OPEN BANKING

JROC Workstream 1 – Levelling Up ASPSP Reporting Data Metrics

Classification: Confidential

Version Control

Date	Version	Details
09/11/2023	1.0	• Initial version presented in tutorial.

ASPSP Data Metrics

- This document provides further information for the data metrics required to be reported by ASPSP, following the JROC workstream 1 consultation.
- Reporting template includes both phase 1 and phase 2 data requirements.
- Reporting is currently optional; however, JROC have indicated they expect ASPSPs to provide data voluntarily:
  - Phase 1 data – from February 2024 (based on January 2024 performance).
  - Phase 2 data – from July 2024 (based on June 2024 performance); however, ASPSPs may submit this data sooner if they are able.
- Reporting data key:

Phase 1 reporting data dimension	Required data allowing OBL to report performance at different levels of granularity.
Phase 1 reporting data measure	Required data allowing OBL to report performance metrics.
Phase 2 reporting data dimension/measure	Secondary colour indicates where metric is a dimension or measure - data can be reported as soon as data is available.

- Monthly submissions to OBL will initially be due by 3pm on working day 10 of the following month. (This may be reduced in future).
- OBL will confirm submission email address ahead of first submissions.
- A secure file transfer platform [Cocoon Data SafeShare or an AWS based solution] is available as an alternative to email

OPEN BANKING

Return 1 – Performance and Availability

Reporting Date	Core/Non-Core *[Phase 2 req]*	ASPSP Brand ID	Endpoint ID	API Version	Successful API calls	Failed API calls - Business	Failed API calls - Technical	Rejected API calls *[Phase 2 req]*	Planned Downtime	Unplanned Downtime	Uptime	Total TTFB (m/s) (Time to First Byte)	Total TTLB (m/s) (Time to Last Byte)
2023-10-01	Core	9999	8	v3.1.10	14785542	1	12	0	0:00	0:03	17:57	6224713182	6313426434
2023-10-01	Non-core	9999	8	v3.1.10	488524	28	461	0	2:15	0:00	3:45	260383292	264291484

Return 1 – Performance and Availability

Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
Reporting Date	The reporting date for each calendar day during the reporting period.	ISOdate(10)	YYYY-MM-DD	Reporting Date is a mandatory field and combines with ASPSP Brand ID, Endpoint ID, and API Version to create the unique record key.
Core/Non-Core *[Phase 2 req.]*	Used for reporting the availability and performance of each individual endpoint during core hours (06.00-0.00) and non-core hours (0.00-06.00) of each calendar day.	TEXT(10)	Core Non-core	
ASPSP Brand ID	Reporting ASPSP Brand ID as defined in Brand ID reference data.	INT(4)	0-9999	ASPSP Brand ID is a mandatory field and combines with Reporting Date, Endpoint ID, and API Version to create the unique record key.
Endpoint ID	Reported Endpoint ID as defined in API Endpoint List. https://openbankinguk.github.io/mi-docs-pub/v3.1.10-aspsp/specification/mi-data-reporting-api-specification.html#_2-1-api-endpoint-list	INT(4)	0-9999	ASPSPs must only report endpoints that have gone live in their systems. Endpoint ID is a mandatory field and combines with Reporting Date, ASPSP Brand ID, and API Version to create the unique record key.
API Version	The Open Banking Standards version of the endpoint implementation by the ASPSP. Must include major, minor, and point version.	TEXT(10)	vN.N.nn	API Version is a mandatory field and combines with Reporting Date, ASPSP Brand ID, and Endpoint ID to create the unique record key.

Return 1 – Performance and Availability (cont.)

Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
Successful API calls	The total number of successful endpoint calls for each endpoint that have been received successfully by the ASPSP brand.	INT(10)	0-2147483647	Calls generating a HTTP Status Code of 200, 201 or 204 depending on the HTTP method of the endpoints.
Failed API calls - Business	This is the total number of failed endpoint calls for each endpoint that have been received by the ASPSP brand and failed due to business rules reasons.	INT(10)	0-2147483647	Calls generating a HTTP Status Code of 4xx.
Failed API calls - Technical	This is the total number of failed endpoint calls for each endpoint that have been received by the ASPSP brand and failed due to technical reasons.	INT(10)	0-2147483647	Calls generating an HTTP Status Code of 500 Internal Server Error. ASPSPs should exclude 5xx calls where a TPP continues to call their services during a period of Planned Outage [only]. For the avoidance of doubt, this means that these endpoint calls will not be reported.

