**Mightypay API Interfacing Guide**

**Version 0.1.e**

**All rights reserved. This document is proprietary and confidential. This document may contain trade secrets and information proprietary to MVI Technologies (S) Pte Ltd. No part of this document may be disclosed in any manner to a third party without the prior written consent of MVI Technologies (S) Pte Ltd. This document is protected under copyright laws as unpublished work of MVI Technologies (S) Pte Ltd.**

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Author** | **Date** | **Description** | **Version** |
| Vijayakumar | 05-Dec-2019 | Initial version | 0.1.b |
| Preethi | 10-Dec-2019 | Addition of P2P Transfer API Specification | 0.1.c |
| Preethi | 11-Dec-2019 | Addition of Redeem API Specification | 0.1.d |
| Divek V | 11-Dec-2019 | Addition of Query Wallet Balance API Specification | 0.1.e |

Contents

[1. About Mightypay System 4](#_Toc26972920)

[2. Topup 4](#_Toc26972921)

[3. Onboard User Entity 5](#_Toc26972922)

[4. P2P Transfer 7](#_Toc26972923)

[5. Redeem 9](#_Toc26972924)

[6. Query Wallet Balance 11](#_Toc26972925)

[7. Update User Entity 13](#_Toc26972926)

[8. Request/Response Samples 15](#_Toc26972927)

[8.1 Topup 15](#_Toc26972928)

[8.2 Onboard 15](#_Toc26972929)

[8.3 Sample Data 16](#_Toc26972930)

[8.4 Response Codes 17](#_Toc26972931)

[9. Security Implementation 17](#_Toc26972932)

[9.1 Acquiring App ID & App secret 17](#_Toc26972933)

[9.2 Securing Messages using JOSE (JWT, JWE, JWS). 17](#_Toc26972937)

# About Mightypay System

In this system there are Players, Sponsors, Game owners, etc., First Phase will have 2 REST APIs (Topup and Onboard) only for Players.

Integration Sandbox URL:

|  |  |
| --- | --- |
| Onboard | http://129.126.122.58:18181/0.1/fe-api-gw/onboard |
| Topup | http://129.126.122.58:18181/0.1/fe-api-gw/topup |

Note: HTTPS will be enabled in the next release.

# Topup

**Resource URL:**

https://<baseURL>/0.1/fe-api-gw/topup

|  |  |
| --- | --- |
| **Resource** | **Description** |
| POST  fe-api-gw/topup | Topup digital asset into an Mightypay account. The quantity will be credited into the eWallet immediately upon successful transaction. |

**Request Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| platformCode | Alphanumeric | M | 5 | This indicates the platform code assigned to the requestor which is also the source of this transaction |
| userEntityId | Alphanumeric | M | 40 | User Entity ID |
| walletId | Alphanumeric | M | 20 | eWallet ID |
| digitalAssetTypeCode | Alphanumeric | M | 5 | Digital Asset Type Code |
| quantity | Numeric as string | M | 18 | Quantity |
| terminalId | Alphanumeric | M | 50 | Terminal ID at the terminal where transaction is done |
| platformRef | Alphanumeric | M | 50 | This is for platform to cross reference with their transaction |
| timestamp | Alphanumeric | M | 14 | This is the time stamp of the transaction at the source in the format “yyyyMMddHHmmss” |
| timeZone | Alphanumeric with special chars | O | 10 | RFU |
| remarks | Alphanumeric | O | 100 | Transaction description |

**Response Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| responseCode | Alphanumeric | M | 3 | 000 – success, any other response code is considered as an error. Refer to message field for detail. |
| message | Alphanumeric | O | 200 | Additional information on the status |
| rrn | Alphanumeric | M | 20 | Retrieval Reference Number |
| authidresp | Alphanumeric | O | 10 | Authorization ID Response, available only for successful transactions |
| txnUid | Alphanumeric | M | 20 | Transaction Unique ID / Transaction reference |
| userEntityId | Alphanumeric | O | 40 | User Entity ID |
| walletId | Alphanumeric | O | 20 | eWallet ID |
| digitalAssetTypeCode | Alphanumeric | O | 5 | Digital Asset Type Code |
| platformRef | Alphanumeric | M | 50 | This is for platform to cross reference with their transaction |
| availableQuantity | Numeric as string | O | 18 | Quantity (available only if responseCode=000) |
| trxnTime | Alphanumeric | M | 17 | This is the time stamp of the transaction in the format “yyyyMMddHHmmssS” |
| trxnTimeZone | Alphanumeric with special chars | O | 10 | RFU |

