AA Uniform Code of Conduct

Community guidelines in the Sahamati AA Ecosystem

Driven by discussions and decisions in steering committees and working groups facilitated by Sahamati

August 31st, 2022

Revision History

Version	Date	Changes Made	Author of changes	References
Version 1.0	31st August, 2022	First release for the AA Community	Vamsi Madhav	NA

Purpose of this document

The AA Master Directions issued by RBI and Technical Specifications published by ReBIT provide an overarching framework to guide dos and don'ts of participants in the AA network.

There are however several questions that arise during implementation, which involve interpreting the above-mentioned high-level directions/specifications and crafting lower-level procedural decisions, that are understood and implemented uniformly by all AA participants.

Such "procedural decisions" (henceforth referred to as "guidelines") are the product of community-deliberations in one or more of the steering committee and/or working groups that Sahamati organises.

Each such guideline follows a lifecycle of passing through two stages, within the community forum that is discussing it:

- "Is Under deliberation"
- "Is Finalised"

Guidelines agreed to

All guidelines that reach a stage of agreement ("Is Finalised"), are expected to be adhered to, by all community members. Modifications to such guidelines, based on newer market feedback or regulatory guidance, is of course, to be handled from time to time.

Such guidelines usually would also make their way into checklists that guide implementations. Optionally, some of these guidelines may be incorporated in future versions of the AA Ecosystem Participation Terms.

However, the incorporation or otherwise, into checklists and the Participation Terms, has no bearing on the expectation of adherence. Once a guideline reaches a stage of agreement, it is expected to be adhered to, in good faith, by all community members.

Guidelines under deliberation

Guidelines that are still under deliberation, are also expected to be implemented in a spirit of consensus. In other words, the fact that a guideline is under deliberation implies that there is a need felt for a harmonious understanding and implementation of that aspect.

Market participants are expected to not proceed with divergent implementations, without submitting their views to the community forum. Market pressures should certainly motivate faster

consensus on such matters but not be reasons for divergent behaviour, as that may be detrimental to both citizens and ecosystem participants.

This document aims to provide a list and details of all guidelines (and their lifecycle stage) discussed thus far, across Sahamati Steering committees and working groups.

Enforcement of adherence to guidelines

Enforcement of adherence follows a three-step process:

- Clarity and explanation - through checklists and ecosystem participation terms
- Review of checklists and explanation of deviations - during onboarding assistance provided by Sahamati to every participant
- Transparency of information pertaining to adherence - through public dashboards available on the Sahamati website

Punitive measures to ensure enforcement of such guidelines are outside the scope of this document.

The overarching spirit of this document is to provide clarity to all participants on what convergent thinking on any subject is. Such clarity is expected to either foster healthy debate or adherence, amongst most participants. This document is intended to serve such an audience.

Summary of the Guidelines

As of this version, there are 120 guidelines grouped across 25 topics as listed below.

Topic	Guidelines Finalised	Guidelines under deliberation
Customer registration and de-registration	2	3
User Identification and Authentication	2	2
Account Discovery	4	5
Account Linking and Delinking	2	2
Consent Request Management	5	8
Data Request Management	1	3
Consent Lifecycle Management	1	2
Recurring Consents Management	0	4
Citizen as a Data Recipient	1	3
Unregulated Entities and their Roles	1	2
FIU Roles and Responsibilities	3	4
FIP Roles and Responsibilities	2	4
Technical Interoperability	3	0
Reciprocity Obligation	1	1
Central Registry and Token Issuance Service	4	0
Purpose Codes	0	5

LSP Implementation	3	0
AA Client Integration	6	5
AA Commercials	1	1
Participation Terms	5	1
Grievance and Dispute Resolution	3	1
SLAs	0	2
API Implementation Best Practices	2	1
Storage of Data	2	2
Certification Framework	4	1
TOTAL	**58**	**62**

Guidelines

Customer Registration and de-registration

Guideline No.	CR001
Purpose	To clarify AA's accountability towards customer authentication, while enabling a customer to register with it, i.e. get a VUA issued.
Description	Every AA must independently authenticate its customer, prior to issuing a VUA (Virtual User Address) to the customer.
Stage	Finalised

Guideline No.	CR002
Purpose	To clarify whether a customer must be allowed to de-register his/her AA profile
Description	Every AA must allow a customer to de-register his/her AA profile. The design of the de-register mechanism is left to each AA. Once de-registered, all active consents attached to that profile automatically get revoked and all accounts previously linked become de-linked.
Stage	Finalised

Guideline No.	CR003
Purpose	To clarify whether a legal entity (such as a company) can register with an AA and get a VUA
Description	A VUA is an identifier issued to the legal entity that owns financial accounts. In the case of a natural person, the VUA is issued to the person. In the case of a company, the VUA is issued to the company.

	For a company to register with an AA and get a VUA, the authorised representative of the company has to authenticate herself, as mentioned in CR001. The workflow needs to be detailed.
Stage	Under Deliberation

Guideline No.	CR004
Purpose	To clarify whether a customer may be issued more than one VUA by an AA
Description	It is left to each AA to determine this, after assessing the need for a citizen (whether corporate or individual) to have more than one VUA issued. Is there a need?
Stage	Under Deliberation

Guideline No.	CR005
Purpose	To clarify whether a customer may port her consent artefact (and related transaction logs) from one AA to another
Description	In the event a citizen decides to de-register her profile with one AA and use another, it should be possible for the citizen to port her consent artefacts (and related transaction logs) from one AA to another. This is currently being discussed within the AA community.
Stage	Under Deliberation

User Identification and Authentication

Guideline No.	UA001
Purpose	To clarify the user identifiers that an AA must support, for authentication during initial registration and subsequent access
Description	To authenticate a user during customer registration, an AA *must* support taking the: ● Mobile number as an identifier To authenticate a user during subsequent access (i.e. login), an AA *must* support taking either of the two below: ● Mobile number as an identifier ● VUA as an identifier In addition, an AA *may* support identification and authentication using ● Email address ● Aadhar number
Stage	Finalised

Guideline No.	UA002
Purpose	To clarify the duration for which an inactive user's session on an AA client remains valid, once a user is authenticated
Description	*As per OWASP best practices, once a user is authenticated by an AA, the session remains valid for a maximum duration of 30 minutes, in case of inactivity by the user.* *Is there a reason to either extend or reduce this duration?* *(This guideline is to particularly enable embedded AA interactions that involve repeated invocations of the AA client from within an FIU environment - e.g. in a loan journey, consent for loan origination is taken once and then separate consent for loan monitoring may need to be taken.)*
Stage	Under deliberation

Guideline No.	UA003
Purpose	To clarify if multi-factor authentication of a user is a MUST for authorization of sensitive actions in the AA domain
Description	*Currently, AAs do not employ multi-factor authentication for either registration, login, profile change or consent management actions.* *Should one or more of these actions be protected via multi-factor authentication? Alternatively, are there more sophisticated means of detecting identity fraud without necessarily resorting to MFA?*
Stage	Under deliberation

Guideline No.	UA004
Purpose	To clarify if KYC norms as prescribed by RBI for entities regulated by them have to be followed, while onboarding users onto AA platforms
Description	KYC Norms are applicable to regulated entities that deal with money flows. While AAs are licensed as a type of NBFCs, they are unique (as compared to all other types of NBFCs) in their role of providing only consent management and data-sharing capabilities to citizens, NOT movement of money or facilitation of transactions involving money transfer. As such, it is not required for AAs to follow KYC norms for customer registration, as applicable to other NBFCs/Regulated entities. However, as prescribed under ReBIT technical specifications, strong authentication is a must for AAs to onboard users. This implies the usage of at least one strong identifier (mobile, email) during registration. Such usage is both necessary and sufficient.
Stage	Finalised

Account Discovery

Guideline No.	AD001
Purpose	To clarify if auto-discovery, i.e. discovering a customer's accounts held across FIPs without the customer explicitly indicating which FIPs, is allowed or not
Description	*Auto-discovery enables convenience for customers and also functional benefits, particularly for purposes such as Wealth Management Service.* *However, it generates a lot of unnecessary traffic and puts stress on FIP systems, if used without guardrails.* *What should such guardrails be, if at all?*
Stage	Under deliberation

Guideline No.	AD002
Purpose	To clarify if discovery can be done on FIPs *specified* by the customer on the FIU interface, which is then subsequently passed to the AA via the FIU-AA integration rails
Description	AAs can execute discovery calls on specific FIPs, the IDs of which are passed by FIUs, via parameters passed during an integration between the FIU front-end and the AA client. This is to support customer journeys that originate on the FIU front-end and involve embedded AA interactions.
Stage	Finalised

Guideline No.	AD003
Purpose	To clarify if discovery can be done using an identifier that is different from what the user provided during registration with the AA
Description	A user may provide different identifier(s) (e.g. mobile number or email ID) for enabling discovery of accounts from one or more FIPs, than what was provided during registration.