Return 1 – Performance and Availability (cont.)

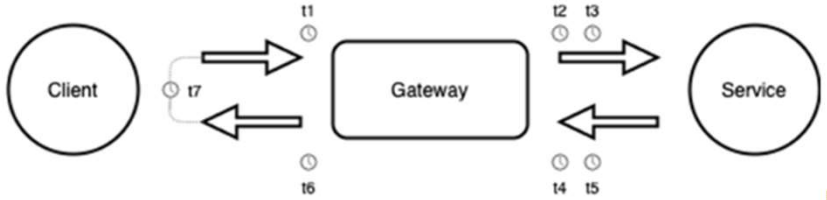
Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
Rejected API calls *[Phase 2 req]*	This is the total number of API calls that have been rejected for each endpoint.	INT(10)	0-2147483647	Where: a) Payments consent resources in the rejected state due to authorisation failing or consent authorisation being rejected. b) Payment resources in the rejected state due to payment initiation being rejected as part of proceeding checks such as technical validation and customer profile. c) Account access consent resources in the rejected state due to authorisation failing or consent authorisation being rejected. d) Funds-confirmation-consent resources in the rejected state due to authorisation failing or consent authorisation not agreed
Planned Downtime	Any planned duration that the API endpoints become unavailable. For the avoidance of doubt, this extends to include all systems that are required for the relevant endpoint to be fully functional. The clock for unavailability should start immediately and consolidated duration must be reported as elapsed time.	Time(5)	hh:mm	For phase 1 reporting, Planned Downtime, Unplanned Downtime, and Uptime must sum to 24:00. For phase 2 reporting, Planned Downtime, Unplanned Downtime, and Uptime must sum to18:00 for Core Hours, 06:00 for Non-core hours. Due to per-minute granularity, rounding is expected to take place to the nearest whole minute (e.g. 1 min 15 sec should be reported as 1 min, 1 min 40 sec should be reported as 2 min).

Return 1 – Performance and Availability (cont.)

Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
Unplanned Downtime	Any unplanned duration that the API endpoints become unavailable due to technical faults or any other reasons. For the avoidance of doubt, this extends to include all systems that are required for the relevant endpoint to be fully functional.	Time(5)	hh:mm	The clock for unplanned downtime should start as defined in https://openbankinguk.github.io/mi-docs-pub/v3.1.10-aspsp/specification/mi-data-reporting-api-specification.html#_1-1-1-dedicated-interface-downtime and consolidated as elapsed time. For phase 1 reporting, Planned Downtime, Unplanned Downtime, and Uptime must sum to 24:00. For phase 2 reporting, Planned Downtime, Unplanned Downtime, and Uptime must sum to18:00 for Core Hours, 06:00 for Non-core hours. Due to per-minute granularity, rounding is expected to take place to the nearest whole minute (e.g. 1 min 15 sec should be reported as 1 min, 1 min 40 sec should be reported as 2 min).
Uptime	Uptime per each individual endpoint in hours and minutes. (Elapsed time). For endpoints to be reported as available, they need to be fully operational in terms of fulfilling their functionality and being able to respond back to the requesting TPP (i.e. no technical 5xx failures). However, this should exclude cases of network errors outside the ASPSP control or cases of TPPs becoming unavailable.	Time(5)	hh:mm	For phase 1 reporting, Planned Downtime, Unplanned Downtime, and Uptime must sum to 24:00. For phase 2 reporting, Planned Downtime, Unplanned Downtime, and Uptime must sum to18:00 for Core Hours, 06:00 for Non-core hours Due to per-minute granularity, rounding is expected to take place to the nearest whole minute (e.g. 1 min 15 sec should be reported as 1 min, 1 min 40 sec should be reported as 2 min).

Return 1 – Performance and Availability (cont.)

Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
Total TTFB (m/s) (Time to First Byte)	Sum of all the TTFB (Time To First Byte) responses of all endpoint calls of each endpoint type during the period.	LONGINT	TTFB <= TTLB	For the avoidance of doubt, this is the sum of all the TTFB response times generated by the Total Number of API calls for each endpoint.
Total TTLB (m/s) (Time to Last Byte)	Sum of all the TTLB (Time To Last Byte) responses of all endpoint calls of each endpoint type during the period.	LONGINT	TTFB <= TTLB	For the avoidance of doubt, this is the sum of all the TTLB response times generated by the Total Number of API calls for each endpoint.