# Onboard User Entity

**Resource URL:**

https://<baseURL>/0.1/ fe-api-gw/onboard

|  |  |
| --- | --- |
| **Resource** | **Description** |
| POST  fe-api-gw/onboard | Onboard a new user entity (Player, sponsors etc.,) |

**Request Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O/C** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| platformCode | Alphanumeric | M | 5 | This indicates the platform code assigned to the requestor which is also the source of this transaction |
| terminalId | Alphanumeric | M | 50 | Terminal ID at the terminal where transaction is done |
| name | Alphanumeric | M | 100 | User Entity Name (Player/Sponsor Name) |
| mobileNo | Numeric as String | M | 20 | Mobile number (numbers only) |
| userEntityIdentityType | Alpha with underscore | O | 20 | Identify Type  (  PASSPORT,  TAX\_ID,  NATIONAL\_ID  ) |
| userEntityIdentity | Alphanumeric | C | 20 | Identify Number  This field is mandatory if the “userEntityIdentityType” field has value. |
| userEntityType | Alpha with underscore | M | 20 | User Entity Type.  (PLAYER,  SPONSOR,  STREAMER,  INFLUENCER,  GAME\_OWNER) |
| address1 | Alphanumeric | O | 80 | Address Line 1 |
| address2 | Alphanumeric | O | 80 | Address Line 2 |
| address3 | Alphanumeric | O | 80 | Address Line 3 |
| postalCode | Alphanumeric | O | 20 | Postal code |
| city | Alphanumeric | O | 40 | City |
| countryCode | Alphanumeric | O | 3 | Country code |
| timestamp | Numeric as String | M | 14 | This is the time stamp of the transaction at the source in the format yyyyMMddHHmmss” |
| timeZone | Alphanumeric with special chars | O | 10 | RFU |
| state | Alphanumeric | O | 40 | State |
| emailId | Alphanumeric with special chars | M | 75 | Email ID |
| kycFlag | Alpha | O | 1 | KYC Flag (‘Y’ or ’N’)  Y – KYC completed N – KYC pending |

**Response Private Claim Fields:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| responseCode | Alphanumeric | M | 3 | 000 – success, any other response code is considered as error. Refer to message field for detail. |
| message | Alphanumeric | O | 200 | Additional information on the status |
| rrn | Alphanumeric | M | 20 | Retrieval Reference Number |
| authidresp | Alphanumeric | O | 10 | Authorization ID Response, available only for successful transactions |
| txnUid | Alphanumeric | M | 20 | Transaction Unique ID / Transaction reference |
| userEntityId | Alphanumeric | O | 40 | User Entity Account ID |
| walletId | Alphanumeric | O | 20 | eWallet ID |
| trxnTime | Alphanumeric | M | 17 | This is the time stamp of the transaction in the format “yyyyMMddHHmmssS” |
| trxnTimeZone | Alphanumeric with special chars | O | 10 | RFU |

# P2P Transfer

**Resource URL:**

https://<baseURL>/1.0/fe-api-gw/p2p-payment

|  |  |
| --- | --- |
| **Resource** | **Description** |
| POST  fe-api-gw/p2p-payment | Transfers Digital Assets from one Wallet to another. |

**Request Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| platformCode | Alphanumeric | M | 5 | This indicates the platform code assigned to the requestor which is also the source of this transaction |
| fromUserEntityId | Numeric | C | 40 | User ID of the wallet holder from where the digital assets will be transferred.  Mandatory if fromWalletId is not available |
| fromWalletId | Alphanumeric | C | 20 | Wallet ID from where the digital assets will be transferred  Mandatory if fromUserEntityId is not available |
| toUserEntityId | Numeric | C | 40 | User ID of the wallet holder to which the digital assets will be transferred  Mandatory if toWalletId is not available |
| toWalletId | Alphanumeric | C | 20 | Wallet ID to which the digital assets will be transferred  Mandatory if toUserEntityId is not available |
| digitalAssetTypeCode | Alphanumeric | M | 5 | Digital Asset Type Code |
| quantity | Numeric as string | M | 18 | Quantity of the digital assets to be transferred |
| registerToUserEntity | Boolean | O | NA | Flag to check if the destination wallet user entity is a registered one.  Default value: FALSE |
| terminalId | Alphanumeric | O | 50 | Terminal ID at the terminal where transaction is done |
| platformRef | Alphanumeric | M | 50 | This is for platform to cross reference with their transaction |
| remarks | Alphanumeric | O | 100 | Transaction description |
| timestamp | Alphanumeric | M | 14 | This is the time stamp of the transaction at the source in the format “yyyyMMddHHmmss” |
| timeZone | Alphanumeric with special chars | O | 10 | RFU |

