

Developer's Guide <Summary>



VERSION 1.2
2020/3/14

Attention

- Note that the contents of this manual are subject to change without prior notice. The latest version of this manual is shown on COMSUITE API Portal.
- Before using the Service, please be thoroughly familiar with and understand how to use the equipment and software as well as restrictions and other assumptions.
- This manual is property of MUFG Bank and shall not be given to any third party.
- Copyright for this manual belongs to the Bank. Reproduction in full or in part of this manual is prohibited; however, the user may reproduce only one copy of this manual for his or her own personal use.
- “COMSUITE” and “GCMS Plus” are registered trademarks or the trademarks of MUFG Bank, Ltd. in Japan and other countries.
- Trademark symbols ™ and ® are not noted in the text of this manual.

Published by: MUFG Bank, Ltd.

Copyright © MUFG Bank, Ltd. All rights reserved.

Table of Contents

0. Purpose of this guidebook	1
1. About COMSUITE API Service	1
1.1 Conceptual diagram.....	1
1.1.1 Production environment	1
1.1.2 Test Facility.....	2
1.2 API Standard	2
1.3 Outline of COMSUITE API Service authentication and API call	2
1.4 List of APIs provided.....	4
1.5 Service hours.....	6
2. Operating environment	6
3. Connection method.....	6
3.1 Processing method.....	6
3.1.1 General information of APIs	6
3.2 Others	7
3.2.1 Volume limit	7
3.2.2 Behavior in case of error	7
3.2.3 Questions about APIs.....	7
4. On Boarding Process.....	7
5. Test Facility	7
5.1 Test Facility	7
5.1.1 Functions to be provided	8
5.1.2 Service hours.....	9
5.1.3 Test method.....	9
5.2 Functions to be provided	11
5.2.1 Overview of Test Facility authentication method and API call	11
5.2.2 Lifecycle of access tokens.....	11
5.2.3 Setting of redirect URI	12
5.2.4 Registration of client certificates	12
Revision history	14

0. Purpose of this guidebook

This guidebook is to assist third party providers (TPP) in using COMSUIE API Service provided by MUFG Bank (hereinafter, referred to as "MUFG"). This guidebook provides a broad explanation on how to use COMSUIE API Service, such as a COMSUIE API Service outline, procedures to use COMSUIE API Service, and termination of using COMSUIE API Service.

1. About COMSUIE API Service

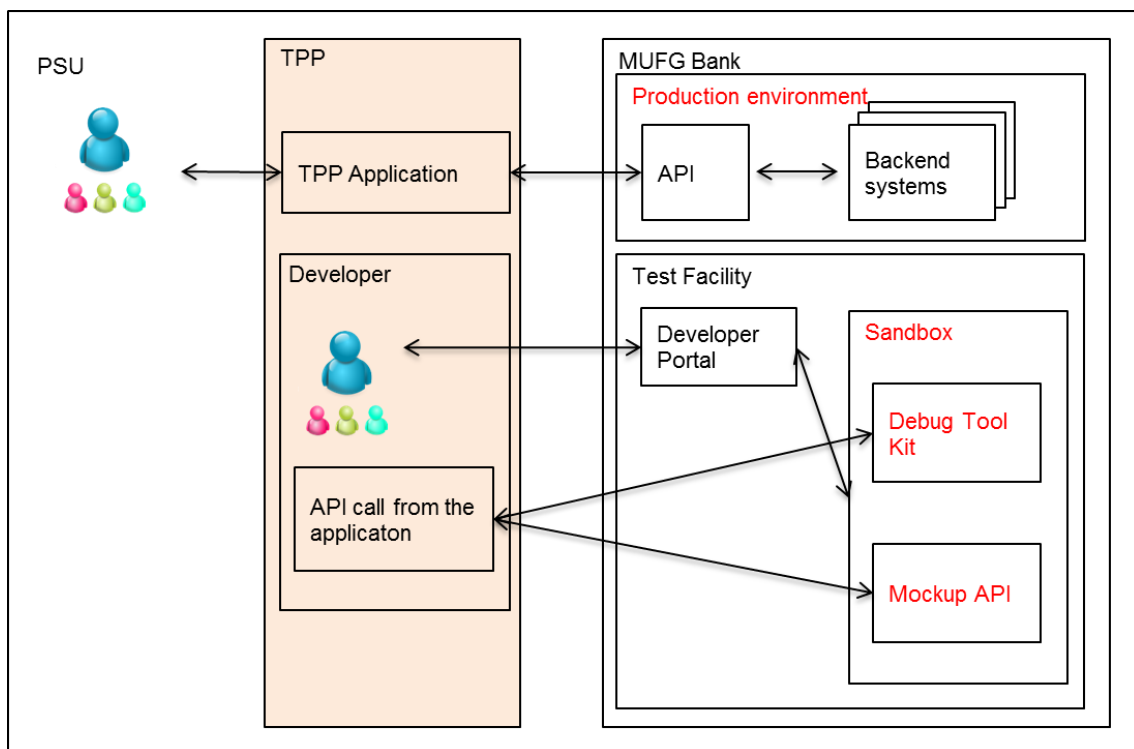
COMSUIE API Service is available to customers using MUFG Global CMS (*1) (GCMS Plus).

