Sahamati®

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

February 23rd, 2024

Disclaimer

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

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

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
Version 1.1	2nd December 2023	Update to PC004 and PC001	Geethashree Srikanta	NA
Version 1.2	23rd February 2024	Structural changes to the documents: removed guidelines tagged "Under Deliberation"	Geethashree Srikanta	NA
		Deprecated sections “Unregulated entities and their Roles” & “LSP Implementation.”		
		Reindexed Code Numbers for Topics - “Customer registration and de-registration, Central Registry and Token Issuance Service”		
		Updated to certain codes based on recent regulatory and policy changes - code nos. UA004 AD004, AD008, AL003, CR001, CR011, CR013, FUR001, FPR004, FPR005, FPR006, R001, PC001, AC007, AAC001, PT005, AI003		
		Added Code DR005		

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(s) and/or working group(s) that Sahamati organizes.

Once guidelines are published upon the conclusion of deliberations, they are expected to be adhered to by all other community members. Modifications to such guidelines, based on newer market feedback or regulatory guidance, are, of course, to be handled from time to time through further deliberations in the steering committee(s) and/or working group(s).

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 such adherence. Once a guideline reaches a stage of agreement in the relevant steering committee(s) and/or working group(s), it is expected to be adhered to, in good faith by all community members.

Market participants are expected by the community members 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 behavior, as that may be detrimental to both customers 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.

Online access to guidelines

These guidelines are also available on the Sahamati website at

https://sahamati.org.in/aa-uniform-code-of-conduct/

Summary of the Guidelines

As of this version, there are 61 guidelines grouped across 20 topics as listed below.

Topic	Guidelines Finalised
Customer registration and de-registration	2
User Identification and Authentication	1
Account Discovery	6
Account Linking and Delinking	3
Consent Request Management	5
Data Request Management	2
Consent Lifecycle Management	1
Customer as a Data Recipient	1
FIU Roles and Responsibilities	3
FIP Roles and Responsibilities	5
Technical Interoperability	3
Reciprocity Obligation	1
Central Registry and Token Issuance Service	4
Purpose Codes	2
AA Client Integration	7
Participation Terms	4
Grievance and Dispute Resolution	3
API Implementation Best Practices	2
Storage of Data	2
Certification Framework	4
TOTAL	**61**

Guidelines

Customer Registration and de-registration

Guideline No.	CG001
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.	CG002
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

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

Account Discovery

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, as per ReBIT Circular No. ReBIT/AA/2024-25/01 dated January 10, 2024. 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.
Stage	Finalised

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 customer 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 customer for additional services (such as the sharing of account information) to NOT be authorised by the FIP.

Stage	Finalised

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 by 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 customer via the customer'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 customer 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.
Stage	Finalised

Consent Request Management

Guideline No.	CR001
Purpose	To clarify the mechanics of an FIU placing a consent request for a customer (natural person) that has not yet registered with an AA
Description	New-to-AA customers will either choose an AA or be presented with a recommendation by an FIU. Once such a customer chooses the AA he/she wishes to use, the FIU may send a consent request to that AA, using the “Mobile Number” in the “Customer Identifier” attribute of the consent request, as per the version 2.0.0 of the NBFC-AA Specifications. This guideline is anchored on the principle that a customer, wishing to use an AA service, is in possession of a mobile device and an active SIM card.
Stage	Finalised

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 customer. 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 may 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 applicable data storage regulations.
Stage	Finalised

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 may 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 Feb 1st 2022” and “To July 31st 2023”.
Stage	Finalised

Guideline No.	CR013
Purpose	To clarify norms for how consent request attributes should be presented on AA Client interfaces to customers
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 customer nor makes it incomprehensible. The community has devised a set of norms as available here: https://github.com/Sahamati/customer-experience-guidelines/blob/main/consent-guidelines.md
Stage	Finalised

Data Request Management

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.	DR005
Purpose	To clarify if FIUs can repeat presenting a specific data **request** to depositories or RTAs, within a given calendar day, if the data against such a specific data request has already been received successfully.
Description	As per the ReBIT data schema for the FI Types made available by depositories and RTAs, such FIPs can only provide data (profile, summary, transactions) as of the previous day's closing. The data provided in each request will remain identical until the next day's closing, irrespective of the number of times a specific data request is submitted to these FIPs in the interim. For instance, where the data **request** for the same consent ID and the same FI Data Range is sent multiple times in a calendar day, all data **fetches** made during the calendar day (for the same consent ID but without the optional attribute of the link reference number), will yield the same information. In light of this, it is recommended that only one data request be made **once in a calendar day** for a given Consent Artefact and a given FI Data Range, provided data is successfully received against that request.
Stage	Finalised

Published Date	21/02/2024

Consent Lifecycle Management

Guideline No.	CL001
Purpose	To clarify if a customer can *initiate* the process of revoking a consent via an FIU or an FIP channel, instead of the AA interface
Description	A customer 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 customer has used previously, for the customer to complete the process of revocation b. Or alternatively, being provided information as to how the customer 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 customers.
Stage	Finalised