Definitions

t1: The timestamp recorded when the request is initially received by the Gateway.

t2: The time when the request was initiated to the next available service.

t3: The time when the request write was started.

t4: The response time for each service.

t5: This is the read time for response content.

t6: The timestamp when the request write was initiated.

t7: The overall time taken between receipt of the incoming request and streaming of the complete response to the client.

Based on the above diagram and definitions:

TTLB = time period (t7) - (t1)

TTFB = time period (t6) - (t1)

Return 2 – Direct Channel Performance and Availability

Reporting Date	Core/Non-Core *[Phase 2 req]*	ASPSP Brand ID	PSU channel	Uptime (%)	Downtime (%) *[Phase 2 req]*
2023-10-01	Core	9999	Online	99.96	0.04
2023-10-01	Core	9999	Mobile	100.00	0.00
2023-10-01	Non-core	9999	Online	66.83	33.17
2023-10-01	Non-core	9999	Mobile	82.15	17.85

Return 2 – Direct Channel Performance and Availability

Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
Reporting Date	The reporting date for each calendar day during the reporting period.	ISOdate(10)	YYYY-MM-DD	Reporting Date is a mandatory field and combines with ASPSP Brand ID, and PSU Channel to create the unique record key.
Core/Non-Core *[Phase 2 req.]*	Used for reporting the availability and performance of each individual endpoint during core hours (06.00-0.00) and non-core hours (0.00-06.00) of each calendar day.	TEXT(10)	Core Non-core	
ASPSP Brand ID	Reporting ASPSP Brand ID as defined in Brand ID reference data.	INT(4)	0-9999	ASPSP Brand ID is a mandatory field and combines with Reporting Date, and PSU Channel to create the unique record key.
PSU channel	The native service channels offered by ASPSPs to allow users to access their accounts or initiate payments.	TEXT(10)	Online Mobile	PSU Channel is a mandatory field and combines with Reporting Date, and ASPSP Brand ID to create the unique record key.
Uptime (%)	Uptime for each PSU Channel, each day/reporting period, as a percentage of total seconds in the period.	Decimal(5,2)	0.00-100.00	Data should be expressed as a percentage without the '%' symbol in the data. For phase 2 reporting, Uptime %, plus Downtime % should equal 100%.
Downtime (%) *[Phase 2 req.]*	Downtime for each PSU Channel, each day/reporting period, as a percentage of total seconds in the period.	Decimal(5,2)	0.00-100.00	Data should be expressed as a percentage without the '%' symbol in the data. For phase 2 reporting, Uptime %, plus Downtime % should equal 100%.

Return 3 – Authentication Efficacy

Reporting Period	ASPSP Brand ID	Authentication type	API Type	TPP Channel	ASPSP Channel	Consents requiring Authentication	Authentications Attempted by PSUs	Authentication failed *[Phase 2 req]*	Authentications abandoned by PSU *[Phase 2 req]*	Consents succeeded	Payments successfully initiated *[Phase 2 req]*
01/10/2023	9999	Redirection	AIS	Non-browser	App	52479	48766	2634	9535	36597	
01/10/2023	9999	Redirection	AIS	Browser	Web	14895	9943	1956	3270	4717	
01/10/2023	9999	Redirection	PIS-Single	Non-browser	App	102664	99953	7881	4807	87265	81002
01/10/2023	9999	Redirection	VRP-Sweeping	Non-browser	App	5039	4871	101	162	4608	

Return 3 – Authentication Efficacy

Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
Reporting Period	The start of the monthly reporting period the data relates too.	ISOdate(10)	YYYY-MM-01	Reporting Period is a mandatory field and combines with ASPSP Brand ID, Authentication Type, API Type, TPP Channel, and ASPSP Channel to create the unique record key.
ASPSP Brand ID	Reporting ASPSP Brand ID as defined in Brand ID reference data.	INT(4)	0-9999	ASPSP Brand ID is a mandatory field and combines with Reporting Period, Authentication Type, API Type, TPP Channel, and ASPSP Channel to create the unique record key.
Authentication type	The type of authentication journeys provided by the ASPSP. It will include 'redirection' and where implemented 'decoupled' model.	TEXT(15)	Redirection Decoupled	Authentication Type is a mandatory field and combines with Reporting Period, ASPSP Brand ID, API Type, TPP Channel, and ASPSP Channel to create the unique record key.
API Type	This is the type of OBL services that are being reported for the efficacy of the authentication journey. It includes Account Information Services (AIS), Payment Initiation Services, excluding VRPs (PIS-Other), Variable Recurring Payments (Sweeping/Commercial), and Card-Based Payment Instrument Issuers (CBPIIs).	TEXT(10)	AIS PIS-Other PIS-sVRP PIS-cVRP CBPII	For the avoidance of doubt, PIS-Other reporting should include Internal transfers, FPS (single domestic), SO, FDP, All International, BACS and CHAPS payments. API Type is a mandatory field and combines with Reporting Period, ASPSP Brand ID, Authentication Type, TPP Channel, and ASPSP Channel to create the unique record key.

