SLA Framework for AA Ecosystem

Driven by discussions and decisions in the Economic Model Committee, FIP and AA Councils facilitated by Sahamati.

August 26, 2026

Disclaimer

Nothing stated herein should be construed as legal advice in any manner. The views expressed in this document are based on outcomes of discussions conducted with stakeholders in relevant committee(s), user council(s) and/or working group(s) anchored by Sahamati and do not affect the requirements of any applicable provisions of law or the rules, regulations, guidelines, or circulars administered by the Reserve Bank of India, Securities and Exchange Board of India or any other relevant regulator or statutory body.

You are advised to seek an independent legal opinion on the applicability of any applicable laws and/or regulations relevant to your specific circumstances.

Table of Contents

1. Purpose of the Document..... 3
2. Introduction: Need for common definitions and SLAs for the AA ecosystem.....3
3. Common Definitions..... 3
4. SLA Framework Design and Measurement Approach..... 5
5. FIP Service Level Agreements.....6
5.1. Service Area-Level Reporting:..... 6
5.2. Service (API)-Level Enforcement:..... 6
5.3. FIP System Uptime:..... 7
5.4. Transparency Reporting / FIP Self-Declaration Dashboard:..... 7
6. AA Service Level Agreements.....8
7. FIU Service Level Agreements..... 9
8. Annexure:..... 11
Response codes used in the SLA framework.....11

1. Purpose of the Document

This document lays out a comprehensive SLA framework for all participants in the Account Aggregator (AA) ecosystem, namely Financial Information Providers (FIPs), Account Aggregators (AAs), and Financial Information Users (FIUs). The purpose is to establish a shared, measurable, and enforceable understanding of service quality expectations across the ecosystem. This is essential to enable:

- Set common and transparent expectations of technical performance across all ecosystem participants
- Credible, scalable, and trusted customer experiences
- Consistent measurement and performance benchmarking
- Support a strong rationale for the Data Fetch fee for FIPs under the upcoming economic model

This document is structured into three core sections:

- **FIP SLAs** – Expectations from data providers
- **AA SLAs** – Expectations from the Account Aggregators
- **FIU SLAs** – Expectations from data users

This document does not override or recommend any modification to the ReBIT technical specifications. All strategies and policies outlined herein must remain fully consistent with ReBIT's published standards, including but not limited to those on idempotency, deduplication, and API behaviour. This document does not authorise or require any change to API contracts or technical implementations in any form. Its sole purpose is to define service performance expectations and provide a framework for uniform measurement and governance across ecosystem participants.

2. Introduction: Need for common definitions and SLAs for the AA ecosystem

The Account Aggregator ecosystem hinges on the reliability of machine-to-machine APIs that deliver financial data based on customer consent. However, the absence of a unified SLA framework means that:

- Trust erodes: The system becomes fragile when there is no accountability or transparency into service performance.
- Disputes become inevitable: FIUs, AAs, and FIPs cannot agree on what constitutes a "failure."
- Billing becomes less reliable: Without common definitions of success, payments to FIPs cannot be fairly computed.

As the ecosystem matures, we aspire to move toward **perfect service**. However, we must begin with **minimum guarantees**. This framework establishes the foundation by defining shared terms, metrics, and thresholds for all ecosystem participants.

3. Common Definitions

The following definitions apply uniformly across this SLA framework and serve as the foundational references for implementation, monitoring, dispute resolution, and continuous improvement.

3.1. "**Business Declines**" for an API refers to a request or callback that fails with **4xx error code**, and

includes the scenarios described in Appendix 8.1. These are counted as Service Success for SLA purposes, but classified as Business Declines for pricing calculations.

3.2. "**Consent Use Counter"** is a numeric measure maintained by the participants that tracks the number of successful data fetches performed under a specific consent. Each increment corresponds to a Successful Data Fetch, as defined in this document.

3.3. "**Declared Business Hours**" are defined as 24 hours minus declared routine nightly downtime and declared scheduled maintenance.

