returned

Mobile App will invoke this service using PBES2 based JOSE communication.

### URL

/shippingaddress/retrieve

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| addressId | String | N | 36 | Unique identifier of address in Wallet Server. |

### Response Parameters

| Attributes | Type | Mandatory | Length | Description |
| --- | --- | --- | --- | --- |
| shippingAddresses | Array[[ShippingAddressData](#_ShippingAddressDetails)] | Yes | N/A | Address details. |

### Sample Request

{

"addressId":"0095ad3b-e66a-4987-929f-436e3b8513cf"

}

### Sample Response

{

"shippingAddresses": [

{

"addressId": "376d34ec-a102-41bb-bafc-a813a8a343bf",

"status": "ACTIVE",

"isPreferred": true,

"addressData": {

"alias": "test",

"firstName": "Pooja",

"lastName": "Jaiswal",

"line1": "37",

"line2": "37",

"line3": "37",

"city": "CALI",

"province": "CA",

"countryCode": "USA",

"postalCode": "61000",

"recepientName": "Pooja",

"mobileNumber": {

"number": "9487548752",

"countryCode": "+11"

}

}

}

]

}

### Exceptions

No specific exceptions will be thrown.

## Set Shipping Address as Default

### Overview

This private API is responsible for setting shipping address as default.

Mobile App will invoke this service using PBES2 based JOSE communication.

### URL

/shippingaddress/setdefault

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| addressId | String | Y | 36 | Unique identifier of address in Wallet Server. |

### Response Parameters

No specific response parameters will be returned. In case of any error, API will return error(s) object.

### Sample Request

{

"addressId" : "8479a391-db4a-4f8b-a0dd-b9f35b906847"

}

### Sample Response

{ }

### Exceptions

| Response Code | | Response Message | | Description | |
| --- | --- | --- | --- | --- | --- |
| SHIPPING\_ADDRESS\_NOT\_FOUND | | Shipping address not found | | Shipping address not found | |

## Delete Shipping Address

### Overview

This private API is responsible to delete address based on addressId.

Mobile App will invoke this service using PBES2 based JOSE communication.

### URL

/shippingaddress/delete

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| addressId | String | Y | 36 | Unique identifier of address in Wallet Server. |

### Response Parameters

No service specific parameters will be returned.

### Sample Request

{

"addressId" : "f2335dfd-01c2-4fe6-92d0-64b6c66ed58d"

}

### Sample Response

{ }

### Exceptions

| Response Code | Response Message | Description |
| --- | --- | --- |
| SHIPPING\_ADDRESS\_NOT\_FOUND | No address found. | Unable to find address based on alias or id. |

# Other Services

## Retrieve Countries

### Overview

This public API is responsible for providing wallet provider supported countries to client. API also provides province details based on request parameter flag “includeProvinces”.

Mobile App will invoke this service using ECDH based JOSE communication.

### URL

country/retrieve

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| includeProvinces | Boolean | Y | N/A | Flag to indicate if response should include province details. Default value is FALSE. |

### Response Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| countries | Array[[CountryData](#_CountryData)] | Y | N/A | List of wallet provider supported countries. |

### Sample Request

N/A

### Sample Response

N/A

### Exceptions

No specific exception will be returned.

## Retrieve field configuration

### Overview

This public API is responsible for providing custom field configurations based on county code and category. The default configuration will be returned if not found for given country.

Mobile App will invoke this service using ECDH based JOSE communication.

### URL

fieldconfig/retrieve

### HTTP Method

POST

### Request Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| countryCode | String | Y | N/A | Three letter ISO country code. |
| category | String | Y | N/A | Category of field. Possible values : ADDRESS, CUSTOM |

### Response Parameters

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| fieldValidationConfigs | Array[[FieldValidationConfig](#_FieldValidationConfig)] | Y | N/A | List of field configuration. |

### Sample Request

N/A

### Sample Response

N/A

### Exceptions

No specific exception will be returned.

# Masterpass Checkout Services

## Initialize Checkout

### Overview

Shoppers will be directed to the Partner site via a checkout initialization URL. Partners must inform Mastercard of this URL as part of the integration process in order for this flow to be configured. Masterpass will execute this URL when the user selects the Partner-hosted wallet. Masterpass will append the set of parameters to the request based on which version of Masterpass the merchant has implemented. Please refer <https://www.mastercard.com/mc_us/wallet/guides/partnerwallet/phw/index.html#me_section_9> for parameter details.

This public API is only applicable for web channel.

### URL

checkout/init?merchant\_return\_url={merchant\_return\_urlflow=checkout&locale={locale}&targetOrigin={targetOrigin}&clientOrigin={clientOrigin}&walletId={walletId}&acceptable\_cards={acceptable\_cards}&checkout\_identifier={checkout\_identifier}&requestedDataTypes=&oauth\_token={oauth\_token}&pairingRequestToken={pairingRequestToken}&checkout\_version=6&merchant\_name={merchant\_name}&merchant\_logo\_url={merchant\_logo\_url}&auth\_options={auth\_option}&cardinal\_merchant\_id={cardinal\_merchant\_id}&amount={amount}&currency={currency}&order\_number={order\_number}&suppress\_shipping\_address={true/false}&merchantSuppressSignup={true/false}

### HTTP Method

GET

### Request Parameters

No parameters except mentioned in the URL.

### Response Parameters

No specific parameter will be returned.

### Sample Request

N/A

### Sample Response

N/A

### Exceptions

No specific exception will be returned.

## Authorize Checkout

### Overview

After the consumer selects card and shipping information using a wallet, the partner (wallet provider) must invoke the Mastercard Checkout Authorization Service, via Open API. This is the API a partner must use to authorize the merchant to access a consumer’s checkout data.

Mobile App will invoke this service using PBES2 based JOSE communication.