(*1) Cash Management Service

1.1 Conceptual diagram

COMSUIE API service has following two environments;

- Production environment
- Test Facility



1.1.1 Production environment

This environment offers MUFG's production COMSUIE API services. It connects to MUFG's internal systems, such as customer authentication system and backend systems.

1.1.2 Test Facility

This environment offers set of functions to test MUFG's API. It consists of following components;

- COMSUITE API Portal

Website to view the reference of MUFG's APIs. You can create accounts and obtain API keys to use the "Mockup API" and "Debug Tool Kit" below.

- Mockup API

Mockup environment to check behaviors of MUFG's APIs.

This is not connected to the production environments, and returns mockup-specific dummy data.

- Debug Tool Kit

<Error Registration Tool>

This tool is used to simulate error responses that cannot be generated by executing the above Mockup API.

1.2 API Standard

MUFG's API follows the standard defined by Berlin Group (*1) which is found in the public document "NextGenPSD2 Access to Account Interoperability Framework - Implementation Guidelines" (*2).

(*1) Berlin Group : <https://www.berlin-group.org/nextgenpsd2-downloads>

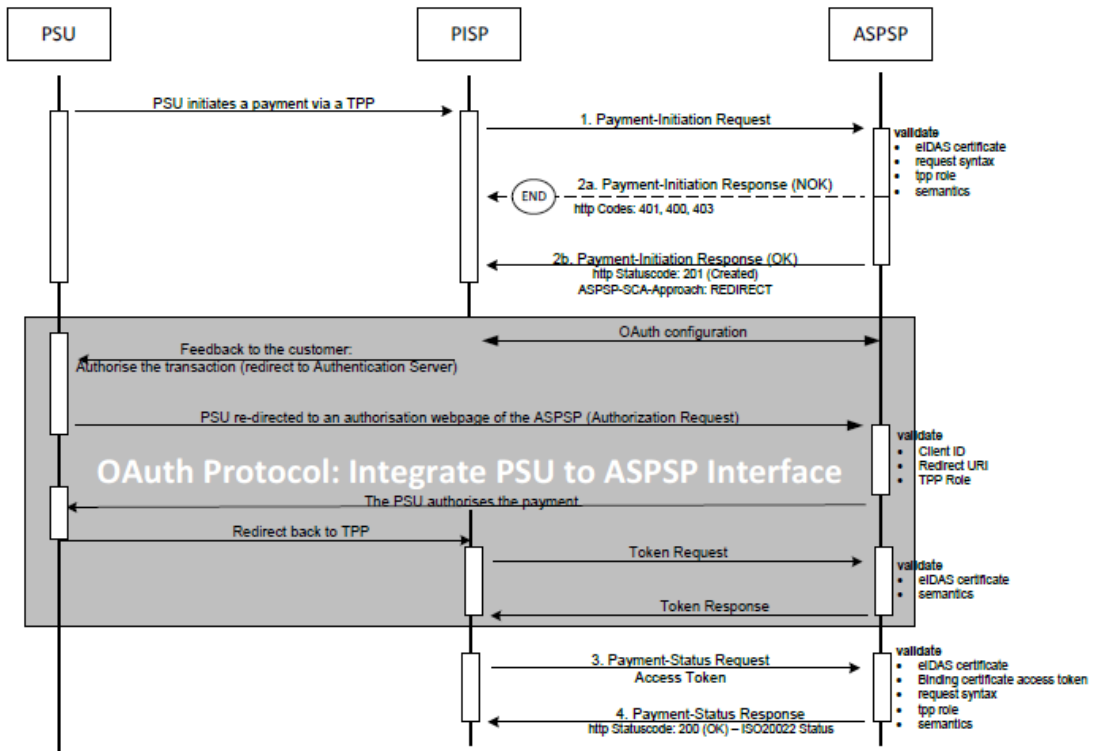
(*2) Version 1.3 as of 2019/03/14

1.3 Outline of COMSUITE API Service authentication and API call

MUFG API supports OAuth2 SCA Approach.

Payment Initiation Service (PIS):

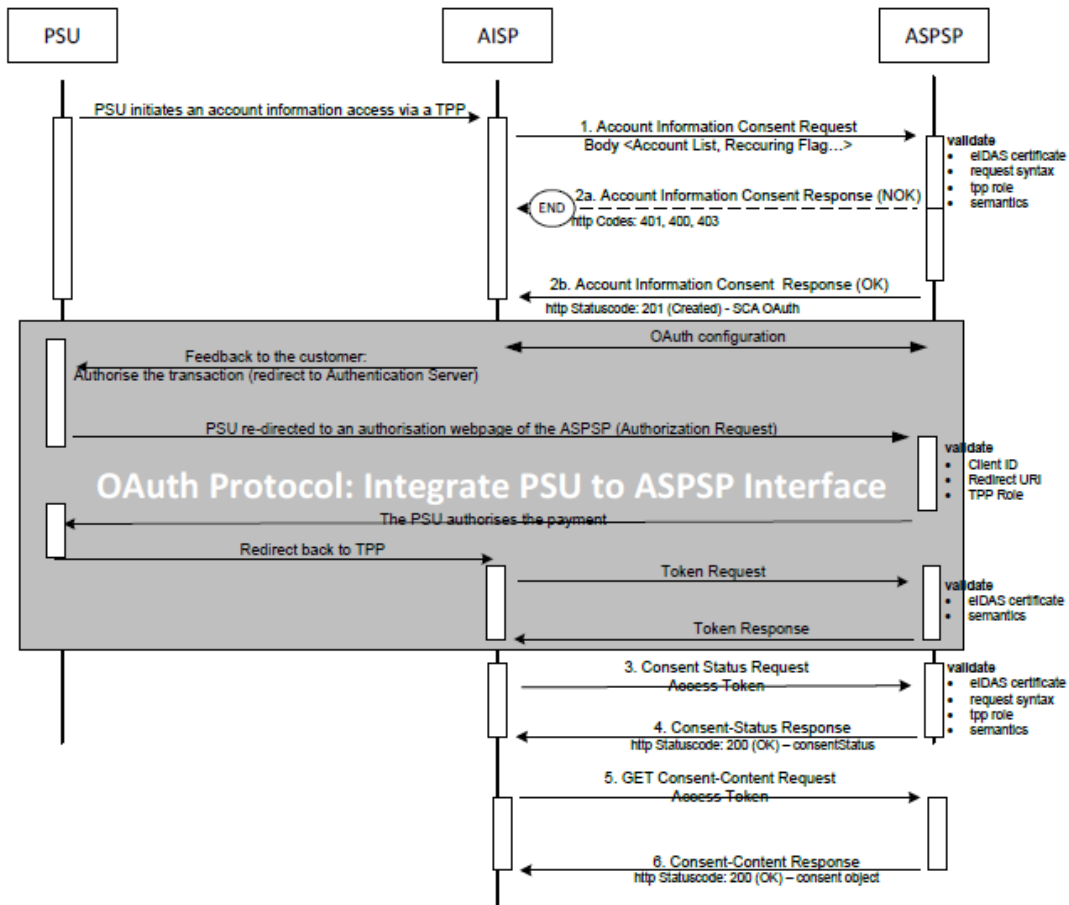
The payment initiation flow with OAuth2 SCA Approach can be shown as below;