	● The different identifier(s) provided must include atleast one strong identifier (i.e. mobile no or email ID) ● The AA must authenticate the new identifier as well, before sending the discovery request to the FIP
Stage	Finalised

Guideline No.	AD004
Purpose	To clarify what are considered "Strong Identifiers" for Discovery and whether additional identifying attributes can be added to these
Description	Strong identifiers are one of the following: ● Mobile Number ● Email ID Additional identifiers, such as Date of Birth, PAN - can be added, as required by each FIP. Such information is stored against each FIP's entry in the Central Registry. All additional identifiers are to be clubbed with the Strong Identifier value using an "AND" condition. However, are FIPs, AAs and the Registry capable of supporting the above?
Stage	Under Deliberation

Guideline No.	AD005
Purpose	To clarify if Aadhar Number is allowed as a Strong Identifier
Description	The ReBIT Technical Specification V 1.1.2 does list Aadhar Number as a Strong Identifier. However, there are UIDAI restrictions around exchange of Aadhaar numbers, as is, between two systems - in this case, between an AA and an FIP. Work is in progress to design mechanisms to use Aadhar, in consultation with UIDAI.

Stage	Under Deliberation

Guideline No.	AD006
Purpose	To clarify the scope of Account Types supported under the FI Type "Deposit" and the workflow required for expansion to joint accounts/corporate accounts
Description	As of now, the scope of Account Types includes: ● Savings and current accounts that are singly held by individuals (this includes current accounts held by sole proprietorships) The scope currently excludes: ● Accounts held jointly - regardless of the "mode of operation" ● NRE/NRO accounts ● Accounts held by companies other than those registered as a sole-proprietorship The workflow details for expansion of scope to the above types is under discussion, amongst RBI/ReBIT and industry participants.
Stage	Under Deliberation

Guideline No.	AD007
Purpose	To clarify if information about "discovered accounts" can be shared with FIUs
Description	No. The information provided by FIPs in response to a discovery request is meant to be stored only at the AA. Such information cannot be shared by the AA with an FIU. FIUs get information for accounts that are included by the citizen, in the consent artefact, while approving the FIUs' consent requests.
Stage	Finalised

Guideline No.	AD008

Purpose	To clarify if discovery of an account can be enabled by an FIP if the account status is NOT active
Description	If the status of an account is NOT active (i.e. it is either dormant or suspended or closed, e.g.), it is in the interest of the citizen for additional services (such as the sharing of account information) to NOT be authorised by the FIP. Hence, discovery of the same should also not be enabled. This needs to be discussed with FIPs once.
Stage	Under deliberation

Guideline No.	AD009
Purpose	To clarify if discovery of an account can be enabled by an FIP if the mobile number (as an identifier) does not resolve to a single customer record
Description	If a mobile number cannot be resolved to a single customer record, the FIP is expected to reject the "Discovery" request. Additional identifying attributes (such as DOB, e.g.) may be defined by the FIP and collected by the AA, to sharpen the query and resolve it to a single record.
Stage	Finalised

Account Linking and delinking

Guideline No.	AL001
Purpose	To clarify if the identifier used an FIP to authenticate and authorise account linking has to be the same as the identifier used by the FIP for discovery
Description	Discovery of an account, at an FIP, has to be on the basis of at least one STRONG identifier (mobile, email) AND one or more additional identifiers (DOB, PAN, etc.). Account linking has to be authorised by an FIP on the basis of the account owner getting authenticated through an identifier that the FIP's records have. Currently, the authentication is through a single-factor. For all practical purposes, an identifier used for enabling a discovery call will be the same as that used to authenticate and authorise a linking request. However, strictly speaking, it is not necessary for these to be the same. It is possible, e.g. for a discovery call to happen via an email ID seeded in the FIP's records while linking may be authorised via a mobile number seeded in the FIP's records. Further, if and when multi-factor authentication becomes necessary for authorising linking, additional identifiers will be sought during linking but not during discovery.
Stage	Finalised

Guideline No.	AL002
Purpose	To clarify if de-linking of an account also needs the FIP's authorization
Description	No authentication and authorization is needed to be performed by the FIP, when it receives a "Delink" instruction from the citizen via the citizen's AA.
Stage	Finalised

Guideline No.	AL003
Purpose	To clarify if linking of accounts can be authorised by an FIP if the account status is NOT active
Description	If the status of an account is NOT active (i.e. it is either dormant or suspended or closed, e.g.), it is in the interest of the citizen for additional services (such as the sharing of account information) to NOT be authorised by the FIP. Hence, linking of such an account should not be authorised. This needs to be discussed with FIPs once.
Stage	Under deliberation

Guideline No.	AL004
Purpose	To clarify if a citizen can de-link his/her account with an AA, via the FIP instead of doing this on the AA client interface
Description	A citizen should be able to instruct that his/her account be de-linked, through a channel offered by the FIP. In addition, if the customer's account with the FIP is CLOSED, the FIP may use the same channel to inform the AA. The AA is then expected to take appropriate action towards removing the linkage of the account with the AA profile. The tech rails for this have to be discussed between FIPs and AAs.
Stage	Under deliberation

Consent Request Management

Guideline No.	CR001
Purpose	To clarify the mechanics of an FIU placing a consent request for a citizen (natural person) that has not yet registered with an AA
Description	New-to-AA citizens will either choose an AA or be presented with a recommendation by an FIU. Once such a citizen chooses the AA he/she wishes to use, the FIU may send a consent request to that AA, using the "Mobile Number@AA_Identifier" in the "Customer Identifier" attribute of the consent request. This guideline is anchored on the principle that a citizen, wishing to use an AA service, is in possession of a mobile device and an active SIM card.
Stage	Finalised

Guideline No.	CR002
Purpose	To clarify the mechanics of an FIU placing a consent request for a corporate entity that has not yet registered with an AA
Description	In place of the mobile number as an identifier for the entity seeking the VUA, an alternative that works well for legal entities such as companies has to be determined. One can anchor this too on the principle that a corporate citizen, wishing to use an AA service, must be in possession of a PAN. The same attribute MUST then be part of the corporate citizen VUA issuance (registration) workflow of every AA. This is to be discussed further in the ecosystem.
Stage	Under deliberation

Guideline No.	CR003
Purpose	To clarify if a request can be placed for an irrevocable consent, by an FIU

Description	There is currently no scope for a consent artefact to be deemed "irrevocable". Consequently, there is no scope for a consent request to be placed, with the additional constraint that consent once given, should be irrevocable. It is understood that there may be adverse consequences in terms of service availability from an FIU, if the consent provided to that FIU is revoked. The same is expected to be dealt with separately between the FIU and the FIU's customer. All consent requests placed in the AA ecosystem are deemed revocable.
Stage	Finalised

Guideline No.	CR004
Purpose	To clarify what the max period of "data storage" is for an FIU and the difference between "Data Life" and "Data Storage"
Description	The consent request placed by an FIU includes a parameter called Data Life. This represents the period that the FIU may "process" the data, once consented to, by the citizen. This is however different from the "Data storage" policy that the FIU has. This policy stems from existing regulations and defines the maximum period that the FIU is expected to keep the data, to aid in any queries, grievances or disputes that may arise later, much beyond the period for which the data is being processed. The AA guidelines do not, in any manner, influence existing data storage policies.
Stage	Finalised

Guideline No.	CR005
Purpose	To clarify what "INF" stands for, in the parameters for Data Life and Frequency, in a consent request
Description	INF - is inferred to be short for "INFinite", or "Undefined". It is not good practice to use this for either of the two attributes - Data Life and or Frequency.

Stage	Under Deliberation

Guideline No.	CR006
Purpose	To clarify what "Consent Mode - Query" stands for and whether data-filter feature is implemented in the AA ecosystem
Description	The QUERY permission allows additional filtering criteria to be included in the consent artefact. This allows the FIP to preprocess the data before responding to the request. The QUERY filter parameters may be defined by the FIP. As of August 2022, this feature is not currently implemented in the AA ecosystem. However, this needs to be discussed further and implemented.
Stage	Under Deliberation

Guideline No.	CR007
Purpose	To clarify what "Consent Mode - Stream" stands for and whether data-filter feature is implemented in the AA ecosystem
Description	The STREAM permission facilitates in-point streaming of information to the FIU. As of August 2022, this feature is not currently implemented in the AA ecosystem. However, this needs to be discussed further and implemented.
Stage	Under Deliberation

Guideline No.	CR008
Purpose	To clarify means to resolve inconsistencies in ENUM values in the specification, e.g TERM-DEPOSIT or TERM_DEPOSIT
Description	A list of such inconsistencies and a decision as to which one to use has to be used. TERM-DEPOSIT (e.g.)