### URL

checkout/authorize

### HTTP Method

POST

### Request Parameter

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| merchantCheckoutId | String | Y | 36 | Merchant checkout identifier |
| oAuthToken | String | Y | 50 | Authentication token for checkout |
| checkoutSelectionData | [CheckoutSelectionData](#_CheckoutSelectionData) | Y | NA | Check Selection Data |
| sessionKeySigningRequest | [SessionKeySigningRequest](#_SessionKeySigningRequestDetails) | N | NA | Calling app details for switch signing. Signature will be returned in response for application verification. |

### Response Parameter

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| id | String | Y | 36 | Checkout Identifier |
| merchantCallbackUrl | String | Y | 500 | This is the merchant callback URL that is returned from Masterpass switch. This URLembeds all the information needed by the merchant to proceed with the checkout. |
| oAuthVerifier | String | Y | 50 | Verifier the merchant will use to retrieve a single-use access token |
| stepupPending | Boolean | Y | NA | True if 3DS is required for a card being passed in the checkout data |
| sessionSigningResponse | [SessionSigningResponse](#_SessionKeySigningResponse) | N | N/A | Switch signing response details. Calling app should verify signature using switch key to ensure checkout is authorized by switch. |

### Sample Request

{

"merchantCheckoutId": "a4d6w3g1jd6s2hkx59jxb1hkzrowz51jj2",

"oAuthToken": "123",

"checkoutSelectionData": {

"paymentCardId": "6e963862-7c59-4a49-bf72-2b5833ceeaca",

"loyaltyCardId": "d819ef76-3e31-4d55-b37c-9b06fa17c67a",

"digitalGoods": false,

"shippingAddressId": "1e37feb3-7d65-45e7-a2cb-d514c601abb4",

"dSRPData": {

"tokenAccountNumber": "TAN",

"cryptogram": "12322",

"unpredictableNumber": "4465654",

"cryptogramType": "UCAF",

"tokenExpiryMonth": "02",

"tokenExpiryYear": "4444"

}

},

"sessionKeySigningRequest": {

"appId": "anksdgiasgd",

"appVersion": "1.0.0",

"appSigningPublicKey": "a6s5d6s5d4f5s4d5f4s5G654FFV4sd65f46s7g4354df34d68f7hg6df874h3687fdh687"

}

}

### Sample Response

{

"id": "62b13d1a-a033-41f0-9946-57ee19a9f47a",

"merchantCallbackUrl": "https://stage2.masterpass.com/lightbox/Switch/callback.html?oauth\_token=709d0539eacc729bf96a40f14089426334c43244&oauth\_verifier=1980149fb6306b1ebfd4988de25c863b2226fd95&checkoutId=102471478&checkout\_resource\_url=https%3A%2F%2Fstage.api.mastercard.com%2Fstage2%2Fmasterpass%2Fv6%2Fcheckout%2F102471478",

"stepupPending": false,

"sessionSigningResponse": {

"sessionSignature": "s6df54g065dsf40g5454SD60F54S0D65F40SD6F049d7f98s73s2d1f0ss8d7f987yuiy98i7p87kjljm7b6v5424sd654f4v015s48df7f7hgjkioll0"

},

"oAuthVerifier": "54qwerdfs89g764hgj3g5h43131jk5374h6j87kl87kl2gv1nm32bvn1m8r54SD6FG4S32F1G31DFHG"

}

### Exceptions

| Response Code | Response Message | Description |
| --- | --- | --- |
| PAYMENT\_CARD\_NOT\_FOUND | Selected payment card not found. | Selected payment card not found. |
| BILLING\_ADDRESS\_NOT\_FOUND | Billing address not found. | Billing address not found. |
| SHIPPING\_ADDRESS\_NOT\_FOUND | Selected shipping address not found. | Selected shipping address not found. |
| LOYALTY\_CARD\_NOT\_FOUND | Selected loyalty card not found. | Selected loyalty card not found. |

# Generic Exceptions

This section contains list of generic errors which can be thrown by any of the service.

| Response Code | Response Message | Description |
| --- | --- | --- |
| General Error Codes | | |
| TECHNICAL\_ERROR | System is unable to process the request. Please try again after some time. | Technical error occurred. |
| INTERNAL\_SERVICE\_FAILURE | Back-end system is unavailable. | Back-end system is unavailable or some unknown error from respective backend. |
| INVALID\_INPUT | Invalid input parameter. | Invalid input parameter. |
| AUTHENTICATION\_FAILURE | Authentication failure | Authentication failure |
| AUTHENTICATION\_FAILURE\_LAST\_ATTEMPT | Authentication failure. Client has only one attempt left for authentication. | Authentication failure. Client has only one attempt left for authentication. |
| Mobile App & Device Specific Error Codes | | |
| FORCE\_UPGRADE\_REQUIRED | Please upgrade application to continue. | Application upgrade is required. |
| ROOTED\_DEVICE\_DETECTED | Rooted device detected. | Rooted device detected. |
| UNAUTHORIZED\_APPLICATION\_SOURCE | Application installed form unauthorized source. | Application installed form unauthorized source. |
| Wallet Provider Specific Error Codes | | |
| WALLET\_PROVIDER\_NOT\_FOUND | Wallet Provider (Tenant) not found | Unable to resolve wallet provider |
| WALLET\_PROVIDER\_LEGAL\_DOC\_UPGRADE\_REQUIRED | Please accept latest legal document(s) to continue. | New version of legal documents is available which needs to be accepted by the user before proceeding. |
| Wallet Account Specific Error Codes | | |
| WALLET\_ACCOUNT\_LOCKED | Wallet account is locked. | Wallet account is locked. |
| Wallet App Instance Specific Error Codes | | |
| APPINSTANCE\_LOCKED | App instance is locked. | App instance is locked. |
| APPINSTANCE\_SUSPENDED | App instance is suspended. | App instance is suspended. |
| APPINSTANCE\_TERMINATED | App instance is terminated. | App instance is terminated. |
| APPINSTANCE\_NOT\_ACTIVE | App instance is not active. | App instance is not active. |

# Push Notifications

## Description

TSP likes MDES notifies wallet server for various events like token status change, notification to retrieve new transaction details etc. As part of it, wallet server is expected to 1) store/update any details it is managing inside its own database and so that its state remains in sync with TSP and 2) to send push notification to mobile app so that it can synchronize its own state with wallet server.

This section describes payload structure of various push notifications sent by wallet server. In push notification, parameter “to” will contain a single registration token.

## Notify Token Updated

As part of notify token updated push notification, wallet server inform mobile app about change in state of a particular payment card token. Once notification is received by mobile app, it should download latest payment card details (associated with token unique reference) from wallet server.

