Account Aggregator

Technical Standards

Banking Standard and Financial Specification

Sequence #: BFS-0006
Version: 1.2
Title: Account Aggregator Technical Standards

Author: ReBIT
Contact: sdo@rebit.org.in

Track: Standard
Maturity Level: Final Draft
Type: Technical Specifications
Status: Under Review

May 31, 2018

Abstract: This document describes the architecture for consented sharing of Financial Information between Account Aggregators, Financial Information Providers, Financial Information Users, and the customers themselves. It outlines the use cases that are enabled, the responsibilities of the various stakeholders and their interactions.

Forward

Dear Colleagues,

The Reserve Bank of India's "Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions" has created the mandate for creation of an ecosystem to enable consent based aggregation of financial information for the benefit of the consumers. We thankfully acknowledge the entrustment of the task of defining the technical standards to ReBIT by the Department of Non-Banking Regulation (DNBR). It goes without saying that well-defined standards, incorporating interoperability requirements, are important ingredients for a robust ecosystem and for providing opportunities of innovation. The technical standards for the Account Aggregator provide the requisite information to the Financial Information Providers (FIPs) and AAs within the Account Aggregator ecosystem, to implement a set of interoperable interfaces.

While the consent-driven approach empowers the end consumer, trustworthy cryptographic protocols protect the data from being accessed without explicit consent provided by the customer. ReBIT has put together the necessary standards documentation with the help of other stakeholders. Technology always evolves and specifications gets updated, and I am sure this technical standards will be no exception. The rightful owners of this specifications are the stakeholders for whom this specifications are defined and ReBIT sees itself in a role more as a facilitator of industry led standards development.

This project has benefitted from vital inputs from our industry peers. In particular, important contributions have been made by the iSpirt team. Additionally, the initial draft was reviewed by industry experts at Mindtree, Aujas Network and other AA ecosystem stakeholders. ReBIT's own Board Member, Shri Rajesh Doshi has provided guidance during the specification development process. We gratefully acknowledge their help and thank them for their valuable contributions.

Sincerely,

Nandkumar Saravade
CEO, ReBIT

Dated:

Version History

Version	Date	Comments
0.1	10/03/2018	Preliminary Draft
0.2	27/03/2018	Industry Consultation/Stakeholders Workshop
1.0	15/04/2018	Draft for Review in WG
1.1	25/05/2018	Redesign of interfaces for clarifying the AA and customer interactions. The AA client added in the architecture to clarify the customer interactions that happen with AA. Renamed User to “Customer” in the document to align with Master Direction.
1.2	31/05/2018	Section 1.4 removed Data Producer and Data Consumer definitions (included in API). Definitions reconciled with MD [1]. Section 1.6 references updated. Section 2.1 updated, AA client ownership clarified. FIU roles/responsibilities wordings updated. Section 2.2 updated with appropriate clarification based on WG deliberations. Updated section 2.4 on Electronic Consent based on WG feedback. Minor editing changes in the document.

Table of Content

1 Introduction

The Account Aggregator (AA) is a Non-Banking Financial Company, set up under the licensing terms of RBI specified in the Master Direction [1], to provide financial information aggregation services to Customers from one or more Financial Information Providers (FIPs) where their account(s) exist, based on the explicit Consent obtained from the Customer.

The different types of Financial Information (FI) applicable for such aggregation are described in [1]. The following table enumerates these financial information types and the corresponding Financial Information Type identifiers:

Table 1.1

#	Financial Information	Financial Information Type (FIType)
1	Demand deposits such as savings deposit accounts, current deposit accounts.	deposit
2	Term Deposits (NBFC, FD) - deposits including fixed deposit accounts. Certificates of Deposit (CD).	term_deposit
3	Recurring deposit accounts	recurring_deposit
4	Structured Investment Product (SIP)	sip
5	Commercial Paper (CP)	cp
6	Government Securities (Tradable)	govt_securities
7	Equity shares	equities
8	Bonds	bonds
9	Debentures	debentures
10	Mutual fund units	mutual_funds
11	Exchange Traded Funds	etf
12	Indian Depository Receipts	idr
13	CIS (Collective Investment Schemes) units	cis

14	Alternate Investment Funds (AIF) units	aif
15	Insurance Policies	insurance_policies
16	Balances under the National Pension System (NPS)	nps
17	Units of Infrastructure Investment Trusts	invit
18	Units of Real Estate Investment Trusts	reit
19	Any other information as may be specified by the Bank for the purposes of these directions, from time to time;	other

The financial information provided by the FIPs, as shown in Table 1.1 above, may be in varied different formats. A specific type of financial information is represented by the financial information type definitions (`FIType`). The architecture described in this standard is generic in nature and supports extension of the financial information that can be aggregated based on new financial information type definitions.