Return 3 – Authentication Efficacy (cont.)

Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
TPP Channel	The reported TPP channel for initiating the AIS, PIS (single or VRP) or CBPII consent.	TEXT(15)	Browser Non-browser Unknown	This may be provided by TPPs in the endpoint Request Header under the field 'x-customer-user-agent'. The reported value will be free format text however if populated, it will have well-known strings of characters for various popular browsers. If the string cannot be mapped to a browser, then it will probably be a mobile app (non-browser). TPP Channel is a mandatory field and combines with Reporting Period, ASPSP Brand ID, Authentication Type, API Type, and ASPSP Channel to create the unique record key.
ASPSP Channel	The reported ASPSP Authentication channel. It can be web-based (Web) or using the mobile banking app (App)	TEXT(15)	App Web Unknown	ASPSP Channel is a mandatory field and combines with Reporting Period, ASPSP Brand ID, Authentication Type, API Type, and TPP Channel to create the unique record key.
Consents requiring Authentication	The total number of PSU consents requiring authentication at the ASPSP for the combination of authentication type, API type, TPP channel and ASPSP authentication channel.	INT(10)	0-2147483647	This is the number of requests where the POST- consent response was 201 with consent status 'awaiting authorisation'.

Return 3 – Authentication Efficacy (cont.)

Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
Authentications Attempted by PSUs	The total number of authentications that have been attempted by the PSUs.	INT(10)	0-2147483647	This means that PSUs have tried to authenticate at least once, using the required method. E.g. providing biometrics, username, passwords etc.
Authentications failed [Phase 2 req]	The total number of consents requiring authentication where users have completed authentication, and authentication has failed (E.g. incorrect biometrics, username, passwords etc. used), or user consciously rejects authentication at any stage.	INT(10)	0-2147483647	Authentication should only be recorded as failed when the consent status is updated to 'Rejected'. For the avoidance of doubt, where a user abandons authentication without rejecting (E.g. they have left, or closed the web page or app, or allowed the confirmation page to time out), authentication should be recorded as 'Abandoned'.
Authentications abandoned by PSU [Phase 2 req]	The total number of PSU consents that required authentication that have been abandoned by the PSUs at any point after they have attempted authentication.	INT(10)	0-2147483647	For the avoidance of doubt, this means that PSUs: a) Attempted, but did not successfully complete authentication, and instead dropped the journey (they left, closed the web page or app or allowed the authentication page to time out), or... b) Successfully authenticated but dropped the journey at subsequent confirmation steps (they left, closed the web page or app or allowed the confirmation page to time out).