### Message Parameter

| Attributes | Type | Mandatory | Max Length | Description |
| --- | --- | --- | --- | --- |
| turPrefix | String | Y | 6 | Token unique reference prefix whose status is changed. |
| turSuffix | [String](#_CheckoutSelectionData) | Y | 6 | Token unique reference suffix whose status is changed. This can be used by mobile app in case app find two TURs with same prefix |
| event | [String](#_CheckoutSelectionData) | Y | NA | Possible value(s): TOKEN\_STATUS\_CHANGED |

### Sample Message

{  
   "to" : "bk3RNwTe3H0:CI2k\_HHwgIpoDKCIZvvDMExUdFQ3P1…",  
   "data" : {  
 "turPrefix":"DWSP1a",

"turSuffix":"1a45df"

"event":"TOKEN\_STATUS\_CHANGED"

   }  
}

# Common Objects

## UserData

| **firstName** | |
| --- | --- |
| Description | First name of user. |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

| **lastName** | |
| --- | --- |
| Description | Last name of user. |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

| **password** | |
| --- | --- |
| Description | User password to access wallet account. |
| Data Type | String |
| Max Length | 100 |
| Required | Conditional – only required during registration |

| **mobileNumber** | |
| --- | --- |
| Description | Mobile number |
| Data Type | [MobileNumber](#_MobileNumber) |
| Max Length | N/A |
| Required | Yes |

| **email** | |
| --- | --- |
| Description | Email address of user. |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

| **countryOfResidence** | |
| --- | --- |
| Description | User country of residence. Expressed as a 3-letter (alpha-3) country code as defined in ISO 3166-1. |
| Data Type | String |
| Max Length | 3 |
| Required | Yes |

| **preferredLanguage** | |
| --- | --- |
| Description | User preferred language. Expressed as a 2-letter language code as defined in ISO 639-1. |
| Data Type | String |
| Max Length | 2 |
| Required | Yes |

| **legalDocAcceptanceData** | |
| --- | --- |
| Description | Legal document acceptance details |
| Data Type | [LegalDocAcceptanceData](#_LegalDocAcceptanceDetails) |
| Max Length | N/A |
| Required | Conditional – Only required during registration |

## MobileNumber

| **number** | |
| --- | --- |
| Description | Mobile number (excluding country code). |
| Data Type | String |
| Max Length | 10 |
| Required | Yes |

| **countryCode** | |
| --- | --- |
| Description | Mobile number country code. |
| Data Type | String |
| Max Length | 3 |
| Required | Yes |

## RNSData

| **rnsRegistrationId** | |
| --- | --- |
| Description | Remote Notification Service registration ID. |
| Data Type | String |
| Max Length | 4000 |
| Required | Conditional – Required only if wallet account registration is initiated from mobile app |

## SafetyNetData

| **jwsPayload** | |
| --- | --- |
| Description | JWS Payload received from Google SafetNet API. |
| Data Type | String |
| Max Length | 4000 |
| Required | Yes |

## DeviceInstanceData

| **imei** | |
| --- | --- |
| Description | Device Fingerprint |
| Data Type | String |
| Max Length | 20 |
| Required | Yes |

| **serialNumber** | |
| --- | --- |
| Description | Serial number |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

| **deviceName** | |
| --- | --- |
| Description | Device Name |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

## DeviceProfileData

| **manufacturerName** | |
| --- | --- |
| Description | Device Manufacturer Name (e.g. Samsung) |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

| **modelNumber** | |
| --- | --- |
| Description | Model Number of a Device (e.g. SM-G900) |
| Data Type | String |
| Max Length | 50 |
| Required | No |

| **screenWidth** | |
| --- | --- |
| Description | Device screen width |
| Data Type | Integer |
| Max Length | N/A |
| Required | No |

| **screenHeight** | |
| --- | --- |
| Description | Device screen height |
| Data Type | Integer |
| Max Length | N/A |
| Required | No |

## ApplicationData

| **name** | |
| --- | --- |
| Description | Name of the wallet application. |
| Data Type | String |
| Max Length | 100 |
| Required | Yes |

| **version** | |
| --- | --- |
| Description | Version of the wallet application. |
| Data Type | String |
| Max Length | 10 |
| Required | Yes |

| **checksum** | |
| --- | --- |
| Description | Application checksum used for temper detection |
| Data Type | String |
| Max Length | 128 |
| Required | No |

## DeviceEligibilityData

| **manufacturerName** | |
| --- | --- |
| Description | Device Manufacturer Name (e.g. Samsung) |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

| **modelNumber** | |
| --- | --- |
| Description | Model Number of a Device (e.g. SM-G900) |
| Data Type | String |
| Max Length | 50 |
| Required | No |

## PaymentCardData

| **paymentCardId** | |
| --- | --- |
| Description | Unique identifier of a Payment Card in Wallet Server |
| Data Type | String |
| Max Length | 36 |
| Required | Yes |

| **status** | |
| --- | --- |
| Description | Status of the Payment Card. Possible values: INACTIVE, ACTIVE |
| Data Type | String |
| Max Length | 20 |
| Required | Yes |

| **isPreferred** | |
| --- | --- |
| Description | Indicates if the PaymentCard is to be marked as Preferred card. At any given time, only one PaymentCard can be marked as Preferred. |
| Data Type | Boolean |
| Max Length | N/A |
| Required | Yes |

| **accountPANSuffix** | |
| --- | --- |
| Description | Payment Card Account Number Suffix (typically last 4 digits) |
| Data Type | String |
| Max Length | 4 |
| Required | Yes |

| **expiryMonth** | |
| --- | --- |
| Description | Expiry month of the payment card. Format: MM |
| Data Type | String |
| Max Length | 2 |
| Required | Yes |

| **expiryYear** | |
| --- | --- |
| Description | Expiry year of the payment card. Format: YYYY |
| Data Type | String |
| Max Length | 4 |
| Required | Yes |

| **cardBrandData** | |
| --- | --- |
| Description | Payment Card data |
| Data Type | [CardBrandData](#_PaymentCardBrandDetails) |
| Max Length | N/A |
| Required | No |

| **cardTokenData** | |
| --- | --- |
| Description | Payment Card token data |
| Data Type | Array[[CardTokenData](#_PaymentCardTokenDetails_1)] |
| Max Length | N/A |
| Required | No |

| **billingAddressData** | |
| --- | --- |
| Description | Contains data of the Billing Address. |
| Data Type | [AddressData](#_CheckEligibilityData) |
| Max Length | N/A |
| Required | No |

| **panUniqueReference** | |
| --- | --- |
| Description | Payment Card unique reference provided by TSP |
| Data Type | String |
| Max Length | 64 |
| Required | No |