1.1 System Design Guidelines

The implementation guide adheres to the following guidelines:

- **Technology Agnostic**: The proposed design in the document is agnostic to applications, programming languages, and platforms and aims at seamless and secure flow of electronic data across different stakeholders.
- **Reliability and Scalability**: Non-repudiation, consent, digital signatures, logging requirements are used to bolster reliability and accountability of the ecosystem. Asynchronous mechanisms and callbacks are used to improve scalability of the system.
- **Privacy by Design**: Customer information needs to be protected from abuse and compromise. The AA implementation defines the data sharing mechanisms, based on Electronic Consent, gives the Customer control of their data and ensures privacy of Customer data ground-up and through generated non-repudiable audit trails.
- **Security by Design**: The software and systems must be designed from the ground up to be secure. There must be end-to-end security of data (PKI, Digital Signature Certificates [2], tamper detection) and it must be network agnostic and data centric.
- **Minimalist and Evolutionary Design**: The design should be simple and minimalistic. It should not present adoption barriers for the ecosystem. The

design of the systems should be evolutionary - their capabilities should be built incrementally while allowing for rapid adoption.
- **Customer Centric**: The Customer experience and ease of use are critical to successfully delivering the various services in the ecosystem. The design principles take into account the various stakeholder responsibilities and mechanisms to simplify interactions and minimise friction.
- **Consent Driven**: Mechanisms for dynamic discovery, empowerment of the Customer in accordance with the consent architecture proposed in the Master Direction [1] have been incorporated to enhance trust and ensure data privacy.
- **Open APIs for Interoperability and Layered Innovation**: People and systems should have programmatic interfaces for sharing and accessing the information available to them. The specification defines the standard APIs to promote interoperability and deliver services that are designed to work with any device, any form factor, and any network.
- **Ecosystem Driven Approach**: An ecosystem approach is necessitated such that the interfaces between the Financial Information Users (FIUs), Account Aggregators (AAs), and Financial Information Providers (FIPs) are well defined and standardized. Hence, there must exist a technology backbone that would hold together this ecosystem.
- **Transparency and Accountability through Data**: Public Open Data [8] shall be made available via APIs for transparency. The access to open data will ensure high-quality analytics, accurate fraud detection, shorter cycles for system improvement and, most importantly, high responsiveness to Customer’s needs.

1.2 Conventions used in the Document

- The key terminologies use `consolas` font type and dark cornflower blue 3 color encoding.
- The `lowerCamelCase` is used in attribute naming. For nouns, `UpperCamelCase` is used.
- The document uses XML to illustrate examples and structures of entities.

1.3 Scope of the Document

This document describes the architecture for the account aggregation ecosystem, the use cases that are enabled in the account aggregation ecosystem and the responsibilities of the various stakeholders, their interactions with other system stakeholders. It further provides examples of FI data schemas that may be queried from the FIP for the purpose of account aggregation.

In the current document, the FI data as applicable to Financial Information Type of “deposit”, “term_deposit”, “equity”, “bonds” and “mf” etc is described [see Table 1.1]. These `FITypes` are used to support multiple data formats of the Financial Information in the account aggregation ecosystem and thus support generic API usage mechanisms and extensions. The FI data format for Financial Information Types are described separately outside of this technical standards . New FITypes may be defined in future without impacting the overall design.

High level API definitions are provided in the Appendix [See 6.2] of the document. A more detailed and formal API specifications for the NBFC-AA ecosystem is described outside of this technical standards.

Technological underpinnings such as digital signatures, automated auditing, logging and non-repudiation concepts shall result in verifiability of transactions thus ensuring integrity of the relevant systems and supporting better grievance redressal.