Stage	Under Deliberation

Guideline No.	CR009
Purpose	To clarify what the term "FI Data Range" represents, for a use case that needs a look-ahead data-fetch (i.e data fetches in the future)
Description	If the purpose of seeking consent is to process data for a time-period into the future (e.g. a personal finance use case), the FI Data Range represents the entire range of time for which data is expected to be fetched. E.g. If on August 1st 2022, the consent is being sought, for data to be fetched for 6 months prior and till 12 months into the future, the FI Data Range will be "From Jan 1st 2022" and "To July 31st 2023".
Stage	Finalised

Guideline No.	CR010
Purpose	To clarify how "Unit and Value" need to be interpreted, for Data Life and Frequency attributes
Description	A unit of "1" and Value of "Month" is to be interpreted as "Once a Month". A unit of "2" and Value of "Day" is to be interpreted as "Twice a day". The computation of time-units is to follow "Calendar" time, i.e. a day is to be deemed as starting 12 midnight, an hour is to be defined as per the system clock, a month is to be defined as per the system calendar. Thus, if "Twice an hour" is the frequency for which consent is provided at 10:30 AM, it implies "two times" in each hour, starting 10-11 AM, 11-12 Noon and so on. This interpretation is true for both Data Life and Frequency attributes.
Stage	Under Deliberation

Guideline No.	CR011
Purpose	To clarify if any consent request parameter can be modified by the citizen, on the AA interface, prior to approving the same
Description	Modifying one or more parameters in the consent request may adversely affect the ability of the citizen to avail herself of the financial service from the FIU. It is therefore best for the AA to enable a simple "Reject" option, which the citizen can exercise in case he/she does not agree to any parameter value in the consent request placed. The FIU is then expected to send a fresh, corrected consent request. The interaction between the FIU and the customer, to do so, is outside of the purview of the AA's role.
Stage	Finalised

Guideline No.	CR012
Purpose	To clarify the guideline for the maximum past duration for which transaction history is made available by FIPs
Description	FIPs are expected to provide the same duration of transaction history as is currently available to a citizen via other digital channels - such as net banking or mobile banking. In case different digital channels offer a different duration currently, the maximum available duration is to be taken as a benchmark for a citizen to avail of, via an AA as well. This is to be discussed within the community.
Stage	Under deliberation

Guideline No.	CR013
Purpose	To clarify norms for how consent request attributes should be presented on AA Client interfaces to citizens
Description	RBI Master Directions direct AAs as follows:

	6.5 At the time of obtaining consent, the Account Aggregator shall inform the customer of all necessary attributes to be contained in the consent artefact as per paragraph 6.3 above and the right of the customer to file complaints with relevant authorities in case of non-redressal of grievances. The "inform customer of all necessary attributes" is to be implemented on AA client (web app, mobile app, e.g.) screens in a manner which neither overwhelms the citizen nor makes it incomprehensible. The community has devised a draft set of norms which have to be Finalised.
Stage	Under deliberation

Data Request Management

Guideline No.	DR001
Purpose	To clarify what the session time-out values are, for session IDs issued by either AAs (to FIUs) or by FIPs (to AAs)
Description	Session IDs issued by AAs or FIPs have a time-out value. This value represents the maximum time that the AA or the FIP may take to service the data request received. 60 minutes is the value that AAs / FIPs are expected to configure as the session time-out value. This implies that FIUs or AAs may expect a notification pertaining to their data request anytime within a maximum of 60 min. If no notification is received within this period, it would essentially mean that the request has "Failed" and a fresh request needs to be initiated.
Stage	Under Deliberation

Guideline No.	DR002
Purpose	To clarify if retries are allowed by AAs (for FIUs) and by FIPs (for AAs) for failed sessions
Description	Once a citizen gives consent, he/she expects the participants to ensure that data is shared amongst them, as per the consent parameters. This implies that FIPs and AAs are expected, by the citizen, to take appropriate corrective measures, if there are technical reasons (and not business reasons) for a data request to be declined. Hence, FIPs and AAs are expected to enable AAs/FIUs (respectively) to "Retry" a data-request, if a previous one fails, i.e. the session state returned for that is "failed" or no notification is received within the session ID time-out value (as defined in DR001). The number of retries is expected to be capped to a number being discussed in the ecosystem.
Stage	Under Deliberation

Guideline No.	DR003
Purpose	To clarify the meanings and behaviours associated with session Status and FI Status values
Description	The meanings and behaviours of these two attributes - Session Status, FI Status - are as per the community guidelines documented here: https://github.com/Sahamati/certification-framework/blob/main/guidelines/session-id-and-fi-status-states.md
Stage	Finalised

Guideline No.	DR004
Purpose	To clarify if a "partial fetch" of data is allowed for an FIU, from an AA, in the event the citizen consents to provide data across multiple accounts, either from one FIP or multiple FIPs
Description	There are financial use cases that offer value to a citizen, even with data partially available, in the event there are technical or business declines for some of the data that the citizen has consented to give. AAs and consequently FIPs have to honour delivery of such "partially" available data. The mechanics of "partial data delivery" have to be first implemented by FIPs and then by AAs. This is currently under discussion.
Stage	Under Deliberation

Consent Lifecycle Management

Guideline No.	CL001
Purpose	To clarify if a citizen can *initiate* the process of revoking a consent via an FIU or an FIP channel, instead of the AA interface

Description	A citizen should be able to initiate his/her intent to revoke a consent on an FIU or an FIP channel. Such a channel may be designed as per the FIU's or FIP's preference.
	
	 The intent, once registered, should result in the customer
	
	     a. either being re-directed digitally to the AA that the citizen has used previously, for the citizen to complete the process of revocation
	
	     b. Or alternatively, being provided information as to how the citizen can independently invoke the AA's interface and complete the process of revocation.
	
	 It is strongly recommended that FIUs and FIPs implement point a, to enable ease for citizens.

Stage	Finalised

Guideline No.	CL002
Purpose	To clarify if a citizen can *fulfil* the process of revoking a consent via an FIU or an FIP channel, instead of the AA interface
Description	A citizen should be able to fulfil his/her intent to revoke a consent via an FIU or an FIP interface. The FIU or FIP ought to use APIs to notify the citizen's AA of the same. If the request comes via an FIU, the AA is expected to immediately consider the consent revoked. No additional confirmation is required from the citizen directly. If the request comes via an FIP, the AA is expected to notify the citizen and design a mechanism for the citizen to explicitly confirm. The distinction is being made on the following logic:

	When the party seeking data seeks to restrict further access to data, the same must be honoured immediately, in the interest of data privacy. When the custodian of the citizen's account conveys a restriction (via a revocation), the citizen's explicit confirmation is required to ensure he/she is not inconvenienced owing to an inadvertent action on the part of the FIP.
Stage	Under deliberation

Guideline No.	CL003
Purpose	To clarify if pause/resume of consents is a necessary feature for an AA to provide to a citizen
Description	While the RBI Master Directions mention these as abilities that an AA ought to enable for citizens, it is understood that these are left to the AA to determine.
Stage	Under deliberation

Recurring Consents Management

Guideline No.	RC001
Purpose	To clarify if the type "INF" can be used as a parameter to denote "undefined / adhoc / infinite" frequency, while seeking recurrent consent
Description	While INF is provided for as one of the valid values, and it is inferred to be short for "INFinite", it is considered to be NOT a good practice to use this, to denote recurring consent frequency. This would effectively imply no limit on the frequency of pulls and is not useful from the perspective of citizens' privacy. It is advised therefore that only one of the other values for frequency - which denote a specific recurrence pattern - be used and not INF.
Stage	Under Deliberation

Guideline No.	RC002
Purpose	To clarify if different consent parameters (such as frequency, date range) can be applied to different financial information types, using a single consent
Description	The current specifications (V 1.1.2) do not allow for consent parameters to be different for each FI type sought in the consent request, by the FIU. Hence, if an FIU seeks three FI types (e.g. deposit, insurance, MF), the consent parameters have to be designed such that they apply for all FI types. It is understood that this may not work for use cases where recurrence may be required at a higher frequency for one FI type (e.g. deposit) but not for the other (e.g. insurance). This needs to be discussed within the community to evolve a change request.
Stage	Under Deliberation

Guideline No.	RC003
Purpose	To clarify if consent can be taken for an indefinite/long period (e.g. multiple years) if the financial service tenure is similarly indefinite or long (e.g. PFM or loan monitoring purposes)
Description	From the citizens' perspective, protecting the citizen against inadvertent sharing of the citizens' data is primary. In the case of a recurring consent with a long-term validity, the risk of the user "forgetting" that such consent has been given has to be factored in as a problem to be solved. As a basic guideline, it is advised that consent validity durations be restricted to 1-2 years, with the understanding that citizens may be able to "extend" the same periodically. The mechanics of this are currently being discussed in the community.
Stage	Under Deliberation

Guideline No.	RC004
Purpose	To clarify if there are maximum limits defined for consent frequency
Description	It is necessary to ensure that a key requirement of data privacy is kept in mind, during implementations ● Collection limitation - FIUs ought to collect only as much data (history, frequency, data types - all included) as is necessary for the financial service being offered to the citizen. One way of enforcing this is to define guidelines for maximum frequency limits, for typical use cases. This is under discussion in the community.
Stage	Under Deliberation

Citizen as a data recipient

Guideline No.	CDR001
Purpose	To clarify if a citizen can be a recipient of his/her own data via an AA
Description	As per the RBI Master Directions, an AA's charter is to enable (amongst other things) presentation of a citizen's data to herself. Given that an AA is data-blind, this implies that an AA service can deliver encrypted data to the device owned by a citizen. Further, to enable presentation of data received by the device, an AA client (front-end application) that is resident on the device of the citizen (such as a mobile app) may offer the feature of decrypting and presenting data. Under no circumstances is the decrypted data allowed to be stored on the servers of the AA, since that is in contravention to the principle of the AA being data-blind.
Stage	Finalised

Guideline No.	CDR002
Purpose	To clarify if the citizen's access to her own data also is based on the structure of an electronic consent artefact
Description	All sharing of data via an FIP's service is to be done on the basis of an electronic consent artefact, regardless of whether the recipient of data is an FIU (a registered/regulated entity) or the citizen herself. Hence, an AA must generate an electronic consent artefact even if the recipient of the data is the citizen herself and share the same with the citizen's FIP. When the recipient is an FIU, a copy of the consent artefact is also shared with the FIU. When the recipient is the citizen herself, it is left to the AA to determine if the citizen (i.e. the device owned by the citizen) gets a copy of the artefact approved by her or not.