Source: NextGenPSD2 Access to Account Interoperability Framework - Implementation Guidelines V1.3_20181019.pdf, Page48, <https://www.berlin-group.org/nextgenpsd2-downloads>

Account Information Service (AIS):

The Account information consent flow with OAuth2 SCA Approach can be shown as below;



Source: NextGenPSD2 Access to Account Interoperability Framework - Implementation Guidelines V1.3_20181019.pdf, Page102, <https://www.berlin-group.org/nextgenpsd2-downloads>

1.4 List of APIs provided

MUFG's APIs are as follows.

Payment Initiation Service (PIS)

API Name	Endpoints	Method	Description
payments1	payments/{payment-product}	POST	Creation of Single Payment: Enables acceptance of single payments.
bulk-payment s1	bulk-payments/{payment-product}	POST	Creation of Bulk Payment: Enables acceptance of bulk payments.
payments2	payments/{payment-product}/{paymentId}/status	GET	Inquiry of Applied Single Payment: Returns status of acceptance of single payments.
bulk-payment s2	bulk-payments/{payment-product}/{paymentId}/status	GET	Inquiry of Applied Bulk Payment: Returns status of acceptance for

			bulk payments.
authorization s2	authorize	GET	Issues authorization code (PIS service).
	token	POST	Issues access token (PIS service).

Account Information Service (AIS)

API Name	Endpoints	Method	Description
consents1	consents	POST	Creation of Consent: Creates end user's consent resource.
consents2	consents/{consentId}	GET	Inquiry of Consent Information: Returns consent details.
		DELETE	Deletion of Consent: Deletes a consent.
accounts	accounts	GET	Inquiry of Account Information: Returns a list of accounts for which consent has been obtained.
	accounts/{account-id}/balances	GET	Inquiry of Account Balance: Returns balance information for a designated account.
	accounts/{account-id}/transactions	GET	Inquiry of Transaction History: Returns transaction details for a designated account.
authorization s1	authorize	GET	Issues an authorization code (AIS service).
	token	POST	Issues an access token (AIS service).

Fund Confirmation Service (FCS)

API Name	Endpoints	Method	Description
funds-confirmations1	/consents/confirmation-of-funds	POST	Creation of Consent: Creates end user's consent resource.
funds-confirmations2	/consents/confirmation-of-funds/{consentId}	GET	Inquiry of Consent Information(FCS): Returns consent details(FCS service).
		DELETE	Deletion of Consent(FCS): Deletes a consent(FCS service).

	funds-confirmations	POST	Checks whether a specific amount is available on a designated account.
Authorization s3	authorize	GET	Issues an authorization code (FCS service).
	token	POST	Issues an access token (FCS service).

1.5 Service hours

➤ Production environment

MUFG's Production Environment is available 24 hours a day except for the following regular maintenance window;

Service suspension period
Saturday 22:00 (JST) ~ Monday 02:00 (JST) every week

➤ Test Facility

Test Facility can be used 24 hours a day regardless weekdays or weekend. Note that the Test Facility may be unavailable without pre-notice due to any urgent maintenance.