**Response Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| responseCode | Alphanumeric | M | 3 | 000 – success, any other response code is considered as an error. Refer to message field for detail. |
| message | Alphanumeric | O | 200 | Additional information on the status |
| rrn | Alphanumeric | M | 20 | Retrieval Reference Number |
| authidresp | Alphanumeric | O | 10 | Authorization ID Response, available only for successful transactions |
| txnUid | Alphanumeric | M | 20 | Transaction Log Unique ID / Transaction reference |
| fromUserEntityId | Numeric | M | 40 | User ID of the source wallet holder |
| fromWalletId | Alphanumeric | M | 20 | Wallet ID of the source wallet |
| digitalAssetTypeCode | Alphanumeric | M | 5 | Digital Asset Type Code | |
| availableQuantity | Numeric as string | O | 18 | Available Quantity of Digital assets in the source Wallet after transfer | |
| platformRef | Alphanumeric | M | 50 | This is for platform to cross reference with their transaction | |
| trxnTime | Alphanumeric | M | 17 | This is the time stamp of the transaction in the format “yyyyMMddHHmmssS” | |
| trxnTimeZone | Alphanumeric with special chars | O | 10 | RFU | |

# Redeem

**Resource URL:**

<https://<baseURL>/1.0/fe-api-gw/redeem>

|  |  |
| --- | --- |
| **Resource** | **Description** |
| POST  fe-api-gw/redeem | Redeem |

**Request Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| platformCode | Alphanumeric | M | 5 | This indicates the platform code assigned to the requestor which is also the source of this transaction |
| userEntityId | Alphanumeric | C | 40 | User Entity ID |
| walletId | Alphanumeric | C | 20 | eWallet ID |
| digitalAssetTypeCode | Alphanumeric | M | 5 | Digital Asset Type Code |
| quantity | Numeric as string | M | 18 | Quantity |
| merchantId | Alphanumeric | M | 15 | This indicate the merchant ID assigned to the requestor that is the source of this transaction |
| merchantRef | Alphanumeric | M | 50 | This is for merchant to cross reference with their transaction |
| terminalId | Alphanumeric | M | 50 | Terminal ID at the terminal where transaction is done |
| platformRef | Alphanumeric | M | 50 | This is for platform to cross reference with their transaction |
| remarks | Alphanumeric | O | 100 | Transaction description |
| timestamp | Alphanumeric | M | 14 | This is the time stamp of the transaction at the source in the format “yyyyMMddHHmmss” |
| timeZone | Alphanumeric with special chars | O | 10 | RFU |

**Response Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| responseCode | Alphanumeric | M | 2 | 00 – success, any other response code is error. Refer to message field for detail. |
| message | Alphanumeric | O | 200 | Additional information on the status |
| rrn | Alphanumeric | M | 20 | Retrieval Reference Number |
| authidresp | Alphanumeric | O | 10 | Available only for successful transactions |
| txnUid | Alphanumeric | M | 20 | Transaction Unique ID / Transaction reference |
| userEntityId | Alphanumeric | C | 40 | User Entity ID |
| walletId | Alphanumeric | C | 20 | eWallet ID |
| digitalAssetTypeCode | Alphanumeric | M | 5 | Digital Asset Type Code |
| availableQuantity | Numeric as string | M | 18 | Available quantity of digital assets in wallet after redemption |
| merchantId | Alphanumeric | M | 15 | This indicate the merchant ID assigned to the requestor that is the source of this transaction |
| merchantRef | Alphanumeric | M | 50 | This is for merchant to cross reference with their transaction |
| platformRef | Alphanumeric | M | 50 | This is for platform to cross reference with their transaction | |
| trxnTime | Alphanumeric | M | 17 | This is the time stamp of the transaction in the format “yyyyMMddHHmmssS” | |
| trxnTimeZone | Alphanumeric with special chars | O | 10 | RFU | |