	This is to be discussed within the community.
Stage	Under deliberation

Guideline No.	CDR003
Purpose	To clarify if a citizen may share her data with any other party, on her own through an AA's mobile app installed on her device
Description	An AA's mobile app may decrypt data, once data has been delivered by the AA service to the device of the citizen. Such decrypted data may be presented to the citizen on the AA's mobile app. It may also be shared by the citizen with any party of the citizen's choice using commonly accepted digital methods - such as via email, whatsapp or any other sharing service that the citizen prefers. This feature is akin to what may be available to a citizen through the citizen's own banking application, e.g. This is to be discussed within the community.
Stage	Under deliberation

Guideline No.	CDR004
Purpose	To clarify if a citizen may share her data with any other party, on her own, through an AA-owned library embedded within the third-party app.
Description	In addition to the guideline described in CDR003 (which applies to even this scenario), an AA must also ensure its fiduciary duty towards the citizen is met, if and when the AA partners with a third-party to offer a deeply-embedded journey. Given that the charter of the AA is to enable either FIUs or the citizen's device to be the destination of the citizen's data, AAs are expected to serve only FIUs or the citizens with data-sharing capabilities. If an AA partners with an entity that is not an FIU (i.e. is not a registered and regulated entity) and enables convenience-mechanisms for citizens to share their data with such entities, does the AA have a fiduciary duty of ensuring safe-handling of data by such entities?

	Can the AA discharge such a duty, even if it has one?
	This is to be discussed within the community.
Stage	Under deliberation

Unregulated entities and their roles

Guideline No.	UR001
Purpose	To clarify the roles that an unregulated entity can play in the AA ecosystem
Description	Entities that are not "registered and regulated" by one of the four financial sector regulators CANNOT be FIUs (as per RBI Master Directions) themselves. Such an entity however, can provide one or more of the following services to AA network participants (FIUs, FIPs, AAs): ● Technology services - such as offering ready-implementations of API specifications, data analytics and user experience middleware, certification services. ● Commercial services - such as being a reseller for an AA, offering reconciliation, billing and settlement services to AAs, FIUs, FIPs, e.g. ● Lead generation services - such as providing a marketplace for FIUs and enabling AA front-end integration on behalf of FIUs ● AA registration services - such as facilitating AA registrations (issuance of AA handles) via marketing partnerships and technical integrations with AAs, with AAs strictly in charge of authenticating and authorising citizens themselves before issuing handles
Stage	Finalised

Guideline No.	UR002
Purpose	To clarify if unregulated entities can access the raw data of citizens, in any of the roles mentioned and guard rails thereof
Description	Technology Service providers that offer data gateway and/or data processing services to FIUs are expected to get access to the raw data that citizens share with the FIUs. FIUs are expected to take explicit, informed consent from citizens for

	them to share raw data with such data processors. This is in addition to the consent that the citizen gives to the FIU, via an AA, and is expected to be taken by the FIU separately. Further, FIUs are expected to ensure all such outsourcing arrangements are in line with extant regulatory norms they are subject to. Also, FIUs are expected to ensure that their data processors are legally bound to: ● Delete all raw data, once the processing is done for the FIU ● Not share the raw data or the insights therefore with any entity other than the FIU ● Not store or use the raw data or insights therefore for its own purpose *Should a TSP offering just data gateway services (and not data processing) also be named by the FIU to the citizen and explicit, informed consent taken?*
Stage	Under deliberation

Guideline No.	UR003
Purpose	To clarify if a lead generator's brand name can be displayed along with the FIU's name, to provide context to the citizen on consent artefacts
Description	A citizen may engage with an unregulated entity - such as a marketplace for financial services or a parent company's app - for a financial service. During the course of the interaction, the citizen may provide consent to an FIU - that the unregulated entity serves. In such a situation, it would be useful for the citizen to see both the name of the FIU (to whom the consent is provided) and the unregulated entity (*through* whom the consent has been provided) on the AA's interface. The current version of the specifications do not provide for a separate field, other than FIU. This has to be discussed within the community as to how to be resolved.
Stage	Under deliberation

FIU roles and responsibilities

Guideline No.	FUR001
Purpose	To clarify the definition of FIUs
Description	As per RBI Master Directions, only entities that are both "Registered with and regulated by" one of the four financial sector regulators (RBI, SEBI, IRDAI, PFRDA) are eligible to be an FIU. Conversely, entities that do not carry a certificate of registration from any of the four financial sector regulators cannot participate as an FIU. Further, it is implicitly understood that the use case/purpose that an FIU is seeking to process the citizen's data for, is permitted as per the licence charter of the FIU. It is the FIU's responsibility to assure itself and the rest of the ecosystem of the permissibility of its use case/purpose.
Stage	Finalised

Guideline No.	FUR002
Purpose	To clarify the fiduciary obligation of an FIU
Description	The term "fiduciary obligation", in the context of an AA, implies that an FIU has an obligation to prudently take care of the data principal's data (the "asset") and establish a relationship of trust. This also means that the FIU has an obligation to not profit from its fiduciary duty, without knowledge and consent of the data principal. The direct implication of this, on an FIU's behaviour, is: ● To use the citizen's data strictly in accordance with the consent artefact, provided by the citizen through an AA ● To ensure that the citizen's data is NOT employed for any other purpose, unless with the explicit knowledge and informed consent of the citizen. Such consent has to be taken in addition, if required,

	to what the citizen has provided for, through the AA. The key question to be deliberated by the community: The FIU may not have a fiduciary relationship with a citizen, for the regular business that it is chartered to perform. E.g. an insurance web aggregator does not have a fiduciary relationship with an insured party, while an insurance broker has. Both however can be FIUs since they are registered with a regulator. Can an insurance web aggregator seek consent from citizens to procure data and discharge its fiduciary obligation towards safe-guarding data, although the larger context of what it offers citizens (a portal to discover offers) is not on the basis of a fiduciary relationship?
Stage	Under deliberation

Guideline No.	FUR003
Purpose	To clarify if an FIU may have multiple entries in the central registry
Description	An FIU may have multiple deployments of its FIU gateway, either to serve different departments within its FIU or as a technical redundancy measure. Each such gateway may have its own public IP, public keys. In the current version of the central registry and token service, each such gateway will have its own entry, with its own unique FIU ID.
Stage	Finalised

Guideline No.	FUR004
Purpose	To clarify if a holding company that is not a registered and regulated entity itself can be considered an FIU
Description	Only entities that are directly "Registered with and regulated by" a financial sector regulator can be considered an FIU. Any other entity, including parent/holding companies of such an entity are

	not considered an FIU.
Stage	Finalised

Guideline No.	FUR005
Purpose	To clarify if an FIU is obligated to integrate itself with all licensed AAs or not
Description	Citizens should be free to choose which AA they set up a profile with. Once the choice is made, all FIUs ought to respect that choice and redirect their consent requests to the citizen's AA. This implies two principles to guide FIU user journeys: ● If a citizen is new-to-AA, i.e. does not declare h/she already has an AA profile, the FIU is free to recommend an AA that the citizen may register with. ● If the citizen however indicates that h/she already has an AA profile, FIUs are obliged, as per community norms, to respect that choice and redirect the citizen to that AA. It is further therefore necessary that FIUs find out if citizens already have an AA profile or not, to enable implementation of the above principles. This is being discussed in the AA community.
Stage	Under deliberation

Guideline No.	FUR006
Purpose	To clarify if FIUs can "discover" which AA a citizen already has a profile with, in order to direct citizens by default to their AA
Description	AAs may offer a standard API that allows FIUs to verify if a citizen (identified through the mobile number) is already registered with them or not. This would enable FIUs to avoid asking the citizen to recollect his/her VUA or worse, enforce citizens re-registering with a different AA altogether. This is currently being discussed within the AA community.

Stage	Under deliberation

Guideline No.	FUR007
Purpose	To clarify if AA handles issued by AAs can include the brand-name of an FIU or not
Description	FIUs play an important role in terms of encouraging citizens (their customers) to use AA. FIUs also partner with one or more preferred AAs, for new customer registrations, initiated in the course of their own digital journeys. FIUs may be interested in ensuring AA handles issued, post-registration, include the brand name of the FIU. This serves as encouragement to FIUs to further use the "AA Handle" as a marketing tool to nudge further usage, within their own products and services. This needs to be discussed further within the AA community.
Stage	Under deliberation

FIP roles and responsibilities

Guideline No.	FPR001
Purpose	To clarify if an FIP can define the combination of identifiers it deems as "unique" for enabling identification of customers
Description	Each FIP can define the combination of identifiers it deems fit for it to uniquely identify an account owner and enable discovery of accounts. This definition is then expected to be made available to all AAs, so that they may collect the necessary attributes on their interface while enabling discovery and linking. Such information is made available through a central registry.
Stage	Finalised

Guideline No.	FPR002
Purpose	To clarify if it is obligatory for a financial institution to be an FIP
Description	Each financial institution is free to determine if it wishes to participate in the AA Network or not. If it does choose to join the network, a community-designed implicit obligation of "Reciprocity" applies to such an institution. Further details are provided under the "Reciprocity" topic. Such an obligation makes it necessary for a financial institution to agree to be an FIP, if it wishes to join as an FIU.
Stage	Finalised

Guideline No.	FPR003
Purpose	To clarify if it is obligatory for an FIP to enable sharing of all data-types applicable to it, as per technical specifications
Description	An FIP is free to determine which FI Types it wishes to enable when via its FIP service.