## CardData

| **cardHolderName** | |
| --- | --- |
| Description | Holder name of the card |
| Data Type | String |
| Max Length | 100 |
| Required | Yes |

| **accountPAN** | |
| --- | --- |
| Description | PAN of payment card which needs to be added. |
| Data Type | String |
| Max Length | 19 |
| Required | Yes |

| **expiryMonth** | |
| --- | --- |
| Description | Expiry month of the payment card. Format: MM |
| Data Type | String |
| Max Length | 2 |
| Required | Yes |

| **expiryYear** | |
| --- | --- |
| Description | Expiry year of the payment card. Format: YYYY |
| Data Type | String |
| Max Length | 4 |
| Required | Yes |

| **securityCode** | |
| --- | --- |
| Description | CVC/CVV2 printed on the back of the card. |
| Data Type | String |
| Max Length | 4 |
| Required | No |

## AddressData

| **alias** | |
| --- | --- |
| Description | Address alias. |
| Data Type | String |
| Max Length | 50 |
| Required | No |

| **firstName** | |
| --- | --- |
| Description | First name of user.  This field is applicable only for shipping address.  If not provided, first name registered during account creation will be used. |
| Data Type | String |
| Max Length | 50 |
| Required | No |

| **lastName** | |
| --- | --- |
| Description | Last name of user.  This field is applicable only for shipping address.  If not provided, last name registered during account creation will be used. |
| Data Type | String |
| Max Length | 50 |
| Required | No |

| **line1** | |
| --- | --- |
| Description | Address line 1. |
| Data Type | String |
| Max Length | 256 |
| Required | Yes |

| **line2** | |
| --- | --- |
| Description | Address line 2. |
| Data Type | String |
| Max Length | 256 |
| Required | No |

| **line3** | |
| --- | --- |
| Description | Address line 3. |
| Data Type | String |
| Max Length | 256 |
| Required | No |

| **city** | |
| --- | --- |
| Description | City to which address belongs to. |
| Data Type | String |
| Max Length | 30 |
| Required | Yes |

| **province** | |
| --- | --- |
| Description | State to which address belongs to. |
| Data Type | String |
| Max Length | 30 |
| Required | Yes |

| **countryCode** | |
| --- | --- |
| Description | Country to which this address is belongs to. Expressed as a 3-letter (alpha-3) country code as defined in ISO 3166-1. |
| Data Type | String |
| Max Length | 3 |
| Required | Yes |

| **postalCode** | |
| --- | --- |
| Description | Postal code of the address. |
| Data Type | String |
| Max Length | 10 |
| Required | Yes |

| **mobileNumber** | |
| --- | --- |
| Description | Mobile number |
| Data Type | [MobileNumber](#_MobileNumber) |
| Max Length | N/A |
| Required | No |

| **recepientName** | |
| --- | --- |
| Description | Name of recipient |
| Data Type | String |
| Max Length | 100 |
| Required | Conditional – Required only for shipping address. |

## CardBrandData

| **name** | |
| --- | --- |
| Description | Name of the Payment Card Brand like American Express, Visa etc. |
| Data Type | String |
| Max Length | 20 |
| Required | No |

| **code** | |
| --- | --- |
| Description | Payment Card Brand category type. Possible values [master, visa, amex, discover, maestro, diners] |
| Data Type | String |
| Max Length | 10 |
| Required | Yes |

## CardTokenData

| **tokenUniqueReference** | |
| --- | --- |
| Description | Unique token reference returned by TSP |
| Data Type | String |
| Max Length | 64 |
| Required | Yes |

| **status** | |
| --- | --- |
| Description | Status of the token in TSP system. |
| Data Type | String |
| Max Length | 30 |
| Required | Yes |

| **tokenPANSuffix** | |
| --- | --- |
| Description | Payment Card Token Suffix. Typically last 4 digit of token PAN. |
| Data Type | String |
| Max Length | 4 |
| Required | Yes |

| **authenticationMethods** | |
| --- | --- |
| Description | When additional authentication is required, this is the list of supported authentication methods. |
| Data Type | Array[[AuthenticationMethod](#_AuthenticationMethod)] |
| Max Length | N/A |
| Required | Conditional – required if decision = REQUIRE\_ADDITIONAL\_AUTHENTICATION. |

## AuthenticationMethod

| **id** | |
| --- | --- |
| Description | Unique identifier assigned to this Authentication Method. |
| Data Type | String |
| Max Length | 32 |
| Required | Yes |

| **type** | |
| --- | --- |
| Description | Specifies the authentication method type. Fore possible values refer MDES specification. |
| Data Type | String |
| Max Length | 64 |
| Required | Yes |

| **value** | |
| --- | --- |
| Description | Specifies the authentication method value (meaning varies depending on the authentication method type). |
| Data Type | String |
| Max Length | 64 |
| Required | Yes |

## OSData

| **osName** | |
| --- | --- |
| Description | Name of an OS (e.g. Android, iOS). |
| Data Type | String |
| Max Length | 10 |
| Required | Yes |

| **osVersion** | |
| --- | --- |
| Description | Version of OS |
| Data Type | String |
| Max Length | 20 |
| Required | Yes |

| **osAlias** | |
| --- | --- |
| Description | Alias of an OS (e.g. L, M etc.) will be available only in case of Android. |
| Data Type | String |
| Max Length | 20 |
| Required | No |