➤ Availability SLO (Service Level Objective): 99.0%

2. Operating environment

The API standard of GCMS Plus complies with Berlin Group. Also, certificates used for APIs comply with eIDAS and OBWAC certificate.

OS and browser depend on the support environment of GCMS Plus.

Berlin Group : <https://www.berlin-group.org/>

eIDAS : <https://www.eid.as/home/>

GCMS Plus : https://www.bk.mufg.jp/ebusiness/e/gplus/environment_otp.html

3. Connection method

3.1 Processing method

This section describes notes for development, such as processing methods when calling API.

3.1.1 General information of APIs

➤ Implementation of OAuth2.0

MUFG's OAuth2.0 API complies with the RFC6749 rules/Berlin Group.

➤ Invalidation conditions for access tokens

AIS: 90 days and PIS: 30 days are set as the validity period for access tokens.

However, even within the validity period, re-registration may be required depending on the customer's status. Also expired access tokens will be invalidated. MUFG does not support refresh tokens, so re-authentication is required by customers upon invalidation.

- Functions for access token invalidation and release of invalidation
As TPP, please develop system functions (token invalidation, etc.) and prepare to respond to customers' requests to suspend usage, terminate usage, and release suspension of COMSUITE API Service.

3.2 Others

3.2.1 Volume limit

- There is a limit on the number of API calls per unit hour per TPP (client ID).
- The number of API calls is counted per requested API.
- If the volume limit is exceeded, it is responded with error details.
- Basically, the limit is 2 calls/s (per API).
(E.g.) Three API requests for balance inquiries in a second → Up to two are accepted, and the third is responded to with an error.
Two API requests for balance inquiry and one API request for transaction inquiry in a second → All are accepted because each number of requests is within the limit per API.
- Separate from the volume limit per TPP, there is another limit on the number of calls that can be accepted simultaneously by MUFG. When the limit is exceeded (busy status), all TPPs are responded with an error of limit excess.
- If a volume excess error (HTTP status 429 or 430) is received, TPP should control the volume to ensure a sufficient interval until the next request.
- TPP needs to adequately schedule evening batches so as not to reach the limit on the number of API calls.

3.2.2 Behavior in case of error

Behavior for returning MUFG's API errors complies with Berlin Group 1.3.

3.2.3 Questions about APIs

Submit questions to the contact at MUFG as per the guidance of the COMSUITE API Portal.

4. On Boarding Process

See COMSUITE API Portal "Getting started" page.

5. Test Facility

5.1 Test Facility

MUFG's API is made available individually for the COMSUITE API Portal user ID that is provided to MUFG.

5.1.1 Functions to be provided

Test Facility is comprised of "Mockup API" to simulate the production environment APIs and "Debug Tool Kit" to drop test data.

➤ Mockup API

Each API is simulated based on dummy data.

Differences from the production environment APIs are described below.

POST /v1/payments/{payment-product}

Statuses after submission cannot be updated by requests.

(because no subsequent functions after payment (approval/rejection function on G+) are provided.)

POST /v1/bulk-payments/{payment-product}

A normal response returns response data of fixed values.

GET /v1/payments/{payment-product}/{paymentId}/status

Statuses and error information that never occur in the Test Facility (e.g. transactionStatus is ACSP) are stored in dummy data. To obtain this information, set paymentId of each dummy data in your request data.

See [5.2.2 "List of dummy data"](#) for details.

GET /v1/bulk-payments/{payment-product}/{paymentId}/status

A normal response returns response data of fixed values.

GET /v1/accounts?{query-parameters}

GET /v1/accounts/{account-id}/balances

GET /v1/accounts/{account-id}/transactions?{query-parameters}

The above API is no different from the API specifications of Production Environment.