	However, a community-designed minimum viable FI types, for each type of FIP, is being discussed. This is necessary for ensuring citizens derive real benefit from this network. E.g. an FIP of type bank is expected to join the network with a minimum of "single-owned current and savings accounts", including accounts owned by a sole-proprietor.
Stage	Under deliberation

Guideline No.	FPR004
Purpose	To clarify FIP types as per SEBI guidelines
Description	As per SEBI guidelines: ● Depositories (NSDL, CDSL) are FIPs. Depository participants are not FIPs. ● AMCs (through their RTAs) are FIPs. This implies AMCs are FIPs but the RTAs will provide the technical capabilities (that of an FIP gateway). This needs to be confirmed through discussions with the AMCs.
Stage	Under deliberation

Guideline No.	FPR005
Purpose	To clarify FIP types as per PFRDA guidelines
Description	As per PFRDA guidelines (generic, not specific to the AA ecosystem): ● CRAs (Central record keeping agencies - Protean, KFin) are FIPs. The pension funds themselves are not. This needs to be confirmed through discussions with the regulator and the CRAs.
Stage	Under deliberation

Guideline No.	FPR006
Purpose	To clarify FI types and account types for GSTN FIP
Description	The proposal tabled is for the following: Account type: GSTIN FI Types: GSTR 1, GSTR 3B The confirmation of the same and the FI schemas pertaining to each of the FI types is awaited from GSTN.
Stage	Under deliberation

Technical Interoperability

Guideline No.	TI001
Purpose	To clarify the definition of technical interoperability
Description	Technical interoperability refers to the ability of every AA participant (FIUs, FIPs and AAs) interacting with another, using a standard technical protocol. The open API specifications, published by ReBIT, complemented by community guidelines, provide a standard technical protocol. Interactions in the AA network are designed as bilateral communications between an FIU and an AA or between an FIP and an AA. As per current specifications (V 1.1.2), there are no direct interactions between an FIU and an FIP. Technical interoperability refers, therefore, to the ability of every FIU interacting with every AA using the same, common, standard technical protocol. Likewise, it also refers to the ability of every FIP interacting with every AA using the same, common, standard technical protocol
Stage	Finalised

Guideline No.	TI002
Purpose	To clarify if technical interoperability implies "AAs" sharing information amongst each other
Description	Technical interoperability does not imply AAs sharing information with each other. Each AA operates as an independent entity, performing the business it is licensed to. Citizens have a choice of which AAs they would like to use. Citizens are free to choose one or more such AAs. Consents (and associated data flows) managed via one AA are not shared by that AA with other AAs.

Stage	Finalised

Guideline No.	TI003
Purpose	To clarify if technology service providers offering gateway capabilities guarantee interoperability or not
Description	Any technology service provider claiming to have an implementation of the open API specifications of the AA network (as published by ReBIT) is _guaranteed to offer interoperability_ - to the AA participant it serves, be it an FIU, FIP or an AA itself. AA participants need NOT engage with multiple technology service providers in order to have the ability to engage with multiple AAs. However, AA participants are free to engage with multiple technology service providers for other reasons - such as for design of redundancy, better service levels, and the like.
Stage	Finalised

Reciprocity Obligation

Guideline No.	R001
Purpose	To clarify the definition of "Reciprocity"
Description	The term "Reciprocity" refers to an implicit obligation of a financial services institution to play two roles, in the AA network - that of an FIP and that of an FIU. Discharging this implicit obligation implies that every financial services institution wishing to join the AA ecosystem as an FIU (a "user" of information) also agrees to be an FIP (a "provider" of information). The principle of reciprocity being an obligation is to ensure citizens are benefited as also to ensure the usage of the AA network by participants is fair and equitable. Such an obligation can however only be practically implemented, if a financial institution is the custodian of one or more of the financial information types listed as part of the open API specifications (published by ReBIT). In the absence of the FIP service being practically implementable, a financial institution may still participate as an FIU, with a clear commitment to implementing its FIP service as and when applicable. Such a commitment is codified explicitly in the AA Ecosystem Participation Terms, a legally enforceable digital commons meant to standardise behavioural expectations amongst participants.
Stage	Finalised

Guideline No.	R002
Purpose	To clarify recommendations for FI types that are applicable to NBFCs, Depository Participants, RIAs and other currently-FIU-only participants
Description	Registered and regulated entities such as NBFCs, Depository Participants (stock brokers), Registered Investment Advisors (RIAs), Insurance Brokers and the like are custodians of information collected or generated during customer interactions on their systems.

	Such information could also fall under the purview of "financial information" that a citizen may wish to share, with other financial institutions. Recommendations for FI types applicable to each such entity type are currently under discussions within the AA community.
Stage	Under deliberation

Central Registry and Token Issuance

Guideline No.	CR001
Purpose	To clarify the purpose of the Central Registry Service
Description	To enable seamless technical interoperability between AA participants, automated discovery of each other's "addresses" on the network is a must. The Central Registry is a list of the public IPs published by each network participant, stored securely, in a highly-available environment. It offers an API to other enlisted AA participants (only), for them to pull the public IPs (and other metadata) of participants they have to connect to. In addition to public IPs of each participant, the Central Registry also stores and provides the public key (used for validating digital signatures) and other metadata (e.g. Customer Identifier types, Financial information types - supported by FIPs) that are necessary for AAs/FIUs/FIPs to have access to. The Central Registry is a Digital Common, i.e. it is not proprietary to any entity in the network nor to Sahamati. Sahamati however takes responsibility for hosting the registry in a secure, highly-available environment.
Stage	Finalised

Guideline No.	CR002
Purpose	To clarify the purpose of the Token Issuance Feature
Description	An adjunct to the Central Registry Service is a Token Issuance Feature. The open API specifications published by ReBIT mandate that API call authorization is done on the basis of callers being authenticated via API tokens presented by them. Such API tokens ought to be issued and validated using a standard protocol to ensure authentication and authorization mechanisms are uniformly applied amongst all participants in the AA network. The AA community has therefore devised the following mechanisms:

	● A shared, standardised token issuance service that all participants can use to procure standard, short-lived API tokens ● A common authorization logic that all participants implement within their systems to verify if API tokens are valid. The Token Issuance feature, as the name suggests, only issues short-lived API tokens to API callers. It does not validate tokens and as such, is not used by API providers for authorising API calls.
Stage	Finalised

Guideline No.	CR003
Purpose	To clarify if the Central Registry is a "Switch" that mediates every transaction in the AA network or not
Description	The Central Registry is NOT a switch. AA participants call the Central Registry API on a periodic basis - typically, once a day - to cache the information of the registry locally. No API call in the network goes via the Central Registry. Likewise, the Token Issuance Feature (API) is called by AA participants, once in 24 hours. The short-lived, 24 hour token is then used by AA participants as part of their API headers. API calls between AA participants are exchanged without an interaction with the Token Issuance service.
Stage	Finalised

Guideline No.	CR004
Purpose	To clarify the prerequisites for participants to be listed in the Central Registry and for them to use the APIs
Description	The Central Registry (and Token Service) offers two environments: ● A UAT environment - which is open to all participants (and technology service providers) looking to test their systems before

	going-live in the AA network
	● A Production environment - which is restricted to only entities authorised as per RBI Master Directions, to be FIUs, AAs or FIPs

For an entity to be listed in the Central Registry, it needs to furnish a copy of the Certificate of Registration (CoR) issued to it, by any of the four financial sector regulators (RBI, SEBI, IRDAI, PFRDA).

In addition, a checklist of implementation best practices (technical, legal) devised by the community are verified to ensure adherence to the same, to prevent grievances by citizens or disputes within participants post go-live.

Non-compliances with the checklist are recommended to be resolved before an entity participates at scale in the ecosystem. |
| Stage | Finalised |

Purpose Codes

Guideline No.	PC001
Purpose	To clarify the mapping between FIU use cases and the purpose codes to be used, for each "Type" of use case
Description	As of V 1.1.2 of the specification, there are 5 purpose codes defined in the specification. The mapping between these and "types" of use cases is as follows: 101 - Wealth Management - to be used by SEBI RIAs and Stock Brokers (and similar licensees) seeking consent for data that enables them to facilitate investment transactions, either on a one-time or recurring basis 102 - Customer spending patterns, budget or other reportings - to be used by SEBI RIAs, PFRDA Retirement Advisors (and similar licensees) seeking consent for data that enables financial advisory use cases, typically on a recurring basis 103 - Aggregated Statement - to be used by lenders, insurers, insurance brokers (and similar licensees) seeking consent for data that enables underwriting and/or verification of income, typically one-time 104 - Explicit consent for monitoring of the accounts - to be used by lenders (and similar licensees) seeking consent for data enabling continuous monitoring of accounts to assess repayment health, typically on a recurring basis 105 - Explicit one-time consent for accounts - to be used by stock brokers (and similar licensees) seeking consent for data enabling verifying the presence and activity of a financial account, while onboarding users or modifying user profiles, typically on a one-time basis Note: The above descriptions are indicative. If new use cases are discovered, the most appropriate purpose code is expected to be used, based on judgement and aligned with the descriptions above, to the best extent possible.
Stage	Under Deliberation