## ShippingAddressData

| **id** | |
| --- | --- |
| Description | Unique identifier for shipping address in wallet server. |
| Data Type | String |
| Max Length | 36 |
| Required | Conditional: in case of address is being added then it will not be present. |

| **addressData** | |
| --- | --- |
| Description | Address Details |
| Data Type | [AddressData](#_CheckEligibilityData) |
| Max Length | N/A |
| Required | Yes |

| **status** | |
| --- | --- |
| Description | Status of address |
| Data Type | String |
| Max Length | 15 |
| Required | Yes |

| **isPreferred** | |
| --- | --- |
| Description | Indicator to denote whether this address is user’s preferred address or not. |
| Data Type | Boolean |
| Max Length | 5 |
| Required | Yes |

## LegalDocData

| **id** | |
| --- | --- |
| Description | Unique identifier of legal document. |
| Data Type | String |
| Max Length | 36 |
| Required | Yes |

| **version** | |
| --- | --- |
| Description | Version of legal document. |
| Data Type | String |
| Max Length | 10 |
| Required | Yes |

| **url** | |
| --- | --- |
| Description | URL location of legal document. |
| Data Type | String |
| Max Length | 100 |
| Required | Yes |

| **contentType** | |
| --- | --- |
| Description | Content type of legal document |
| Data Type | String |
| Max Length | 40 |
| Required | Yes |

| **legalDocType** | |
| --- | --- |
| Description | Type of legal document.  Possible values:   * TERMS\_CONDITIONS * PRIVACY\_POLICY * COOKIES\_POLICY * TERMS\_CONDITIONS\_COOKIES\_POLICY * TERMS\_CONDITIONS\_PRIVACY\_POLICY * PRIVACY\_POLICY\_ COOKIES\_POLICY * TERMS\_CONDITIONS\_PRIVACY\_POLICY\_COOKIES\_POLICY |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

## LegalDocAcceptanceData

| **legalDocType** | |
| --- | --- |
| Description | Type of legal document.  Possible values:   * TERMS\_CONDITIONS * PRIVACY\_POLICY * COOKIES\_POLICY * TERMS\_CONDITIONS\_COOKIES\_POLICY * TERMS\_CONDITIONS\_PRIVACY\_POLICY * PRIVACY\_POLICY\_ COOKIES\_POLICY * TERMS\_CONDITIONS\_PRIVACY\_POLICY\_COOKIES\_POLICY |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

| **legalDocVersion** | |
| --- | --- |
| Description | User has accepted legal document version details |
| Data Type | String |
| Max Length | 10 |
| Required | Yes |

## CheckoutSelectionData

| **paymentCardId** | |
| --- | --- |
| Description | Payment card identifier used for performing checkout |
| Data Type | String |
| Max Length | 36 |
| Required | Yes |

| **shippingAddressId** | |
| --- | --- |
| Description | Shipping address identifier used for performing checkout |
| Data Type | String |
| Max Length | 36 |
| Required | Conditional – Not required while performing checkout for digital goods or shipping address details is passed in request |

| **shippingAddress** | |
| --- | --- |
| Description | Shipping address for performing checkout |
| Data Type | [AddressData](#_CheckEligibilityData) |
| Max Length | N/A |
| Required | Conditional – Not required while performing checkout for digital goods or shipping address identifier is passed in request |

| **loyaltyCardId** | |
| --- | --- |
| Description | Loyalty card identifier used for performing checkout |
| Data Type | String |
| Max Length | 36 |
| Required | No |

| **digitalGoods** | |
| --- | --- |
| Description | Flag to indicate if consumer is performing checkout for digital goods |
| Data Type | Boolean |
| Max Length | N/A |
| Required | No |

| **dSRPData** | |
| --- | --- |
| Description | DSRP Details |
| Data Type | [DSRPData](#_DSRPData) |
| Max Length | N/A |
| Required | No |

## DSRPData

| **tokenAccountNumber** | |
| --- | --- |
| Description | Token account number. |
| Data Type | Numeric |
| Max Length | 24 |
| Required | Y |

| **cryptogram** | |
| --- | --- |
| Description | DSRP cryptogram generated by the MP-SDK |
| Data Type | Alphanumeric |
| Max Length | 512 |
| Required | Y |

| **unpredictableNumber** | |
| --- | --- |
| Description | Encoded EMV-quality random number generated by either the merchant or masterpass |
| Data Type | Alphanumeric |
| Max Length | 8 |
| Required | Y |

| **cryptogramType** | |
| --- | --- |
| Description | Indicates the type of cryptogram generated. Possible values [UCAF, ICC] |
| Data Type | Alphanumeric |
| Max Length | NA |
| Required | Y |

| **tokenExpiryMonth** | |
| --- | --- |
| Description | Token expiration month |
| Data Type | String |
| Max Length | 2 |
| Required | Y |

| **tokenExpiryYear** | |
| --- | --- |
| Description | Token expiration year. |
| Data Type | String |
| Max Length | 4 |
| Required | Y |

## SessionKeySigningRequest

| **appId** | |
| --- | --- |
| Description | App identifier, could be merchant app or wallet app |
| Data Type | String |
| Max Length | 50 |
| Required | Yes |

| **appVersion** | |
| --- | --- |
| Description | Merchant application version |
| Data Type | String |
| Max Length | 20 |
| Required | Yes |

| **appSigningPublicKey** | |
| --- | --- |
| Description | Public Key of the in-memory session key pair generated by calling app. |
| Data Type | String |
| Max Length | N/A |
| Required | Yes |

## SessionKeySigningResponse

| **sessionSignature** | |
| --- | --- |
| Description | Session signature provided by Masterpass switch for verification. |
| Data Type | String |
| Max Length | 256 |
| Required | Yes |

## CountryData

| **iso3166Alpha3** | |
| --- | --- |
| Description | Country Code. Expressed as a 3-letter (alpha-3) country code as defined in ISO 3166-1. |
| Data Type | String |
| Max Length | 3 |
| Required | Yes |

| **iso3166Alpha2** | |
| --- | --- |
| Description | Country Code. Expressed as a 2-letter (alpha-2) country code as defined in ISO 3166-1. |
| Data Type | String |
| Max Length | 2 |
| Required | Yes |

| **iso3166Numeric** | |
| --- | --- |
| Description | Country Code. Expressed as a 3-letter (numeric) country code as defined in ISO 3166-1. |
| Data Type | String |
| Max Length | 3 |
| Required | Yes |

| **name** | |
| --- | --- |
| Description | Country name. |
| Data Type | String |
| Max Length | 30 |
| Required | No |

| **provinces** | |
| --- | --- |
| Description | Country’s subdivisions. |
| Data Type | Array[[ProvinceData](#_SubdivisionData)] |
| Max Length | N/A |
| Required | No |