Customer as a data recipient

Guideline No.	CDR001
Purpose	To clarify if a customer 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 customer'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 customer. Further, to enable presentation of data received by the device, an AA client (front-end application) that is resident on the device of the customer (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

FIU roles and responsibilities

Guideline No.	FUR001
Purpose	To clarify the definition of FIUs
Description	As per RBI Master Directions, “Financial information user” means an entity registered with **and** regulated by any financial sector regulator. As per PFRDA’s Circular No.: PFRDA/2023/32/REG-POP/07 dated 22nd November 2023: “Financial information user (FIU) means an entity registered with and regulated by any financial sector regulator. Notwithstanding anything to the contrary mentioned above, it is expressly stated that the Point of Presence registered under Regulation 3(1)(i) and 3(1)(ii) of PFRDA (Point of Presence) Regulations, 2018, shall act as Financial Information User (FIU), while other intermediaries registered with PFRDA would not qualify to become FIU.”
Stage	Finalised
Published Date	21/02/2024

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

FIP roles and responsibilities

Guideline No.	FPR001
Purpose	To clarify if a 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.	FPR004
Purpose	To clarify FIP types as per SEBI guidelines
Description	As per SEBI Circular SEBI/HO/MRD/DCAP/P/CIR/2022/110 dated August

	19, 2022: ".....Depositories and AMCs (through their RTAs) are referred as FIPs in the securities markets" This also implies: ● Depository participants are not FIPs. ● While AMCs are the FIPs, the RTAs will provide the technical capabilities akin to that of an FIP gateway.
Stage	Finalised

Guideline No.	FPR005
Purpose	To clarify FIP types as per PFRDA guidelines
Description	As per PFRDA circular No: PFRDA/2022/26/FT&DA/02 dated 30th September 2022: "..... The CRAs appointed by PFRDA (are) designated as FIP." This implies that: ● The pension funds themselves are not FIPs.
Stage	Finalised

Guideline No.	FPR006
Purpose	To clarify FI types and account types for GSTN FIP
Description	This is specified in NBFC-AA Specification version 1.1.0 of the FI Type - Goods and Services Tax Return (GSTR), published at: https://specifications.rebit.org.in/api_schema/account_aggregator/documentation/gstr1_3b_v1.1.0.html
Stage	Finalised

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. Customers have a choice of which AAs they would like to use. Customers 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 the 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 customers 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. Further, this obligation is also codified in Clause 7.7 of the RBI’s Master Direction- Non-Banking Financial Company - Account Aggregator: “7.7 Joining the Account Aggregator Ecosystem as Financial Information User With a view to ensure efficient and optimum utilisation of the Account Aggregator ecosystem, regulated entities of the Reserve Bank joining the Account Aggregator ecosystem as Financial Information User shall necessarily join as Financial Information Provider also, if they hold the specified financial information and fall under the definition of Financial Information Provider.”
Stage	Finalised

Central Registry and Token Issuance

Guideline No.	CT001
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.	CT002
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.	CT003
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.	CT004
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 customers 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, (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	Finalised

Guideline No.	PC004
Purpose	To clarify if multiple financial services or processes can be tied to one purpose and one consent artefact
Description	The intent behind the concept of “purpose-limitation” is to ensure there is a one-to-one mapping between the customer’s understanding of the purpose for which the FIU is seeking the financial information and legal basis for the FIU to process such information. The purpose can be for a financial service and/or a process to avail a financial service. Financial services refer to loans, insurance, financial advisory etc, while processes include the process of loan underwriting, loan monitoring, assessing risk for advisory, etc. For instance, consider a financial service such as a loan. It involves two separate processes: a) one for assessing the customer's eligibility for the loan, and b) another for monitoring the repayment risk of the loan . Even though it’s the same financial service (the loan), there are two distinct purposes, and two data sets are required for the two different purposes – So, two different consents are needed. Accordingly, an FIU should not bundle two purposes into one consent request. 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 customer is aware that the data shared will be used for purposes that are intrinsically linked and –conjoined. However, the converse – where data is taken for one specific financial service or process but used, additionally or in its place, for another financial service or process, that the customer is not explicitly seeking – is not in compliance with applicable laws.
Stage	Final
Published Date	0/12/2023

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 customers 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 customer 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”, as available here: https://github.com/Sahamati/customer-experience-guidelines 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.	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 customer. In addition to such information pertinent to an individual customer'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" are as defined here: https://sahamati.gitbook.io/aa-redirection-guidelines/v/1.2.1/specification/response-specification
Stage	Finalised

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 customer will be redirected. This is to enable contextual continuity to users while switching between the FIU and AA interfaces.
Stage	Finalised

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 customer, 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 customers 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.	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 customer 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	<u>For grievances raised by customers:</u> 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. <u>For grievances raised by AA participants:</u> 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 customer 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 customer or an AA participant
Description	If a grievance by a customer 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

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.	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 customer, 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 customer 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. Thls 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

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 customers, 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.	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