1.4 Terms and Definitions

AA	Account Aggregator is an entity that acts as a consent collector for the Customer and mediates the Financial Information data flows from the FIP to the recipient FIU/Customer. The financial information pertaining to the customer shall not be the property of the Account Aggregator, and not be used in any other manner.
Consent Artefact	A consent artefact is a machine-readable electronic document that specifies the parameters and scope of data sharing that a Customer consents to in any data sharing transaction.
FI	Financial Information refers to information about a Customer's financial products such as Bank Deposits, Structured Investment Products (SIP), Mutual Fund Units, Equity Shares, Insurance Policies and other information as specified by the Bank. It is obtained from Financial Information Providers.
FIP	“Financial Information Provider” means bank, banking company, non-banking financial company, asset management company, depository, depository participant, insurance company, insurance repository, pension fund and such other entity as may be identified by RBI for the purposes of these directions, from time to time Examples of FIPs under different regulators: PFRDA ● Central Record Keeping Agency (CRA) RBI ● Banks ● NBFCs IRDA

	● Insurance Companies ● Insurance Repositories ○ CDSL Insurance Repository Limited (CDSL IR) ○ Karvy Insurance repository Limited ○ National Insurance-policy Repository by NSDL Database Management Limited ○ CAMS Insurance Repository Services Limited, SEBI ● Depository ○ NSDL and CDSL have information of shares, Bonds, Gsec and other such securities such as certificate of deposit, Commercial papers etc. held by investors in dematerialised form ● Stock Exchange ● Issuers and Issuances ● RTAs (Registrar and Transfer Agents) ● Mutual fund holding and transactions information ○ CAMS ○ KARVY ● Some Mutual funds may have inhouse set up for RTA work.
FIU	“Financial information User” means an entity registered with and regulated by any financial sector regulator that wishes to consume the services from Account Aggregator for providing value added services to the **Customer**.
FSR	For the purpose of this document, “Financial Sector Regulator” means the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority (IRDA) and Pension Fund Regulatory and Development Authority (PFRDA)
Customer	Customer for the purpose of NBFC-AA service means a ‘person’ who has entered into a contractual arrangement with the Account Aggregator to avail services provided by the Account Aggregator. Customer maintains account(s) with one or more FIPs. The Customer register with Account Aggregators and provide consent for enabling access to their FI maintained by the FIPs.
Central Registry	The Central Registry provides the FIP and AA public key information so that ecosystem components can validate digital signatures of these entities.
CIN	The Corporate Identity Number is a unique 21 digit alpha-numeric number given to all Private Limited Company, One Person

	Company, Limited Company, Section 8 Company, Nidhi Company and Producer Company registered in India.
XML	Extensible Markup Language

1.5 About Banking and Financial Specifications

The Banking and Financial Specifications are developed via industry led collaborative efforts with ReBIT providing the logistic support as a standards development organization (SDO).

1.6 References

[1] Reserve Bank of India (RBI). “Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions”*.* RBI/DNBR/2016-17/46, Master Direction DNBR.PD.009/03.10.119/2016-17. 2016 (Updated 2017). https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD46859213614C3046C1BF9B7CF563FF1346.PDF (accessed February 12, 2018)

[2] What are the different classes of Digital Signature Certificates? http://cca.gov.in/cca/?q=node/45, (assessed 10 March 2018)

[3] XML Signature Syntax and Processing Version 1.1, https://www.w3.org/TR/xmldsig-core1/ (accessed 2 February, 2018)

[4] Leach, Paul J., Michael Mealling, and Rich Salz. "A Universally Unique Identifier (UUID) URN Namespace." (2005). https://tools.ietf.org/html/rfc4122 (accessed 2 February, 2018)

[5] “JSON Schema”. http://json-schema.org/ (accessed 2 February, 2018)

[6] Jones, Michael, and Dick Hardt. “The oauth 2.0 authorization framework: Bearer token usage”. No. RFC 6750. 2012. https://tools.ietf.org/html/rfc6750 (accessed 2 February,2018)

[7] Institute for Development and Research in Banking Technology (IDRBT). “Certificate Authority”. http://www.idrbt.ac.in/idrbtca.html (accessed 2 February,2018)

[8] Department of Science & Technology, Government of India. “National Data Sharing and Accessibility Standards”.

https://data.gov.in/sites/default/files/NDSAP.pdf (accessed 2 February,2018)

[9] Jones, Michael, John Bradley, and Nat Sakimura. “JSON web signature (JWS)”. No. RFC 7515. 2015. https://tools.ietf.org/html/rfc7515 (accessed 2 February,2018)

[10] T. Berners-Lee, R. Fielding, and L. Masinter, Uniform Resource Identifier (URI): Generic Syntax, (January 2005) https://tools.ietf.org/html/rfc3986 (accessed 10 March, 2018)

[11] Income Tax Department, Online PAN verification Options, https://www.incometaxindia.gov.in/Pages/tax-services/online-pan-verification.aspx (accessed 10 March, 2018)

[12] Daniel J. Bernstein and Tanja Lange. SafeCurves: choosing safe curves for elliptic-curve cryptography. https://safecurves.cr.yp.to , (accessed 10 March 2018).