## ProvinceData

| **code** | |
| --- | --- |
| Description | Subdivision/Province/State Code. Expressed as a 5-letter (alpha-3) subdivision code as defined in ISO 3166-2. |
| Data Type | String |
| Max Length | 10 |
| Required | Yes |

| **name** | |
| --- | --- |
| Description | Province/State name. |
| Data Type | String |
| Max Length | 30 |
| Required | No |

## AccountVerificationData

| **paymentCardData** | |
| --- | --- |
| Description | Payment Card Data for account verification. Only account number suffix (typically last 4 digits), expiry month and expiry year is needed. |
| Data Type | [PaymentCardData](#_PaymentCardInfo) |
| Max Length | 4 |
| Required | Yes |

## ErrorData

| **responseCode** | |
| --- | --- |
| Description | Unique code to identify a specific exception scenario in API invocation. Examples below -   * WALLET\_ACCOUNT\_LOCKED * CARD\_VERIFICATION\_ERROR   TENANT\_RESOLUTION\_FAILED |
| Data Type | String |
| Max Length | 30 |
| Required | Yes |

| **responseDescription** | |
| --- | --- |
| Description | Brief localized description of the exception scenario in API invocation |
| Data Type | String |
| Max Length | 100 |
| Required | No |

| **inputField** | |
| --- | --- |
| Description | UI input field name |
| Data Type | String |
| Max Length | 20 |
| Required | No |

## FieldValidationConfig

| **name** | |
| --- | --- |
| Description | Field name. Possible values: CUSTOM Category - MIDDLE NAME, NATIONAL ID, BIRTHDATE, GENDER and ADDRESS category LINE1, LINE2, LINE3, CITY, SUBDIVISION and POSTAL CODE. |
| Data Type | String |
| Max Length | 20 |
| Required | Yes |

| **enabled** | |
| --- | --- |
| Description | Indicated whether the field is enabled or diabled. |
| Data Type | Boolean |
| Max Length | N/A |
| Required | Yes |

| **displayOrder** | |
| --- | --- |
| Description | Indicate the order in which fields should be displayed. |
| Data Type | String |
| Max Length | 255 |
| Required | No |

| **minLength** | |
| --- | --- |
| Description | Minimum length. |
| Data Type | Integer |
| Max Length | N/A |
| Required | No |

| **maxLength** | |
| --- | --- |
| Description | Maximum length. |
| Data Type | Integer |
| Max Length | N/A |
| Required | No |

| **required** | |
| --- | --- |
| Description | Indicate whether field is mandatory. |
| Data Type | Boolean |
| Max Length | N/A |
| Required | Yes |

| **expression** | |
| --- | --- |
| Description | Regular expression for validation. |
| Data Type | String |
| Max Length | 255 |
| Required | No |

| **visible** | |
| --- | --- |
| Description | Indicate whether field should be visible or not. |
| Data Type | Boolean |
| Max Length | N/A |
| Required | Yes |

# MDES Objects

For MDES Integration object structure, please refer MDES API Specification version 1.1.1. Mobile App is expected to pass parameters which are described in specific below sections. Other MDES integration parameters will be fetched/calculated by Wallet Server.

## RegisterMobileAppRequest

Please refer MPA Management > Register API in MDES specification for request structure & details. Mobile App is expected to pass only following list of parameters.

* publicKeyFingerprint
* rgk
* newMobilePin

## RegisterMobileAppResponse

Please refer MPA Management > Register API in MDES specification for request structure & details. Wallet server will pass following list of parameters to mobile app.

* mobileKeysetId
* mobileKeys
* remoteManagementUrl

## CheckEligibilityRequest

Please refer Digitization > Check Eligibility API in MDES specification for request structure & details. Mobile App is expected to pass only following list of parameters.

* tokenType
* source
* nfcCapable
* storageTechnology
* formFactor
* consumerLanguage

## CheckEligibilityResponse

Please refer Digitization > Check Eligibility API in MDES specification for request structure & details. Wallet server will pass following list of parameters to mobile app.

* deviceNotEligibleReasons
* termsAndConditionsAssetId

## DigitizationRequest

Please refer Digitization > Digitize API in MDES specification for request structure & details. Mobile App is expected to pass only following list of parameters.

* tokenizationAuthenticationValue
* decisioningData

## ActivateTokenRequest

Please refer Digitization > Activate API in MDES specification for request structure & details. Mobile App is expected to pass only following list of parameters.

* tokenUniqueReference
* authenticationCode
* tokenizationAuthenticationValue

# Appendix

1. **Sample JOSE Envelope for Request**

**B.1 ECDH**

|  |
| --- |
| {  "protectedHeader": "",  "recipients": [  {  "headers": {},  "encryptedKey": "K\_Q8QtZAG\_5fEpTvXoJ5HB6b8IxwQUaQlrh6tuf\_ygJCyKTDcGwmOeIpzIwOr6UDUgpuxxkfI50AgF66bqWUH8QfZvox4\_HXSvOd4CbvaYU="  }  ],  "iv": "0ZHDlromgr7xmSt7F4\_oVw==",  "m": "3BLgtRVCgH78pnue\_8vS0JK9Z8y01mOUuTSyLXbzznSKZq58YB4IzVypjz9r0RRTR775MWmjnL9WYEeHaUH9CADSXM6h9T0SNVZKKwCZEnls0-lK-VHb4ER23IXXZi8KSkrb49WOR\_WJxXHO0YZrrKoTUWsmstgQYGv0vUtp5t1LIng7SDc1FWCAfmiG09xa0D7jYWSpDf3r07GPC\_\_y4Zabhh-LV3ngM-NnbUBOszD0VKmqnoG7KvH3zDOw9Mug8mIZSFctaD7b8QJz0UUh\_NsybQQh0ylMM4SIBSI\_LJWZd5e8k2GUdhw6Kt8N5yCiAlIQeJafogDDsT7JXxF\_l-7uIAhb-ksv-6R8Xczw5n\_NlCB3m5Ot1m-GtLH3a2ojzCbApci5rgdJr6KSqhp6hd1G3JIK1k5qTHr\_zkB5MdLFqVdwD9wplREzMBuPFnIAxobALV63lYxCm2iN\_uzyrE-JaONGxUcH1ujh1Z7bvRsMJP1U96yuOnfd0FbVyJaZUw3xudYoUHVzleRb3F-jPAhbo33XFUL05aQxdSo\_p2Zu2DMHAl-5hYRtaTnTdYSC8agigGMA8d2pV2IDGorsnnVZV\_qxUTAYnqUf53gA\_B7bPcCGiY7N3n9Xk2eNYpY34lAWIRkdWpCduL44x4X-6MxLQHTBZ3N-cauw-AsGHl2Byz8ofX66kbpeNswbvCOULhRC7rPGFYARPmLxbw7y3g==",  "tag": "XoN9mLiwLv5jPk-v9qbNbdLNA9s7Km4mT3d2fx8aT7qg5aEoYMNwxECO9YpKB8ZgoOHOoTYGcHfypYoe-aETkA=="  } |