POST /v1/consents

POST /v2/consents/confirmation-of-funds

Statuses after submission cannot be updated by above requests.

(Because data required for updating the status (e.g. PSU user information) is not held.)

GET /v1/consents/{consentId}

GET /v2/consents/confirmation-of-funds/{consentId}

For the above API, statuses that never occur in the Test Facility (e.g. consentStatus is revokedByPsu) are stored in dummy data. To obtain this information, set consentId of each dummy data in your request data.

See [5.2.2 "List of dummy data"](#) for details.

DELETE /v1/consents/{consentId}

DELETE /v2/consents/confirmation-of-funds/{consentId}

For the above API, registered information is not updated, and actual deletion (change of consentStatus to terminatedByTpp) is not performed. Based on request information, it only determines whether the consent can be deleted or not.

POST /v1/funds-confirmations

The above API is no different from the API specifications of Production Environment.

GET /authorize

For the above API, the same customer authentication as Production Environment does not exist, and a static customer authentication screen is generated.

POST /token

In the above API, access tokens never expire.

➤ Debug Tool Kit

Error Registration Tool

Forcedly instructs the specified API to return error response.

5.1.2 Service hours

Test Facility can be used 24 hours a day regardless weekdays or weekends.

(It may be suspended without prior notification due to maintenance, etc.)