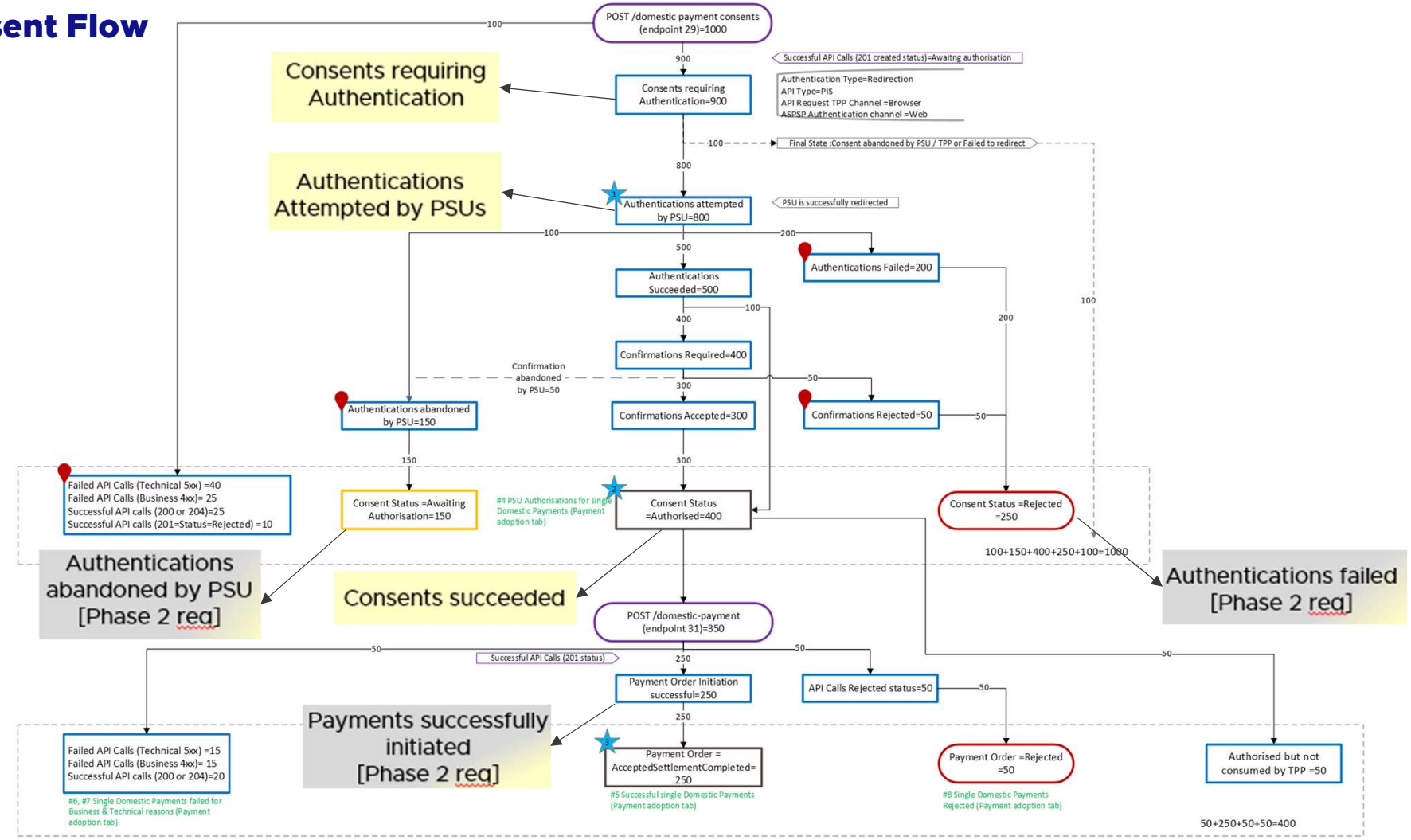
Return 3 – Authentication Efficacy (cont.)

Field Name	Description	Data Type	Data Format/ Constraints	Additional Information
Consents succeeded	The total number of consents requiring authentication that have completed authentication (and if required, confirmation steps) successfully by PSUs.	INT(10)	0-2147483647	Authentication where the consent status is 'Authorised'.
Payments successfully initiated [Phase 2 req.]	The number of 'PIS-Other' consents where the authorisation token is subsequently consumed and the POST - payment order initiation is successful.	INT(10)	0-2147483647	Should be reported for PIS-Other consents only.

Additional data validations

1) Authentications Attempted by PSUs <= Consents requiring authentication
2) Authentications failed <= Authentications Attempted by PSUs
3) Authentications abandoned by PSU <= Authentications Attempted by PSUs
4) Consents succeeded <= Authentications Attempted by PSUs
5) Authentications failed + Authentications abandoned by PSU + Consents succeeded = Authentications Attempted by PSUs
6) Payments successfully initiated <= Consents succeeded

Typical Consent Flow



ASPSP Brand IDs

- OBL are currently investigating if it is possible to use data sources for ASPSP Brand ID.
- OBL will confirm the brand ID's to be used by each ASPSP ahead of first data collection.

OPEN BANKING

What we plan to do with the data

- In the first instance, provide analysis and report to JROC - we assume this may drive discussions if underperformance relative to peers is evident.
- Data will be held securely and only accessible to a restricted list of OBL employees.
- As per the framework document, in terms of dissemination, to reflect the objective of “levelling up”, once OBL is comfortable with the quality of data being provided (and the accuracy of our analysis of it!) we will seek to supplement the existing public reporting of CMA9 MI with non-CMA9 ASPSP data.
- Generally, public reporting of CMA9 MI is aggregated and anonymised with a few exceptions.
- The publicly available CMA9 reporting can be found at https://www.openbanking.org.uk/api-performance/.