# Query Wallet Balance

**Resource URL:**

<https://<baseURL>/1.0/fe-api-gw/queryWalletBalance>

|  |  |
| --- | --- |
| **Resource** | **Description** |
| POST  fe-api-gw/queryWalletBalance | Returns the digital asset details for the requested User Entity ID or eWallet ID. |

**Request Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| platformCode | Alphanumeric | M | 5 | This indicates the platform code assigned to the requestor which is also the source of this transaction. |
| userEntityId | Alphanumeric | O | 40 | User Entity ID. This is Mandatory, when if walletId is not provided. |
| walletId | Alphanumeric | O | 20 | eWallet ID. This is Mandatory, when if userEntityId is not provided. |
| digitalAssetTypeCode | Alphanumeric | O | 5 | Digital Asset Type Code. If it is empty, returns all the digital asset details for the equivalent eWallet ID or User Entity ID given. Else returns only the digital asset details for the given digital asset type code. |
| terminalId | Alphanumeric | M | 50 | Terminal ID at the terminal where transaction is done |
| platformRef | Alphanumeric | M | 50 | This is for platform to cross reference with their transaction. |
| timestamp | Alphanumeric | M | 14 | This is the time stamp of the transaction at the source in the format “yyyyMMddHHmmss”. |
| timeZone | Alphanumeric with special chars | O | 10 | RFU |
| remarks | Alphanumeric | O | 100 | Transaction description |

**Response Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| responseCode | Alphanumeric | M | 3 | 000 – success, any other response code is considered as an error. Refer to message field for detail. |
| message | Alphanumeric | O | 200 | Additional information on the status |
| rrn | Alphanumeric | M | 20 | Retrieval Reference Number |
| authidresp | Alphanumeric | O | 10 | Authorization ID Response, available only for successful transactions |
| txnUid | Alphanumeric | M | 20 | Transaction Unique ID / Transaction reference |
| userEntityId | Alphanumeric | O | 40 | User Entity ID. |
| walletId | Alphanumeric | O | 20 | eWallet ID. |
| digitalAssetList | JSON Array | O | 5 | Empty if no digital asset found |
| platformRef | Alphanumeric | M | 50 | This is for platform to cross reference with their transaction |
| trxnTime | Alphanumeric | M | 17 | This is the time stamp of the transaction in the format “yyyyMMddHHmmssS” |
| trxnTimeZone | Alphanumeric with special chars | O | 10 | RFU |

**Digital Asset List Fields:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| digitalAssetTypeCode | Numeric as string | M | 40 | Digital Asset Type Code |
| digitalAssetName | Alphanumeric | M | 45 | Digital Asset Name |
| availableQuantity | Numeric as string | M | 18 | Available Quantity of the digital asset. |
| status | Alphanumeric | M | 20 | digital asset status |

# Update User Entity

**Resource URL:**

http://<baseURL>/0.1/ fe-api-gw/update-user

|  |  |
| --- | --- |
| **Resource** | **Description** |
| POST  fe-api-gw/update-user | Update user entity details (mobileNo, email, etc.,) |

**Request Private Claim Fields:**

| **Parameter** | **Data Type** | **M/O/C** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| platformCode | Alphanumeric | M | 5 | This indicates the platform code assigned to the requestor which is also the source of this transaction |
| terminalId | Alphanumeric | M | 50 | Terminal ID at the terminal where transaction is done |
| userEntityId | Alphanumeric | M | 40 | User Entity Account ID |
| userEntityDetails | JSON Object | M | - | User Entity Details |
| timestamp | Alphanumeric | M | 14 | This is the time stamp of the transaction at the source in the format yyyyMMddHHmmss” |
| timeZone | Alphanumeric with special chars | O | 10 | RFU |

**User Entity Details Fields:**

| **Parameter** | **Data Type** | **M/O/C** | **Size** | **Value** |
| --- | --- | --- | --- | --- |
| mobileNo | Alphanumeric | O | 20 | Mobile number (numbers only) |
| userEntityIdentityType | Alphanumeric | O | 20 | Identify Type  (  PASSPORT,  TAX\_ID,  NATIONAL\_ID  ) |
| userEntityIdentity | Alphanumeric | O | 20 | Identify Number  This field is mandatory if the “userEntityIdentityType” field has value. |
| address1 | Alphanumeric | O | 80 | Address Line 1 |
| address2 | Alphanumeric | O | 80 | Address Line 2 |
| address3 | Alphanumeric | O | 80 | Address Line 3 |
| postalCode | Alphanumeric | O | 20 | Postal code |
| city | Alphanumeric | O | 40 | City |
| countryCode | Alphanumeric | O | 3 | Country code |
| state | Alphanumeric | O | 40 | State |
| emailId | Alphanumeric | O | 75 | Email ID |
| kycFlag | Alpha | O | 1 | KYC Flag (‘Y’ or ’N’)  Y – KYC completed N – KYC pending |