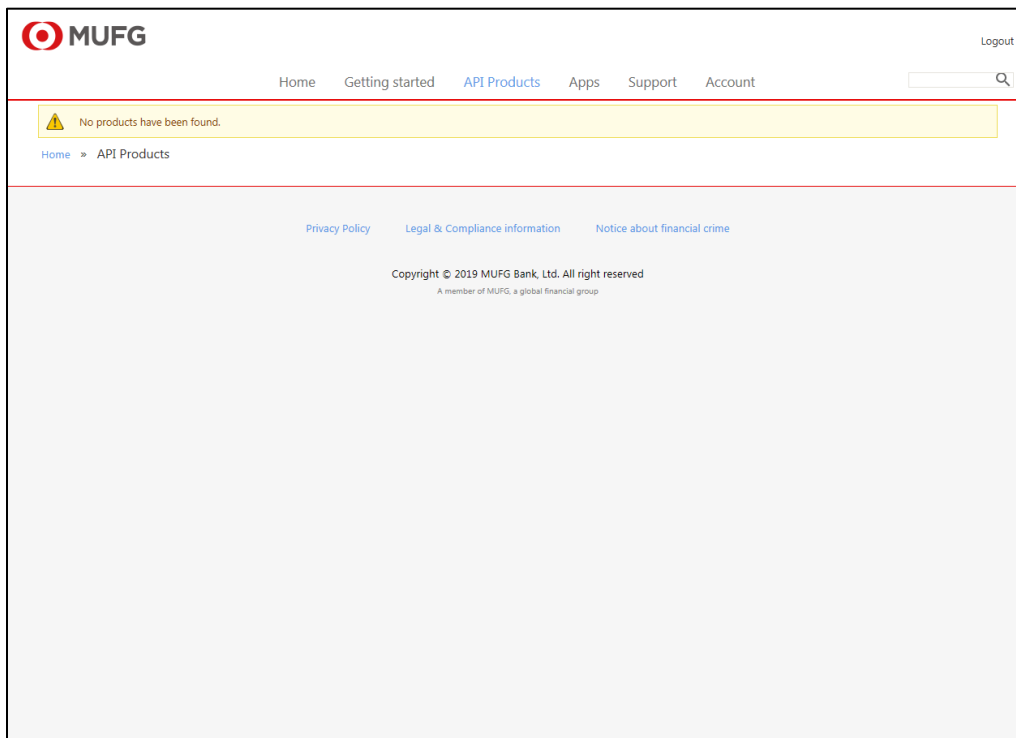
5.1.3 Test method

➤ Starting test

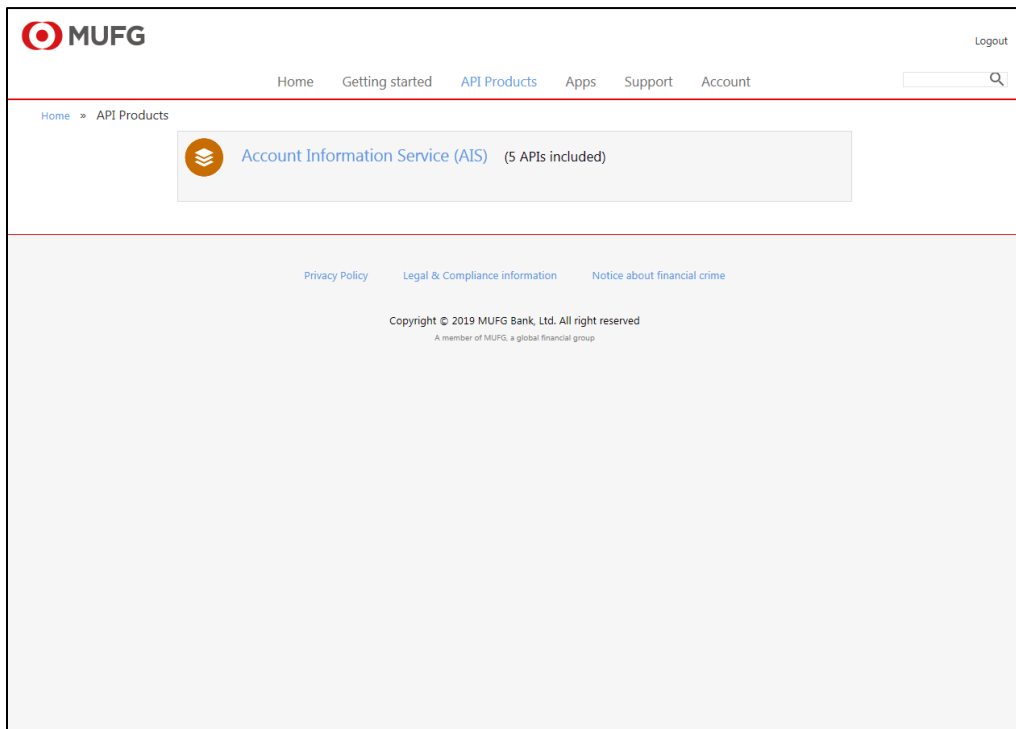
Please go through the following procedure to perform tests.

(1) Test Facility is opened upon application for use.

E.g.) Before application



E.g.) After application



Please confirm that the number of selected API products is increased.

(2) After informed by MUFG that Test Facility is available, select a course to be used respectively for AIS, PIS, or FCS from the above screen, and subscribe for a client ID for testing.

(3) Perform test to check variations in the test data and error occurrence status. Use Error Registration Tool from the debug tool as needed.

➤ Volume limit

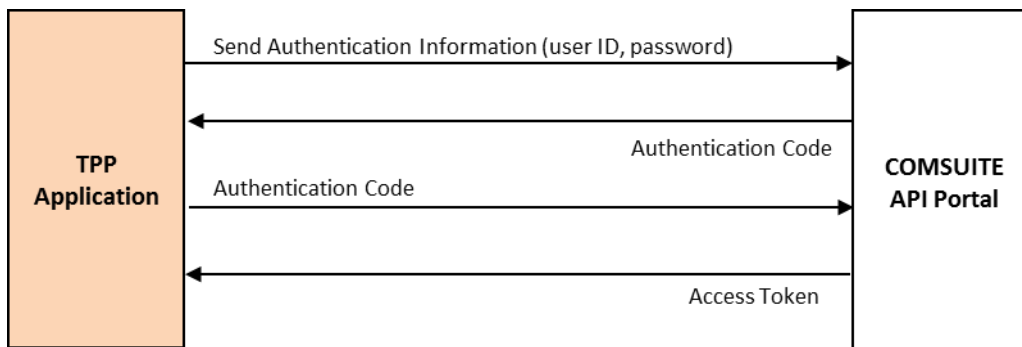
The API volume limit for Test Facility is 2 calls/s (per API).