Guideline No.	PC002

Purpose	To clarify whether displaying the balance and transaction history of a single account is a valid use case under purpose code 102
Description	Purpose code 102 refers to "customer spending patterns, budget or other reportings" under the category "Personal Finance". The implicit expectation is that some degree of "analysis" on top of the raw data (i.e. balance, transactions) is being offered by an FIU. Therefore, a "use case" of just a display of the balance, profile and/or transaction history is not a valid implementation of this purpose code. However, an aggregation of balances across accounts (at a minimum), to provide a consolidated view across accounts is indeed a valid implementation. A drill-down feature, that allows the consolidated view to be broken into balance/profile/transaction histories of individual accounts, is a valid implementation.
Stage	Under deliberation

Guideline No.	PC003
Purpose	To clarify whether regular monitoring of accounts for purposes of a prospective financial service offer is a valid use case under purpose code 104
Description	Purpose code 104 refers to "explicit consent for monitoring of the accounts" under the category "Account query and monitoring". A "prospective" offer - refers to an offer to be made in the future. If a financial services institution wishes to seek citizen's consent for periodic monitoring of accounts, with the intent of profiling the financial position on a continuous basis and providing suitable financial offers in the future, the same may be done under this purpose code.
Stage	Under deliberation

Guideline No.	PC004
Purpose	To clarify if multiple financial services can be tied to one purpose and one consent artefact

Description	The intent behind the concept of "purpose-limitation" is to ensure that there is a one-to-one mapping between the citizen's understanding of the financial service h/she is interested in availing of, and the organisation's usage of the data shared. If a financial service involves the opening of multiple accounts as part of a single "Transaction" (e.g. often opening of a loan account also involves opening of a deposit account simultaneously), the "purpose" is deemed to be the same. In such a situation, the citizen is aware that the data shared will be used for opening of both accounts - since that is conjoined. However, the converse - where data is taking for one specific financial service but used, additionally or in its place, for another financial service that the citizen is not explicitly seeking - is not good practice.
Stage	Under deliberation

Guideline No.	PC005
Purpose	To clarify if the "purpose text" can be used by an FIU to provide specific, contextual information to the citizen, in place of the generic "purpose code" description provided for in the specifications
Description	The intent behind the design of the electronic consent artefact is to allow citizens to have clear and explicit knowledge of what their consent is being taken for. The purpose description (against each purpose code) mentioned in the specifications is meant to be an overarching guide as to what the code means. This is meant to enable FIUs to use the appropriate code in their consent requests. However, citizens would need specific, contextual information (such as a loan application number or a brand name of a financial product, e.g) as the real "purpose" for which they are being asked their date. The purpose text field can therefore be used by FIUs to provide such rich, contextual information subject to community-designed limits and guardrails (e.g. no PII to be shared, character limits to be enforced) Further, such information should NOT be part of the copy of the consent artefact sent by AAs to the citizen's FIPs. The FIP, is by design, as per current specifications, blind as to which FIU a

	citizen wishes to share her data with. Hence, context information input by the FIU in the consent request should not be visible to the FIP. AAs have to implement this in their design.
Stage	Under deliberation

LSP implementation

Guideline No.	LSP001
Purpose	To clarify if an LSP (Lending Service Provider) can be an FIU
Description	An LSP is an intermediary that partners with lenders. As such, an LSP need not itself be "a registered and regulated entity", with any of the four financial sector regulators. If an LSP is not a registered and regulated entity, it cannot be an FIU in the AA ecosystem.
Stage	Finalised

Guideline No.	LSP002
Purpose	To clarify the role an LSP plays vis-a-vis the AA ecosystem, as per the OCEN protocol
Description	An LSP plays a role akin to a marketplace. It allows borrowers to state loan requirements, view loan offers and complete the process thereafter to avail of the loan. As part of this journey, the front-end integration with an AA client - either via redirection, app-to-app integration or embedded library invocation - is the feature that the LSP may offer. This is just a digital workflow feature and does not involve the LSP receiving any financial information of the borrower. All interactions vis-a-vis the AA, from placing a consent request, to receiving the (approved) consent artefact and then receiving data, always happen directly between the lenders and the AA.
Stage	Finalised

Guideline No.	LSP003
Purpose	To clarify if a borrower can provide consent to multiple lenders (FIUs) in a single interaction on an AA client

Description	In an LSP-led digital journey, the borrower expects to get a choice of loan offers from several lenders that he/she chooses.
	In such an interaction, consent requests from all the lenders are simultaneously raised for the AA to present to the borrower. The AA presents all the consent requests in one single interaction with the borrower.
	The borrower may approve one, more or all of the consent requests presented, in a single interaction on the AA client.
Stage	Finalised

AA Client Integration

Guideline No.	AC001
Purpose	To clarify the definition of an "AA Client"
Description	ReBIT guidelines define an "AA Client" as possessing the following characteristics: ● An application that enables citizens to interact with the AA for the purposes of registration, account discovery and linking and consent management - thus implying that the "interface" (e.g. a screen) used by the citizen during the interaction is considered part of the AA Client. ● Available as either a web application or a mobile application or a library that can be embedded in other web or mobile applications (subject to constraints imposed by security concerns) ● Owned by an AA The term "library" is interchangeable with the term "SDK". Further, as mentioned in the first characteristic, the "library" (or "SDK") includes the customer-facing interface (such as a "Screen"). _A "set of APIs" or a "headless library" (i.e. without screens) does not qualify to be called an AA Client_. These are internal engineering assets of an AA, which may be provided to their partner FIUs on the basis of bilateral agreements, for the purpose of co-development of an AA client.
Stage	Finalised

Guideline No.	AC002
Purpose	To clarify ownership vs co-development aspects between an FIU and an AA, of an AA Client
Description	An AA Client is necessarily owned by an AA. However, the interfaces (e.g. screens) that are part of the AA Client design may be customised or co-designed by FIUs, in partnership with AAs, to suit their user interface and user experience requirements.

	The co-development scope may include any or all of the following: ● User interface redesign ● User experience (i.e. workflow or sequence of steps that a user experiences) redesign ● Development assistance, supporting the redesign efforts As long as the interaction is bound by common guidelines derived from Master Directions and/or technical specifications, FIUs and AAs are free to redesign AA Client interfaces as per their requirements. Such common guidelines are codified in a community-driven "Customer Experience Guidelines Checklist". Further, any redesigned interface screens are also "owned" by the AA, with respect to all aspects of development and devops. As part of a joint design and development effort with respect to the interface screens, AAs may provide access to internal APIs as they deem fit, while retaining complete control over all aspects of development, testing and distribution. FIUs and AAs are, however, free to enter into any bilateral legal agreements to restrict usage of such co-designed interfaces to named parties mutually agreed to.
Stage	Finalised

Guideline No.	AC003
Purpose	To clarify if a single AA library can connect to multiple AA services
Description	An AA library is a form of AA Client. An AA Client, as specified by ReBIT, is necessarily owned by an AA. While it is possible for one AA to partner with other AAs and provide an AA library that works with multiple AA services, it is not necessary for AAs to do so. Further, given that AA libraries have to be owned by AAs, a "super library" owned by a TSP in partnership with AAs is also not feasible. FIUs therefore, as of now, have to integrate AA libraries from different AAs, if they wish to connect to different AA services using the "library" mode of integration.

	One possibility is for AAs to come together to co-own a single library that connects to their services. This has to be further discussed within the community.
Stage	Under deliberation

Guideline No.	AC004
Purpose	To clarify the modes of integration available for an FIU to integrate its front-end application with that of an AA
Description	An FIU may integrate its front-end applications using any of the following modes: For web apps of an FIU: ● *Redirection* to a web application of an AA The redirection may result in the web application of the AA being rendered either standalone or as an iFrame, within the parent web application. For mobile apps of an FIU: ● *Redirection* to a web application of an AA ● *Invocation* of an embedded mobile library of an AA ● *App-to-app* integration, with an pre-installed mobile application of the AA on the same device Technical guidelines for *Redirection* have been Finalised within the community. Technical guidelines for *Invocation and app-to-app integration* are being discussed within the community.
Stage	Under deliberation

Guideline No.	AC005
Purpose	To clarify if an embedded Web Library is an acceptable form of an AA

	client
Description	Embedded Web libraries (e.g. those built using Javascript) pose a serious data privacy risk. Applications that embed such web libraries, in their web applications, are likely to gain control over data that flows to-and-fro between the library and the backend service. Such risks can be mitigated technically for mobile libraries (e.g. built using Android, iOS) embedded within host mobile applications. They cannot be mitigated for web libraries. It is therefore recommended that no AA offers an embedded web library to FIUs as an AA client.
Stage	Finalised

Guideline No.	AC006
Purpose	To clarify what "ownership" of an AA Client implies
Description	An AA Client is necessarily "owned" by an AA. This implies the following: For AA clients of type = web application: ● Ownership of the application code and its underlying infrastructure (including the environment the application is hosted on) has to reside with the AA For AA clients of type = mobile application OR mobile library: ● Ownership of the application code, distribution of the applications, ownership of the distributed app packages has to reside with the AA The accountability of all aspects pertaining to the AA client rests solely with the AA.
Stage	Finalised