**Response Private Claim Fields:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Parameter** | **Data Type** | **M/O** | **Size** | **Value** |
| responseCode | Alphanumeric | M | 3 | 000 – success, any other response code is considered as error. Refer to message field for detail. |
| message | Alphanumeric | O | 200 | Additional information on the status |
| rrn | Alphanumeric | M | 20 | Retrieval Reference Number |
| authidresp | Alphanumeric | O | 10 | Authorization ID Response, available only for successful transactions |
| txnUid | Alphanumeric | M | 20 | Transaction Unique ID / Transaction reference |
| userEntityId | Alphanumeric | M | 40 | User Entity Account ID |
| trxnTime | Alphanumeric | M | 17 | This is the time stamp of the transaction in the format “yyyyMMddHHmmssS” |
| trxnTimeZone | Alphanumeric with special chars | O | 10 | RFU |

# Request/Response Samples

## Topup

**Request**:

{

"platformCode": "META",

"userEntityId": "PL000000000000107301",

"walletId": "MPW00000000000106704",

"digitalAssetTypeCode": "GC001",

"quantity": "10",

"terminalId": "T0000004",

"platformRef": "20190412111910",

"timestamp": "20190412111910",

"remarks": "Topup"

}

**Response**:

{

"responseCode": "000",

"message": "Success",

"rrn": "191209090551",

"authidresp": "9785705485",

"platformRef": "20190412111910",

"txnUid": "19120900105451",

"trxnTime": "20191209121042310",

"digitalAssetTypeCode": "GC001",

"availableQuantity": "87.000",

"userEntityId": "PL000000000000107301",

"walletId": "MPW00000000000106704"

}

## Onboard

**Request:**

{

"platformCode": "META",

"terminalId": "T0000004",

"name": "Player 1",

"mobileNo": "8765987",

"userEntityIdentityType": "PASSPORT",

"userEntityIdentity": "G19992244X",

"userEntityType": "PLAYER",

"address1": "address1",

"address2": "address2",

"address3": "address3",

"postalCode": "345990",

"city": "SG",

"countryCode": "SG",

"timestamp": "20190412111910",

"state": "SG",

"emailId": "abc@abc.com",

"kycFlag": "N"

}

**Response:**

{

"responseCode": "000",

"message": "Success",

"rrn": "191209090555",

"authidresp": "6965574669",

"userEntityId": "CUST00107552PLAYER",

"txnUid": "19120900105455",

"trxnTime": "20191209121826685",

"walletId": "MPW00106954"

}

## Sample Data

|  |
| --- |
| platformCode |
| META |

|  |
| --- |
| terminalId |
| T0000004 |

|  |  |
| --- | --- |
| digitalAssetTypeCode | description |
| GC001 | Gold Coins |

|  |  |
| --- | --- |
| walletId | userEntityId |
| MPW00000000000106704 | PL000000000000107301 |
| MPW00000000000106754 | PL000000000000107351 |
| MPW00000000000106755 | PL000000000000107352 |

Field “userEntityId” must be used with its own associated “walletId” as described in the above table.

## Response Codes

|  |  |
| --- | --- |
| responseCode | message |
| 000 | Success |
| 500 | Incorrect Request data |
| 300 | Platform not found |
| 900 | User Entity not found |
| 920 | Wallet not found |
| 270 | Digital Asset Type not found |
| 930 | Wallet not Active |
| 910 | User Entity not Active |
| 940 | Duplicate User Entity |

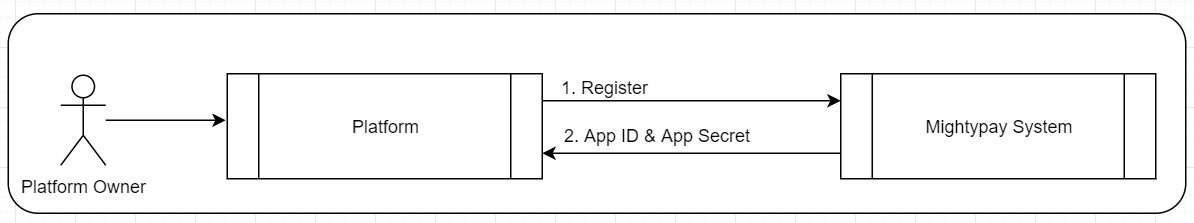
# Security Implementation

In phase 2, the Mightypay system will use JOSE to send/receive the message (payload) securely from the platform owner.