**B.2 PBES2**

|  |
| --- |
| {  "tag": "5m0j6EVzg\_oMcSIkp4XE4JP3rIvMrvD6NGhAh64wJMC8xyHrNjXTEA4aLxxoley5Fpwktb\_NWmHj938l5bkaeQ==",  "iv": "TsX4r4NfuAagE83TjUKcQw==",  "m": "5wdIS4AhQdoSv-FNqCjXrqR7dA0O0SnDGiQg4OmENXz\_oU5UWlAcYjPUuRXuD2gqnwzAK\_owqjyDE\_hMHIuozvKZsXVH651Bh9BqRqbrGa-6b328i49uSWua6G3bxoJsP9b3dP\_-2GLrTEc8Fj4nWotVsrBj5Y1ohrtiRU8tiwZtzBerOmd3KGwxDSdCZ9WaLaXoh20G8\_Oka6XJR1m\_WKTTCbJbjwMQcbkjrYZ2nVKlKGfZmDkyR3riqjdzRXGN4dRiodvMjI9A4TcV1aN9q6ARWrMlDNG0DGNq3yOysdk0xu3SytrHEwyGr5851MGXh7AtNVN6AaDqGShmEoz8ppLNpHsG\_lUiyHRYSlHSYgAUfOMQYmMOSw7S8uEb3\_VtXLNWZmaYVbgusp0Vf8MIHAjsfRS3pzaoAuNTKbXAkzU=",  "protectedHeader": "",  "recipients": [  {  "encryptedKey": "-AsiEy2-equvgtWCxObpr3wxDYn6qOmQe5Ey-u7Qy9VlrwB\_rKME1f5doLM6pIef2RrhgaQPNfV4ELelSqp6ZWNHPBQK5gFJQoTV8RSMGbY=",  "headers": {}  }  ]  } |

1. **Sample JOSE Envelope for Response**

**ECDH**

|  |
| --- |
| {  "protectedHeader": "",  "recipients": [  {  "headers": {},  "encryptedKey": "A01RF3nzyeKeqK3vp48FUKEp\_K-qCducJ5MLPsO2tMr-xtJjGK6n6TE5mTARp9S0ZlPaXl1VcIE22OtA9bNgegwbMersFvs1zDCJ0zJt6LM="  }  ],  "iv": "bHMn7wbebnL2T5UAOuCGug==",  "aad": "MTIzNDU2",  "m": "6luaajNlQDqZWzoYmYHIKf8hWS58xRdxK7mviRBBFlhzCJ4m0hrtL2F7L1jcF4gRNgmUU\_BfdBhS\_045tH6vhcmEfaJbDcMHTZ4fft0zCRBcAIrQlhL-l3GyeObIopHTWtMj68hbireHWkeUp6NVEAzJO1koTAXG06TjQniaGgWdc-UrFGtourajYluDHaU39\_xrHTUZTb1UtFRJMsmpd-a\_nvorawltHoTJIlf6nYWI4I1nrPK7As1BgxAmXPZE7CrABMl0LObtWU7jazVbIQQrdFnfPZuR6Kd7HW6hxhk=",  "tag": "AhlEBiIhbTE1JYQf5RdLnfqvgkXAmt8jdUlhrHvXCAzlPu6ML2T47TZfoF4Jgwf9v2zgkHqWMupHmdENilRz0w=="  } |