3.4. "**Error Rate**" for an API refers to the percentage of responses that do not result in Service Success.

3.5. "**Service-API**" refers to an API offered by an ecosystem participant to provide a Service within their Service Area, in the AA ecosystem, and includes related functions (such as a notification) implemented by any AA ecosystem participant.

3.6. "**Service Area**" refers to one or more Service-APIs offered and managed by a participant (AA, FIP, or FIU) that directly impacts customer interactions, account handling, consent management, or data delivery.

3.7. "**Service Success**" for APIs refers to a **request / call-back request not failing.** It implies the APIs met their intended functionality and includes the following:

3.7.1. Where the HTTP response code is 200, AND the response payload is valid and usable - there is no "bad payload", e.g., if there is gibberish in the response, although the HTTP status code says 200, the service is considered "down".

3.7.2. Where the HTTP response code is 4xx[1], implying there is an error on the API client side. e.g., invalid parameters, FI/request for unliked account, etc. HTTP response code 429 (rate-limiting) is treated as a service-level error (issue) if it exceeds the accepted error rate threshold.

3.7.3. Where the callback payload indicates an "FI Status" other than "Timeout" (Relevant for FIP callbacks to AAs and AA callbacks to FIUs)

3.8. "**Successful Data Fetch**" for the purpose of consent use refers to a data pull from an FIP in which the AA receives a valid and final response from the FI/Fetch API corresponding to a given consentId and sessionId. Only such successful outcomes shall be counted toward the Consent Use Counter.

While the Consent Use Counter does not monitor the quality of data delivered, FIPs are expected to ensure that all data delivered meets the following standards:

3.8.1. The data shared should be accurate, updated, and complete as per the consent artefact.[2]

3.8.2. The data must conform to the latest ReBIT FI Schema.

3.8.3. The data, including narration and other details, must align with standard bank statement formats issued through other channels.

3.8.4. All mandatory and optional fields as required by ReBIT must be provided with accurate information.

3.9. "**Technical Declines**" for APIs refer to a **request/call-back failing with a 5xx error code (server-side failure)**, and include the scenarios described in Appendix 8.1. These are considered failures for both API technical success and pricing calculations.

---

[1] Annexure 8.1 illustrates response codes to various technical and business declines.

[2] Section 8(3) of the DPDP Act obligates Data fiduciaries to ensure that data provided by them is accurate, complete and consistent, where:
1. the personal data processed by a fiduciary is likely to be used to make a decision that affects the data principal; OR
2. disclosed to another data fiduciary

4. SLA Framework Design and Measurement Approach

This SLA framework sets the performance standard for the entire Account Aggregator ecosystem by formally classifying all API interactions into customer-critical **Service Areas**. The Service Areas represent structured milestones within the customer journey and are rooted in practical implementation realities across all AA participants.

Each participant's SLAs are designed to **measure performance at the Service API level**, where technical granularity is highest. Still, they are intended to be **reported and governed at the Service Area level**, where outcomes align with end-user expectations. This layered approach enables operational accuracy while maintaining ease of understanding for governance, compliance, and business stakeholders.

This approach is also aligned with how **ReBIT classifies the APIs** in the technical specifications (version 2.1.0), providing common ground for both compliance and implementation.

Three Service Areas - The individual services are clubbed in 3 broad buckets based on a logical grouping of services that collectively support key customer journeys: account handling, consent management, and data flow Management, as follows:

4.1. **Account Handling** - Covers the customer's ability to discover, link, verify, and delink accounts within the AA system. Failures here prevent customers from proceeding at all.

- POST /Accounts/discover
- POST /Accounts/link,
- POST /Accounts/link/verify,
- POST /Accounts/delink,
- POST /Account/link/Notification

4.2. **Consent Management -** covers the creation, notification, and tracking of consent artefacts. Reliable Consent Management is essential for transparency, auditability, and compliance.

- POST/Consent,
- POST/Consent/fetch,
- POST/Consent/handle,
- POST/Consent/Notification

4.3. **Data Flow Management** - Involves the actual flow of financial data between FIPs, AAs, and FIUs. Failures here directly affect the fulfilment of the end use case and the perceived value of the AA framework.

