Introduction

CApp is a core API designed by Cellcard, which receives requests from Clients (first-party or third-party application) who want to make manipulation system information. To make this possible, there will be a connection between Clients and CApp performing communication through the protocol defined in this document.

Purpose

In essence this document provides all the detailed information on “how third party apps” can interact with cellcard’s self-care application. The content of this document is highly focusing on defining the API contracts that can be consumed by any eligible third party .

Document Scope

This document focus on API which allows third party applications perform various functions as permitted by Cellcard.

Overview

This is a sample API which provides an insight of the API documentation of actual API published to public users.

Sending Information

The request of information over the Web-Service will done over the establishment of an **HTTP(s)** connection, and body content will indicate the requested method and the input parameters.

The request payload must be JSON. The **HTTP(s)** response will be in form of JSON too.

Field Definition

The type of fields to be defined, will be interpreted according to the following definition:

String characters: ***String [length].***

The number between "[]" is the length of the String. It can be defined in two ways:

· String [0-20]: String with length from "0" to "20" characters

· String [14]: String with length of "14" characters.

The mandatory or optional fields will be defined as follows:

· **M**: Mandatory Field

· **O**: Optional Field

Possible Values: [type]{length}: The number between "[]" is the accepted type of values and the value between {} indicates the accepted length of the parameter.

Token Generation

We support the standard OAuth 2.0 Client Credentials OAuth Flow. To generate token:

*$ curl -d "grant_type=client_credentials" *

*-H "Authorization: Basic {BASE64_OF_CONSUMER_KEY:CONSUMER_SECRET}" *

https://stg-api.cellcard.com.kh:8243/token

{"access_token":"489fea0e-5786-3073-b2f0-6b82c2b00449","scope":"am_application_scope default","token_type":"Bearer","expires_in":3600}

API Description

API Base URLs

Production	https://prd-api.cellcard.com.kh:8243/cappcore/v1/
Staging	https://stg-api.cellcard.com.kh:8243/cappcore/v1/

Usage

Sample Request format

```
curl -k --request POST \
--url https://stg-api.cellcard.com.kh:8243/cappcore/v1 \
--header 'authorization: Bearer 24a73h756-bol8-3f9a-950b-484jn9f23' \
--header 'content-type: application/json' \
--data '{
  "Retrieve":{
    "msisdn":"85592260627",
    "method_name":"Get Cellcard Infor V2",
    "channel":"ussd",
    "reqID":"123456"
  }
}'
```

- *This is a sample request. Actual request payload will differ based on req method.*

Input Headers

Header Name	Value	Description
Content-Type	application/json	Only supports JSON
Authorization	Bearer {API Access Token}	OAuth 2 based access token

Payload Parameters

Parameter	Type	Description
msisdn	String	MSISDN value for the SIM
method_name	String	Execution method name
channel	String	Input Channel
reqID	String	Unique ID of the request

Output Response Codes

HTTP Code	Description
201	Successfully completed the operation
401	Unauthorized access with invalid or expired token
403	Unauthorized to perform the action
500	Internal server error

Result Codes

Result Code	Description
0000	Success

Authorization

API is exposed from WSO2 API Gateway with standard OAuth based authentication mechanism which an access token needs to be sent as a header field along with the API call. Currently a 1 hour-expiring token is provided but this token can be rotated and communicated to the clients if required.

Auth information in request

API key MUST be sent as a header parameter as bearer token as described below. This key will be sent to relevant third party apps via secured channel.

Header Name	Type	Description	Sample
Authorization	Bearer	Standard header field to send bearer tokens	authorization: Bearer 0c94f4b6-sf87fas-30a6-a7b4-gd d786fd76sfa

Unauthorized Error Response

In the case of key unavailability in the request or invalid key API returns below standard HTTP status code for unauthorized access.

HTTP Status Code	Description
401	This implies the request unauthorized due to an invalid access token