Guideline No.	AC007
Purpose	To clarify what metadata, if any, can be communicated between an AA client and the FIU app
Description	The technical guidelines for *Redirection* and *Mobile library invocation/ app-to-app integration* provide clarity around what parameters can be passed back-and-forth between the FIU app and the AA client. In addition to parameters that help an AA authenticate the app user (e.g. mobile number) and the FIU determine user experience post-AA-interaction (e.g. whether the user approved a consent request or not), it may be useful for an FIU to determine the termination stage in a user's AA journey. This is useful for the FIU to provide appropriate support for repeat tries / grievance redressal to the citizen. In addition to such information pertinent to an individual citizen's AA journey, it would also be useful for the FIU to get anonymized, aggregated metadata about its customers' AA journey. Such metadata may include all information necessary for the FIU and the AA to jointly construct a "drop-off funnel" and use the same to improve user experience. The parameters that constitute such "metadata" - both for an individual citizen and at an aggregated, anonymized level - are being discussed within the community.
Stage	Under deliberation

Guideline No.	AC008
Purpose	To clarify branding guidelines for co-designed AA Client screens
Description	All AA Client screens that are co-designed with FIUs ought to include a "Powered by <AA Name>" in a clearly visible area of the screen. The AA Logo may be optionally added, next to the AA Name. The FIU name and logo may also be optionally added to such co-designed screens, to ensure there is contextual continuity to users while switching between the FIU and the AA interfaces.
Stage	Finalised

Guideline No.	AC009
Purpose	To clarify if the FIU name and logo can be displayed on AA Client screens in a *redirection* type of integration
Description	AA Client screens may, optionally, show the FIU name and/or logo, from-and-to which the citizen will be redirected. This is to enable contextual continuity to users while switching between the FIU and AA interfaces.
Stage	Finalised

Guideline No.	AC010
Purpose	To clarify if names of FIPs and logos are available for FIUs/AAs to display to citizens
Description	FIUs are encouraged to design user journeys in which citizens can verify if their data custodian (FIP) is already part of the AA network or not. In order to do so, FIUs may get FIP names via the Central Registry API. FIP logos are currently not part of the Central Registry. The same is being discussed currently.
Stage	Under deliberation

Guideline No.	AC011
Purpose	To clarify if constraints (such as "count of accounts") limiting the data to be collected, can be communicated by FIU through a redirection parameter
Description	The consent request attributes allow an FIU to specify which FI Types the FIU would like consent for. However, there are use cases where the FIU would like to state the "count of accounts" (e.g. "1 savings account only") that it wishes to seek consent for. The *redirection* and *invocation* guidelines may include this as an additional parameter. The same is being discussed within the community.
Stage	Under deliberation

AA Commercials

Guideline No.	AAC001
Purpose	To clarify if there is a "Standard" pricing model that all AAs are expected to follow
Description	The AA business model typically involves FIUs paying an AA, for the service of enabling delivery of citizen's consent-backed data. An AA may opt to also charge a citizen, for the service of being the consent manager of the citizen. As per RBI Master Directions: "Pricing of services will be in strict conformity with the internal guidelines adopted by the Account Aggregator which need to be transparent and available in public domain." However, there is no "Standard" monetary value or range of values that AAs are expected to follow. Pricing is a subject matter of negotiation amongst market participants.
Stage	Finalised

Guideline No.	AAC002
Purpose	To clarify if FIPs are compensated for the FIP service
Description	This is under discussion within the ecosystem.
Stage	Under deliberation

Participation Terms

Guideline No.	PT001
Purpose	To clarify the purpose of the AA Ecosystem Participation Terms
Description	The RBI Master Directions and open API specifications published by ReBIT provide an overarching techno-legal standard framework for the AA ecosystem. The Master Directions state that the interactions between the citizen, an account aggregator and an FIP must be backed by appropriate agreements. Further, the interactions between an FIU and an account aggregator also have to be backed by appropriate agreements. Legal agreements Implemented as a set of non-uniform, independent bilateral agreements between various parties would make dispute resolution a very inefficient purpose. The community has therefore evolved a uniform, standard set of terms and conditions, that are directly derived from the RBI Master Directions and bind all AA participants (FIPs, FIUs, AAs) and citizens into a common legally enforceable framework. This greatly simplifies the operational aspects of having appropriate legal agreements amongst parties and also makes dispute resolution efficient.
Stage	Finalised

Guideline No.	PT002
Purpose	To clarify if the Participation Terms are an "agreement with Sahamati"
Description	The Participation Terms are NOT a (bilateral) agreement between a single AA participant and Sahamati. They are akin to a multilateral treaty, between all the participants in the AA ecosystem. Each participant independently becomes a signatory to the treaty, rather than two (or more parties) jointly "signing" an agreement amongst themselves. Sahamati plays a role in the AA ecosystem and is obliged to adhere to a

	standard set of terms and conditions as well. These are codified in the Participation Terms, much like the terms and conditions binding AAs, FIPs and FIUs as well. Sahamati itself is also an independent signatory to the Participation Terms.
Stage	Finalised

Guideline No.	PT003
Purpose	To clarify if the Participation Terms are legally enforceable
Description	The Participation Terms are a legally enforceable document.
Stage	Finalised

Guideline No.	PT004
Purpose	To clarify if the Participation Terms are a "static" document or are subject to changes sought by independent signatories
Description	The Participation Terms are meant to enforce a standard, uniform set of terms and conditions. As such, at any point in time, unless all AA participants adhere to the same terms, the Participation Terms are ineffective. Hence, an independent signatory seeking customizations in the Participation Terms for itself, is not possible. However, the Participation Terms, unlike other Digital Commons, are a community-driven asset. Feedback from independent signatories may be collated periodically, discussed within the community and an update to the Terms released. This is akin to version upgrades in the open API specifications (or any other software asset), with a community-managed change management process. The change management process is being discussed within the community.
Stage	Under deliberation

Guideline No.	PT005
Purpose	To clarify if being a "member" of Sahamati is a prerequisite to being a signatory to the Participation Terms
Description	The Participation Terms are Digital Commons, part of a community-driven techno-legal stack of techno-legal assets meant to drive efficiency and scale in the AA ecosystem amongst FIPs, FIUs and AAs. "Membership of Sahamati" is meant to enable participation in the workings of Sahamati and to benefit from a set of services that Sahamati offers exclusively only to its members. An AA participant may become a signatory to the Terms without becoming a member of Sahamati. However, to become a member of Sahamati, becoming a signatory to the Participation Terms is a prerequisite. Thus, AA participants may join and leave membership of Sahamati, without it affecting them remaining as a signatory to the Participation Terms.
Stage	Finalised

Guideline No.	PT006
Purpose	To clarify if the Participation Terms also include "commercial" terms between AA participants
Description	The Participation Terms do NOT include any reference to commercials between AA participants. AA participants therefore have to enter into bilateral commercial agreements (such as between an FIU and an AA), based on negotiations amongst themselves.
Stage	Finalised

Grievance and Dispute Resolution

Guideline No.	GD001
Purpose	To clarify the definition of a "grievance" versus a "dispute" as defined in the AA community
Description	A grievance - is a query or a complaint raised by either the citizen or an AA participant, with any other AA participant. (The term "AA participant" refers to any of the three entities - AA, FIP, FIU). A dispute - exists when a claim based on a grievance is rejected either whole or in part. Disputes have to be resolved using any of the following methods - negotiation, mediation, conciliation, arbitration, litigation.
Stage	Finalised

Guideline No.	GD002
Purpose	To clarify who is responsible for "grievance redressal" in the AA ecosystem
Description	For grievances raised by citizens: As per RBI Master Directions, Account Aggregators must have a board-approved policy, a dedicated set up and an SLA of no more than a month for disposing of customer grievances. In addition, FIUs and FIPs may also have their own grievance redressal setup to handle AA-related grievances of their customers. Such a setup may involve integrating their systems with the grievance redressal system of an AA, to offer a unified response to the customer. For grievances raised by AA participants: The AA ecosystem is centred around all interactions in the ecosystem flowing through an AA, necessarily. Thus, an AA must have a set-up to redress grievances raised by an AA participant, even if redressing it involves interacting with other AA participants. In addition, AA participants may directly raise grievances with other AA participants.

	AA participants may also choose to use a Sahamati-hosted support system that allows collaboration amongst AA participants for speedy, effective resolution. If the response to a grievance is rejected either wholly or in part, the citizen or the AA participant may choose to either escalate the same to a regulatory grievance redressal scheme (such as the RBI Ombudsman scheme) or use alternative dispute resolution mechanisms, via an ODR (online Dispute Resolution) agency empaneled by Sahamati.
Stage	Finalised

Guideline No.	GD003
Purpose	To clarify the dispute resolution mechanisms available for a citizen or an AA participant
Description	If a grievance by a citizen or an AA participant escalates to it becoming a "dispute", one or both of the following resolution mechanisms are available: ● The aggrieved party may raise an issue with the RBI ombudsman (or any other ombudsman scheme set up by the regulator aligned to the aggrieved party's interests) ● The aggrieved party may use the services of an ODR agency empaneled by Sahamati, to utilise the agency's dispute resolution mechanisms - such as negotiation, mediation, conciliation or arbitration. ● The aggrieved party may use any other legal mechanism of its choice.
Stage	Finalised

Guideline No.	GD004
Purpose	To clarify the costs involved in grievance redressal and/or dispute resolution, if utilising Sahamati's services
Description	This is under discussion within the community.