- POST/FI/request
- POST/FI/fetch
- POST/FI/Notification

Each API is measured individually for accuracy and accountability. However, all reporting, benchmarking, and SLA reviews shall be conducted at the service area level, as described above. This ensures that monitoring reflects complete user journeys while retaining the precision of individual API-level metrics. The service area-level performance of a participant is thus calculated by aggregating the relevant API metrics under each service area.

The following sections define the SLA obligations and success metrics for each participant type: FIPs, AAs, and FIUs.

5. FIP Service Level Agreements

FIPs play a foundational role in the AA ecosystem by responding to valid consent-artefacts presented to them in a secure and reliable manner. As such, the SLA expectations for FIPs are geared towards ensuring consistent availability, speed, and correctness of data provisioning.

5.1. Service Area-Level Reporting:

FIP performance is reported in terms of overall success rate and responsiveness within each of the three critical service areas. Each area contributes equally to the overall SLA score, with weights subject to revision as the ecosystem matures.

Service Area	Success Rate	Weightage	Success Rate % of calls
1. Account Handling	Account Handling Success Rate = Discovery × Link Initiation × Link Verification Success Rates	33.34%	>88.00%
2. Consent Management	Consent Management Success Rate = Consent API × Consent Notification API Success Rates	33.33%	>99.50%
3. Data Flow Management*	Data Management Success Rate = Request Success × Data Ready Notification Rate[3] × Fetch Success Rate	33.33%	>95.00%
Combined Success Rate	Weighted 1+2+3	100.00%	>94.10%

** Conditions for data delivery -*

- *The data shared should be **accurate, updated and complete** as per the consent artefact.[4]*
- *Data must conform to the **latest ReBIT FI Schema**.*
- *The **data, narration and other details** match the standard bank statement formats issued through other modes.*
- *Accurate information on all fields is provided for **mandatory and optional fields** as required by ReBIT*

5.2. Service (API)-Level Enforcement:

While reporting is done at the service area level, SLA enforcement happens at the API level, where precision and accountability are highest. This ensures that each technical interface exposed by FIPs meets minimum performance guarantees in terms of:

- **Service Success Rate**: % of API calls that are fulfilled successfully
- **Error Response Rate**: % of API calls resulting in technical decline
- **Response Time**: Time taken to respond, measured at P95 and P100 percentiles

Together, these API-level thresholds define the minimum service performance required for each FIP to be considered SLA-compliant.

[3] Data Ready Notification = POST /FI/Notification (to AA) for every valid session ID
[4] Section 8(3) of the DPDP Act obligates Data fiduciaries to ensure that data provided by them is accurate, complete and consistent, where:
1. the personal data processed by a fiduciary is likely to be used to make a decision that affects the data principal; OR
2. disclosed to another data fiduciary

Service Area	Service APIs	Service Success Rate %	Error Response Rate %	Response Rate (P95)	Response Rate (P100)
Account Handling	POST /Accounts/discover	>90%	<10%	<5 seconds	<10 seconds
	POST /Accounts/link	>99%	<1%	<500 ms	<750 ms
	POST /Accounts/delink	>99%	<1%	<500 ms	<750 ms
	POST /Accounts/link/verify	>99%	<1%	<500 ms	<750 ms
Consent Handling	POST /Consent/Notification	>99.75%	<0.25%	<500 ms	<750 ms
	POST /Consent	>99.75%	<0.25%	<500 ms	<750 ms
Data Delivery	POST /FI/request	>98.5%	<1.5%	<500 ms	<750 ms
	POST /FI/Notification (to AA)[5]	>98.5%	<1.5%	<30 s data range 1yr (per account)	<60 s data range 1 yr (per account)
	POST /FI/Fetch/ API	>98.5%	<1.5%	<50 ms per KB	<100 ms per KB
Heartbeat	GET /Heartbeat[6]	>99.5%	<0.5%	<500 ms	<750 ms