5.2 Functions to be provided

5.2.1 Overview of Test Facility authentication method and API call

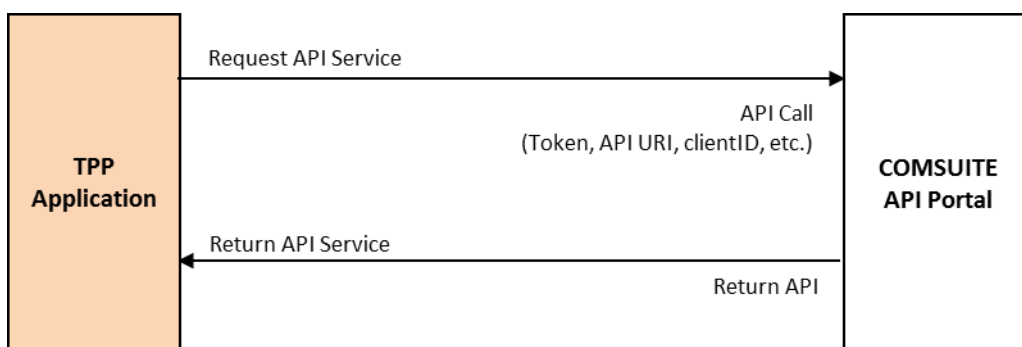
➤ Mechanism of authentication/authorization

Authentication and authorization processes when Test Facility is used are as follows.



➤ Mechanism for API call

The process when Test Facility is used is as follows. (It is assumed that authentication/authorization is done and tokens are issued for the process.)



5.2.2 Lifecycle of access tokens

Tokens never expire. Before checking behavior upon token invalidation, make the invalidated state with the Debug Tool Kit (Error Registration Tool).

5.2.3 Setting of redirect URI

Set redirect URI from the API key issuance registration screen or the registered API key editing screen of the API developer portal. Input redirect URI used for your company's test in the "OAuth Redirect URI" field on these screens.

The screenshot shows the MUFG API developer portal interface. At the top left is the MUFG logo. The top navigation bar includes links for Home, Getting started, API Products, Apps, Support, and Account, along with a search icon and a Logout link. The breadcrumb trail indicates the current page is 'Home » Create Application'. The main heading is 'Register application'. The form contains several fields: 'Title *' (a text input field), 'Description' (a text area), 'OAuth Redirect URI' (a text area highlighted with a red border), and 'Certificate' (a text area). Below the 'Certificate' field is a 'Submit' button. The 'OAuth Redirect URI' field has a placeholder text: 'The URL authenticated OAuth flows for this application should be redirected to.'

5.2.4 Registration of client certificates

Set client certificate information from the API key issuance registration screen or the registered API key editing screen of the API developer portal. Input and register client certificates to be used for your company's test in the "Certificate" field on these screens.

Home > Create Application

Register application

Title *

Enter preferable title such as application name, API user name etc.

Description

Enter any other information if necessary.

OAuth Redirect URI

The URL authenticated OAuth flows for this application should be redirected to.

Certificate

Paste the content of your application's x509 certificate.

Submit

Revision history

Date	Version	Detail of change
14 th Mar 2019	Version 1.0	Frist Publish
13 th Dec 2019	Version 1.1	1.4 List of APIs provided 5.1.1 Functions to be provided - Added APIs Modified based on Developer's Guide version 1.4
14 th Mar 2020	Version 1.2	5.1.1 Functions to be provided - Deleted old version FCS API