Stage	Under deliberation

SLAs

Guideline No.	SL001
Purpose	To clarify if there are service level objectives defined for AA participants
Description	Service level objectives covering the following aspects have been drafted by the AA community and are being discussed: ● API health - uptime, response time, error rates ● Grievance redressal - first response time, resolution time ● Interoperability support - multi-AA integration As of now, these are still at draft stage.
Stage	Under deliberation

Guideline No.	SL002
Purpose	To clarify if FIU-AA commercial agreements include a reference to AA SLAs and penalties
Description	AA SLAs are based on FIPs committing SLAs to AAs. Since FIP SLAs are still at draft stage and being discussed within the community, FIU-AA agreements currently may not include any reference to AA SLAs and/or penalties.
Stage	Under deliberation

API Implementation Best Practices

Guideline No.	AI001
Purpose	To clarify implementation best practices regarding technical aspects of the API specification
Description	Implementation best practices are as defined in these community guidelines: https://github.com/Sahamati/certification-framework/blob/main/guidelines/general-guidelines.md
Stage	Finalised

Guideline No.	AI002
Purpose	To clarify the mechanism defined for API Governance (versioning and compatibility best practices)
Description	The open API specifications follow semantic versioning principles. Changes are expected to be introduced in a non-breaking manner, thus ensuring existing implementations are forward compatible, while newer implementations (that have implemented the latest version) are backward compatible. Only when unavoidable will there be a breaking change introduced, signalled through a major version change. Older versions will be sunset on the basis of a reasonable migration window provided to all implementers. All version changes and other aspects of API governance are currently controlled and published by ReBIT. These guidelines are informal interpretations of what is understood to be their policy.
Stage	Under deliberation

Guideline No.	AI003
Purpose	To clarify the version of the API specifications that the ecosystem is "live" on
Description	The version of the open API specifications (across FIP, FIU, AA APIs) that all entities are live on (as of August 2022) is V 1.1.2. While V 1.1.3 has been published by ReBIT, there are no API governance guidelines published and/or implemented by participants, that would ensure backward and forward compatibility amongst entities operating on two different versions. Hence, no entity is live on V 1.1.3. As newer versions get released, a discussion on API Governance principles and implementations needs to happen to ensure a smooth migration to newer versions takes place.
Stage	Finalised

Storage of data

Guideline No.	SD001
Purpose	To clarify the difference between "Data Life" and "Data Storage" for an FIU
Description	Data Life - as defined in the open API specification of the electronic consent artefact, refers to the time window declared by an FIU for "processing" or "using" the data shared by a citizen, for the purpose declared. E.g. a lender may declare a data life of 24 hours, to process the data shared by a borrower and underwrite the loan application. FIUs are expected to "delete" the data, after the Data Life time-window expires. However, the term "delete" is to be interpreted as a "Soft delete", since it cannot contravene existing regulatory directives regarding long-term archival of data collected by the FIU. Thus, an FIU is expected to continue adhering to existing regulatory norms with respect to "storage of data", where it is understood that such stored data is not meant to be "processed" or "used" in any manner, other than dictated by existing regulatory norms.
Stage	Finalised

Guideline No.	SD002
Purpose	To clarify if an AA stores financial data in its servers
Description	AAs may operate in a "Store-and-forward" mode, i.e. in order to serve a data fetch request from an FIU (or from the citizen herself), the AA may fetch data from an FIP, store in its servers and notify the FIU to pick such data up. All data stored on the AAs servers is encrypted by the FIP using the ECDH algorithm, using key material generated by the FIU. ThIs prevents the AA from being able to decrypt any data stored on its servers. Further, a maximum period of 6 hours has been codified as a best practice

	by the AA community, for any such store-and-forward mechanism employed by the AA. This implies that if an FIU is not able to pick the data up within 6 hours of the AA notifying it, the AA is expected to delete all data stored. Such a "Delete" is expected to be a hard-delete and not a "soft-delete", i.e. the data is not expected to be "archived" in a separate area by the AA. If the FIU picks the data up within 6 hours, the AA is expected to delete the data immediately after that.
Stage	Finalised

Guideline No.	SD003
Purpose	To clarify storage norms for data that an AA collects or generates (PII, consent artefacts, transaction logs)
Description	PII (Personally identifiable information) An AA does not perform KYC of citizens and as such, does not collect any KYC information - such as OVDs (officially valid documents), proving identity or address. An AA however collects and stores identifiers of its users - such as mobile numbers, email addresses, Date of birth, PAN - as mandated by FIPs to facilitate discovery and linking of FIP accounts. All such PII (Personally Identifiable Information) is expected to be stored securely (employing IT best practices for data-at-rest and data-in-transit) by the AA. If a citizen closes his/her profile with an AA, all PII is expected to be archived as per extant regulatory norms applicable to NBFCs, i.e. for a period of 6 years. Consent artefacts All consent artefacts generated on behalf of citizens by an AA are expected to be stored, beyond the expiry of the artefact, for a maximum period of 6 years, as per extant regulatory norms. This is to be discussed and Finalised within the AA community.

	Transaction logs All transaction logs spanning API interactions with FIUs and/or FIPs - and citizens' activity logs spanning registration, discovery, linking, consent management - are expected to be stored as per extant information security best practices. This is to be discussed and Finalised within the AA community.
Stage	Under deliberation

Guideline No.	SD004
Purpose	To clarify storage norms for FIPs and FIUs for data generated or collected by them
Description	FIPs and FIUs collect copies of consent artefacts and generate transaction logs of API activity. FIUs, in addition, generate activity logs on their front-end pertaining to integrations with AA clients. Consent artefacts All consent artefact copies received from AAs are expected to be stored, beyond the expiry of the artefact, for a maximum period of 6 years, as per extant regulatory norms. This is to be discussed and Finalised within the AA community. Transaction logs All transaction logs spanning API interactions with AAs are expected to be stored as per extant information security best practices. This is to be discussed and Finalised within the AA community. AA-integration activity logs All activity logs pertaining to citizens getting redirected to AA client interfaces have to be stored as per extant information security best practices. This has to be discussed and Finalised within the AA community.

Stage	Under deliberation

Certification Framework

Guideline No.	CF001
Purpose	To clarify the purpose of "Certification"
Description	"Certification" is essentially a technical guarantee of adherence to the open API specifications (published by ReBIT). The Certification framework comprises three community-defined elements: ● An open (i.e non-proprietary) suite of test cases, complementing the open API specifications - designed by the community ● A set of third-party certifiers, empaneled by Sahamati ● A set of rules governing the process of certification The benefit of being certified is that it provides a guarantee of "good behaviour" (technically) to other members of the community, thus generating trust amongst AA participants and citizens, reducing the count and cost of downstream errors and grievances. The open test cases of the certification framework, much like the Central Registry, Token Service and legal Participation Terms - form part of a stack of Digital Commons designed and driven by the community. They are not part of RBI Master Directions or ReBIT Technical Specifications.
Stage	Finalised

Guideline No.	CF002
Purpose	To clarify the frequency of re-certification required, if any
Description	The Certification Framework is based on a set of tests, which are aligned to a version of the open API specifications. The first version of the Certification framework is aligned to V 1.1.2 of the ReBIT open API specifications. Once certified for a particular version of the specifications, an entity need not be recertified so long as the entity is on the same version.

	However, a periodic self-assessment and submission of reports to a certifier is expected to be conducted on a quarterly basis. This is to ensure that inadvertent errors have not crept in, owing to changes introduced in the application, post-certification.
Stage	Finalised

Guideline No.	CF003
Purpose	To clarify the role of empaneled certifiers
Description	The scope of the first version of the Certification Framework is limited to verifying API implementations.

The role of the empaneled certifiers for this version, has been to devise test automation solutions that allow an entity to perform two activities:

    ● Get certified against the version of the specification the entity would like to go-live with
    ● Submit periodic self-assessment reports

These test automation solutions (also known as Certification Toolkits) are usually offered for a price.

AA participants may negotiate prices with the empaneled certifiers directly or via their TSP (Technology Service Provider) partners.

As the ecosystem grows, the scope and mechanics of the certification framework has to grow in two directions:

*reducing barriers of cost and complexity for API certification
*enhancing scope of certification to include data governance audits

In this context, the role of empaneled certifiers will also undergo a transformation. The same is currently being discussed within the AA community. |
| Stage | Under deliberation |

Guideline No.	CF004

Purpose	To clarify the role of TSPs in the certification process
Description	TSP (Technology Service Providers) may get their solutions pre-certified via any of the empaneled certifiers and acquire the status of an "Intermediate Certified Entity". Such TSPs may then negotiate with empaneled certifiers, as resellers, to onboard FIUs onto their systems and get the FIUs certified through a one-time re-run of their systems, for each FIU. The intent behind this is three-fold: ● To enable AA participants to deal with the TSP as their SPOC, for the entire AA implementation - and avoid the commercial and operational overheads of having to deal with the empaneled certifiers directly ● To encourage TSPs to become force-multipliers for the AA ecosystem, by enabling them to be the SPOC for all technical, legal and even commercial aspects ● To ensure the coverage of certification expands and is not limited to the reach of a small set of empaneled certifiers
Stage	Finalised

Guideline No.	CF005
Purpose	To clarify if a holding company can be certified on behalf of its subsidiary FIUs
Description	The intent of the certification framework is to ensure AA participants give the technical guarantee of their implementations adhering to the specifications. A holding company that is not an FIU, cannot provide this guarantee on behalf of other companies, even there is a shareholding relationship amongst them.
Stage	Finalised