5.3. FIP System Uptime:

FIP system availability is critical to maintaining reliability across the AA ecosystem. The minimum SLA for system uptime is 99.5%, measured over a quarterly period, which translates to a maximum allowable downtime of 10h 52m 2.2s per quarter. System Downtime is classified into three categories:

5.3.1. Routine Settlement / End-of-Day Downtime (declared in Transparency Dashboard as given in 5.4),

5.3.2. Scheduled Maintenance Downtime (declared in advance with at least two days' notice), and

5.3.3. Unplanned Downtime (exceptional and not declared in advance).

Uptime SLA calculations exclude declared nightly downtime and scheduled maintenance; all unplanned downtime counts toward SLA performance and must be immediately communicated to the ecosystem by FIPs. Uptime is calculated as:

Uptime (%) = (Declared Business Hours−Unplanned Downtime) / Declared Business Hours * 100

5.4. Transparency Reporting / FIP Self-Declaration Dashboard:

To promote ecosystem-wide trust and accountability, each FIP is required to publish and regularly update a Transparency Dashboard. This dashboard acts as a structured self-declaration mechanism, offering critical insights into system behaviours that directly affect downstream participants (AAs and FIUs). The declarations will keep the ecosystem informed of any specific FIP-level limitations and also serve as a tracker to gradually shift the participation towards the default response as expected at an ecosystem level. The declarations must cover the operational characteristics as listed below:

[5] Callback response time is calculated from the time of the FI/Request response received from FIP to the FI/Notification callback notification sent by the FIP.

[6] Heartbeat API thresholds are revised from >95% to >99.5% in with System Uptime SLAs

FIP Transparency Dashboard				
I	II	III	IV	V
Sl. No.	Declaration Item	Expected response	Declaration	Declaration (where relevant)
1	Rate Limitation Applied?	No	Yes/No	Per API
				Per AA
				Per Customer
				Per financial account, or such other metric
2	Limitations on data packets delivered?	No	Yes/No	Max size (KB/MB)
				Max transactions per packet
				Max period per packet (e.g., 3M)
				Any other limitations
3	Does the data shared correspond to most recent data available in FIP records?	Yes	Yes/No	Data typically updated up to: _____ (e.g., T-1, T-2)
4	Is there any lag in handling data during Nightly Downtime/Settlement/Holidays?	No	Yes/No	Max allowable lag: _____ days
5	Does a nightly Routine Downtime window exist where FIP systems are not available?	No	Yes/No	Window (e.g., 2AM–4AM IST): _____
6	Does a regular Scheduled Maintenance downtime window exist where FIP systems are not available?	No	Yes/No	Please share if known in advance, or give notice of the same two days in advance of the scheduled downtime
7	Is there a data field restriction or deviations from ReBIT FI Schema?	No	Yes/No	*[Please list fields & reasons]*
8	Is the Narration available in line with official account records or customer-facing statements outside of AA?	Yes	Yes/No	If it deviates, please explain the nature and rationale
9	Do you have any deviations from the ReBIT API specifications?	No	Yes/No	If it deviates, please explain the nature and rationale
10	Do you have any additional validation requirements for identifiers other than mobile number during Account Discovery?	No	Yes/No	If identifiers are other than Mobile Number, please declare
11	Are the fair use rules implemented?	Optional	Yes/No	If yes, please share the restrictions

6. AA Service Level Agreements

Similar to the FIP's SLAs, AA SLAs are also split into 2 parts: Service Area SLAs and Service API SLAs.