## Acquiring App ID & App secret

This is a manual step (for now).

Each platform owner who needs to call the Mightypay system will have to be registered and be provided with an application identifier and an application secret. Application identifier and application secret are used in the API calls for the system to be able to identify and authenticate that the transactions come from a valid source.



## Securing Messages using JOSE (JWT, JWE, JWS).

The secure messaging between the platform owner system and Mightypay system is designed based on JavaScript Object Signing and Encryption (JOSE), thereby ensuring confidentiality, integrity and authentication during communication between the two parties.

EX.

Messages will be sent in the form of **JWS** to the Mightypay system.

**JWS**:

Format:

JWS = Header.Payload.Signature

* **Header** = BASE64URL(UTF8(**JWS Protected Header**))

**JWS Protected Header** is in the form of a JSON message containing the following fields: “alg” and “typ”

Example = {“typ”: “JWT”, “alg”: “HS256”}, indicates that encoded object is a JSON Web Token (JWT) and the payload is signed with HMAC SHA-256

* **Payload**= BASE64URL(UTF8(**JSON message**))

JSON message

|  |  |
| --- | --- |
| Claims (Fields) | Description |
| iss | indicates the Application ID |
| iat | issue at time, indicates timestamp of the current request |
| sub | type of request (ex: Load Wallet/Onboard User) |
| jwe | **Actual JSON message** **payload** in encrypted form |
| appId | indicates the Application ID |
| authToken | session ID after successful authentication.  This will be used for all the request except login. |

* **Signature** = BASE64URL(HMAC SHA256**appSecret**(**data**))

**data** = ASCII(BASE64URL(UTF8(JWS Protected **Header**)) || '.' || BASE64URL(JWS **Payload**))

**JWE:**

**Actual JSON Message Payload in encrypted form.**

To encrypt the **CEK** (Content Encryption Key) **Auth token & Auth Secret** (This will be obtained upon successful login using the valid platform owner credentials. Details related to login API (which will be provided in phase 2) needs to use for all the request except login.

For login, App ID & App Secret will be used for CEK encryption.

Format:

JWE = Header.encryptedCEK**.**IV**.**Ciphertext**.**AuthenticationTag

* **Header** = BASE64URL(UTF8(**JWS Protected Header**))

JWS Protected Header is in the form of a JSON message containing the following fields: “enc” and “alg”

|  |  |
| --- | --- |
| Claims (Fields) | Description |
| enc | content encryption algorithm to produce the ciphertext and the Authentication Tag |
| alg | identifies the cryptographic algorithm used to encrypt or determine the value of the CEK |

* **encryptedCEK** = BASE64URL(Encrypted CEK)

CEK – Content encryption key. This is used to encrypt the actual payload.

Encrypted CEK - Encrypt the CEK with shared secret (**Auth token & Auth Secret** or **App ID & App Secret**) using A256KW algorithm

* **IV**

JWE Initialization Vector

* **Ciphertext** = BASE64URL(encrypted payload)

Additional Authenticated Data = ASCII(BASE64URL(UTF8(JWE Protected Header)))

Encrypted payload – Encrypt payload with AES GCM using CEK with IV and additional authenticated data.

Authentication Tag – Obtain Authentication Tag using the encrypted payload.

* **AuthenticationTag** = BASE64URL(Authentication Tag)

Complete JWE Representation

Assemble the final representation: The Compact Serialization of this result is the string BASE64URL(UTF8(JWE Protected Header)) || '.' || BASE64URL(JWE Encrypted Key) || '.' || BASE64URL(JWE Initialization Vector) || '.' || BASE64URL(JWE Ciphertext) || '.' || BASE64URL(JWE Authentication Tag).























Refer this [link](https://tools.ietf.org/html/rfc7516) for more information related to the JWE.