**PBES2**

|  |
| --- |
| {  "protectedHeader": "eyJyZXNwb25zZU1lc3NhZ2UiOiJudWxsIiwiYWxnIjoiUEJFUzItSFM1MTIrQTI1NktXIiwicDJzIjoic2ZSRFpyX291QTQ5eHc1a1hCdHNXZyIsInJlc3BvbnNlQ29kZSI6IjAiLCJ3YWxsZXRJZCI6ImI5OWZkNzE0LWY3ZDItNGY4Yy04MzBkLTEzZjUxY2I5NDhkMSIsInAyYyI6IjEwMDAwIiwicmVxdWVzdElkIjoiODIzMTFmNzEtOWMxMC00NDQ4LTgxMzctYmRmYjIzNTAyOTFhIiwiZW5jIjoiQTI1NkNCQy1IUzUxMiJ9",  "recipients": [  {  "headers": {},  "encryptedKey": "BJq\_M3a7xJwY7wIBRRRlKGJvZU9dLFdpMOLMljfsaMOJQkLD7BcG0H6S644v70TZke8mWubyx77DwG5sU1OsS5THxcjuSzFKkgePUz1JQ8M="  }  ],  "iv": "bKcEYQ5InQRkcA3YlgUvVg==",  "aad": "MTIzNDU2",  "m": "h57l3aLsSNsUfZ9vViDDhmCEpWIgj5DvcDbMBLFLbIVH5QFLIUO0O5QzGyykslhGsk30T-X\_PQ5gZLiXnc6urJRdEVbRK52doned0TkgED5ZM13P6iKePv1BHscO-zTokKhDng6euM9vcVx48vvSy40217cPYtubuU619qd76RNSIh6xUa9d2RHf5NNvXkf-lTQm2X5BdjjEgYA\_-vz0PQBqEEhy3N0aZRZaKPRXgNXiIlqMOtfh6Lk2tB\_5l\_nnnV6WLnqKXJNEiS4ng5Q3teJoNQ8x0LrDGqQ4FJYcfBSyNTniyZOBb8KlEnZfBor-p-bAqOpFPQSbMFoYAXBCdVMxzIDb7QeW4BWjf2DPhEyShNTpYO2RIcXznrD0o3f-DgvImpedxnScT0o5dMHl8s\_GPEvs2yuUu5956kUPXn9Ak8aYWwwG2FEf-M5jSPNCx4lGwOG\_IXBZ1f7wk5E8z19jqtoCAn6Ss6WrgDdBP5gqJJro\_PJRx66zkUBBxcyu8T334IeXHLMKfhQU1qek6XbgE498ykvUqFcFW0qLyjUteEnfHDrBnGzRIQ-dMFckwjM5dIkD1hWS4e5jkr8B7ek2FSyN8Km\_V20RjOwcUUKKnsZjRqlmVF9Fre5DlThWfF6JYlPiXsUev5LMRgFdSelcDbOAvPk3KeCsZhNNk6w7xl\_sIDJEOwJJgW7hA3kYD\_TxAilgTmsHdtUGw5zGik0SsxQdjmMuOYQihSXYtC2pacpLGM9I2vsVQi\_bb3iaZku-E7RFvHnWkm6qIdAFDxCwEq56es2vRQam0EHYlLZYb\_y8PxKfiFFn6rdbmNgusS5xbwiBdHfxFPD3CtHCe0NS1VAo7zhxuJB8QmIT0QQeifFG9yipui40RdMPcK5BgkvP6ddFg1n2hSpVdIBRDE\_ih1u4X1GdrlO9jOApEvn20-j9XDaEQUrFyp5RZkI4a4zBXs-WrFKCWIcimhz--WxrTMs3AwDEaGbvbCBcRFvTLQJSKHmhAI9KZ9S0yXhf",  "tag": "LDwCNu9NJ3Br5zidJD2GKpTn9VArEr0UftxvdHL5Wyx7iUJmQ\_HHIZuI-OZ3EmgRLpOW5kFXNodL8g7BMN3Ahg=="  } |

1. **Sample Terms and Conditions**

|  |
| --- |
| <!DOCTYPE html>  <!--  To change this license header, choose License Headers in Project Properties.  To change this template file, choose Tools | Templates  and open the template in the editor.  -->  <html>  <head>  <title>Términos y Condiciones</title>  <meta charset="UTF-8">  <meta name="viewport" content="width=device-width, initial-scale=1.0">  <script type="text/javascript" src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>  <script type="text/javascript" src="tnc\_html\_resource/js/accordion.js"></script>  <link rel="stylesheet" href="tnc\_html\_resource/css/stylesheet.css" type="text/css" charset="utf-8" />  </head>  <body>  <div class="main tnc">  <div class="accordion tnc-accordion">  <div class="section">  <div class="title">Términos y Condiciones</div>  <div class="summary">Maecenas sed diam eget risus varius blandit sit amet non magna. Maecenas faucibus mollis interdum. Donec ullamcorper nulla non metus auctor fringilla. Nullam id dolor id nibh ultricies vehicula ut id elit. Nullam id dolor id nibh ultricies vehicula ut id elit. </div>  <div class="accordion-section">  <div id="accordion-1">  <p class="accordion-tncContent">Mauris interdum fringilla augue vitae tincidunt. Curabitur vitae tortor id eros euismod ultrices. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Praesent nulla mi, rutrum ut feugiat at, vestibulum ut neque? Cras tincidunt enim vel aliquet facilisis. Duis congue ullamcorper vehicula. Proin nunc lacus, semper sit amet elit sit amet, aliquet pulvinar erat. Nunc pretium quis sapien eu rhoncus. Suspendisse ornare gravida mi, et placerat tellus tempor vitae.</p>  <div class="tncExndLinkWrap">  <a class="accordion-tncExndLink" href="#accordion-1">See full terms & conditions</a>  <img class="tnc-img" width="16" src="tnc\_html\_resource/img/ic\_tnc\_arrow\_expand.png" alt="Expand">  </div>  <div class="tncClpsLinkWrap">  <a class="accordion-tncClpsLink" href="#accordion-1">Collapse terms & conditions</a>  <img class="tnc-img" width="16" src="tnc\_html\_resource/img/ic\_tnc\_arrow\_collapse.png" alt="Collapse">  </div>  </div><!--end .accordion-section-content-->    </div><!--end .accordion-section-->  </div>  <div class="section">  <div class="title">política privada</div>  <div class="summary">Aenean eu leo quam. Pellentesque ornare sem lacinia quam venenatis vestibulum. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. </div>  <div class="accordion-section">  <div id="accordion-2">  <p class="accordion-tncContent">Curabitur vitae tortor id eros euismod ultrices. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Praesent nulla mi, rutrum ut feugiat at, vestibulum ut neque? Cras tincidunt enim vel aliquet facilisis. Duis congue ullamcorper vehicula. Proin nunc lacus, semper sit amet elit sit amet, aliquet pulvinar erat. Nunc pretium quis sapien eu rhoncus. Suspendisse ornare gravida mi, et placerat tellus tempor vitae.</p>  <div class="tncExndLinkWrap">  <a class="accordion-tncExndLink" href="#accordion-2">See full private policy</a>  <img class="tnc-img" width="16" src="tnc\_html\_resource/img/ic\_tnc\_arrow\_expand.png" alt="Expand">  </div>  <div class="tncClpsLinkWrap">  <a class="accordion-tncClpsLink" href="#accordion-2">Collapse private policy</a>  <img class="tnc-img" width="16" src="tnc\_html\_resource/img/ic\_tnc\_arrow\_collapse.png" alt="Collapse">  </div>    </div><!--end .accordion-section-content-->    </div><!--end .accordion-section-->  </div>  </div><!--end .accordion-->  </div>  </body>  </html> |

# References

* <https://www.owasp.org/index.php/REST_Security_Cheat_Sheet>