6.1. **Service Area-Level Reporting:** AA performance is reported in terms of overall success rate and responsiveness within each of the three critical service areas:

Service Area	API Group (hosted by AA)	Target Success Rate	Response Time (P95)
Account Handling	POST /Account/link/Notification	>99.5%	< 500 ms
Consent Management	POST/Consent x POST /Consent/Notification	>99.0%	< 500 ms (in total)
Data Management	POST /FI/request x POST/FI/fetch x POST /FI/Notification	>98.5%	< 500 ms (for FI/Fetch)

6.2. **Service (API)-Level Enforcement:** Each API's performance is measured in terms of Success rate, Error response and Response rate:

Service Area	Service APIs (hosted by AA)	Service Success Rate %	Error Response Rate %	Response Rate (P95)	Response Rate (P100)
Account Discovery	POST /Account/link/Notification	>99.5%	<0.5%	<500 ms	<750 ms
Consent Management	POST /Consent	>99.5%	<0.5%	<500 ms	<750 ms
Consent Management	POST /Consent/handle	>99.5%	<0.5%	<500 ms	<750 ms
Consent Management	POST /Consent/fetch	>99.5%	<0.5%	<500 ms	<750 ms
Consent Management	POST /Consent/Notification	>99.5%	<0.5%	<500 ms	<750 ms
Data Management	POST /FI/request	>99.5%	<0.5%	<500 ms	<750 ms
Data Management	POST /FI/fetch	>99.5%	<0.5%	<50 ms/KB	<100 ms/KB
Data Management	POST /FI/Notification	>99.5%	<0.5%	<500 ms	<750 ms
Infrastructure	GET /Heartbeat	>99.5%	<0.5%	<500 ms	<750 ms

6.3. **Adherence to additional codes of conduct and guidelines:** As with FIPs, the above AAs' SLAs must also be accompanied by adherence to all jointly agreed standards and guidelines set out in the Sahamati Code of Conduct for Members.

7. FIU Service Level Agreements

FIUs have two primary responsibilities that are evaluated under the SLA framework: Consent Management and Data Management. Unlike AAs and FIPs, each of these service areas in the FIU context corresponds directly to a single API. Therefore, the Service Area SLAs and Service API SLAs are effectively the same but are presented separately below for consistency with the SLA framework structure.

7.1. Service Area-Level SLAs:

Service Area	Service API (hosted by FIU)	Service Success Rate %	Response Rate (P95)
Consent Management	POST /Consent/Notification	>99.5%	<500 ms
Data Management	POST /FI/Notification	>99.5%	<500 ms

7.2. Service APIs-Level SLAs:

Service Area	Service API (hosted by FIU)	Service Success Rate %	Error Response Rate %	Response Rate (P95)	Response Rate (P100)
Consent	POST /Consent/Notification	>99.5%	<0.5%	<500 ms	<750 ms

Management					
Data Management	POST /FI/Notification	>99.5%	<0.5%	<500 ms	<750

8. Annexure:

Response codes used in the SLA framework

The following list captures response codes used in the SLA framework for calculating service success and error rates. This list is not static - additional codes or clarifications may be elaborated from time to time based on ecosystem learnings and operational updates.

Response codes used in the calculation of Service Success Rates			
Status of Transaction	**Response Code**	**Response Description**	**Illustrations / Remarks**
Successful Transactions	200	OK	Response as per ReBIT specs
Business Decline	400	Invalid Request	AA sent an invalid request, or FIP could not validate the request
Business Decline	401	Unauthorized Access	Lack of valid authentication credentials for the AA to make the request
Business Decline	403	Forbidden Request	Lack of valid permissions for the AA to make the request
Business Decline	404	Account Not Found	FIP is unable to uniquely identify the customer
Business Decline	412	Pre-Condition Failed	When Consent parameters do not meet the Fair Use Rules
Business Decline	429	Too Many Requests	FIP is unable to process requests due to higher volumes (allowable only up to the error rate threshold)

Response Codes used in computation of Error Rates (declined transactions)			
Response	**Response Code**	**Response Description**	**Illustrations / Remarks**
Technical Decline	500	Internal Server Error	FIP's internal server is unavailable
Technical Decline	501	Not Implemented	Backward compatibility issue at FIP end.
Technical Decline	502	Bad Gateway	FIP Server does not send a response or sends null response
Technical Decline	503	Service Unavailable	FIP is unable to service the request for any reason
Technical Decline	504	Gateway Timeout	FIP Server does not send a response in time

****End of Document****