[13] NIST Special Publication 800-63B, Digital Identity Guidelines, https://pages.nist.gov/800-63-3/sp800-63-3.html , (assessed 10 March 2018).

2 Technical Specification

2.1 Entities Roles and Responsibilities

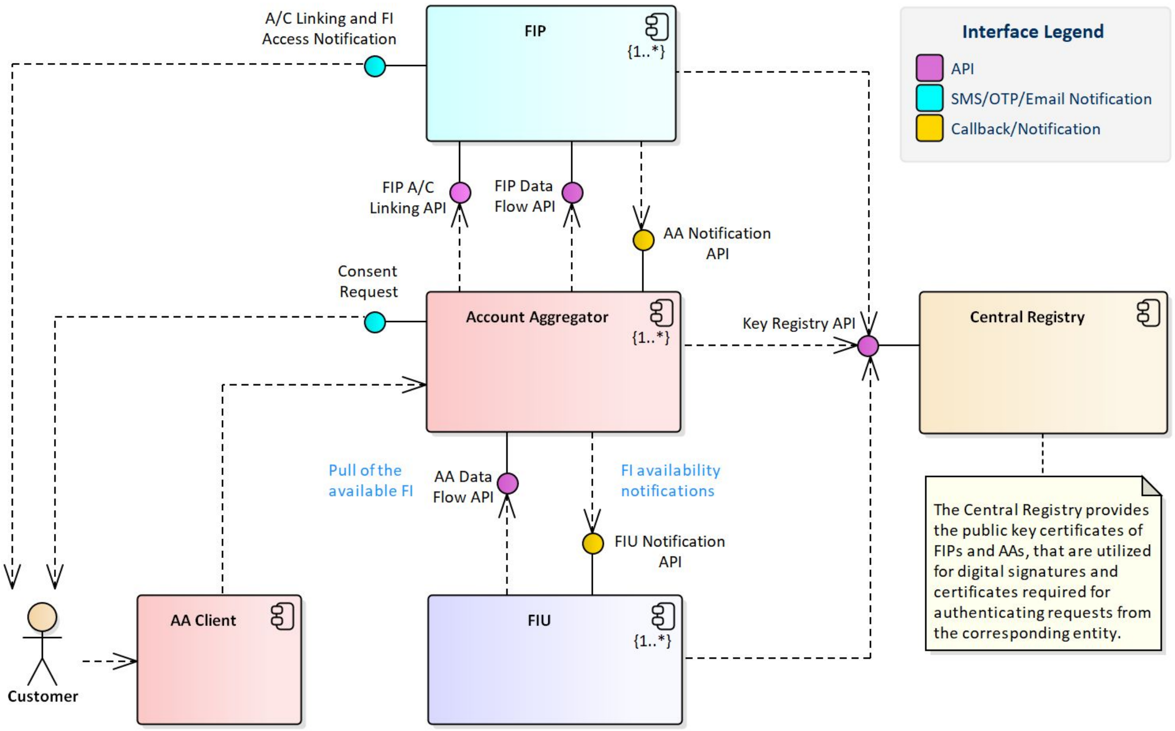
The following table defines the roles and responsibilities of the entities in the account aggregation ecosystem.

AA	The AA is responsible for ensuring that information is requested from FIPs based on Customers’ explicit consent. It collects consent from the Customer for every information request and creates consent artefacts which contain all parameters of the consent granted by the Customer. The AA manages the lifecycle of consent artefacts, including activities like revocation and pausing of consent. It also mediates the actual flow of information from FIPs to FIUs (or from FIPs to other entities authorized by the Customer), first fetching information from the FIPs and then securely forwarding it to the FIU The AA does not maintain any financial information about the customer itself; it only acts as a “pass-through” of information and ensures that no information passes through it without the customer’s consent. The AA maintains logs of all requests for information from FIUs and all events associated with the flow of information. It also maintains logs about consent granted by the customers and any events associated with the consent lifecycle management. The AA must notify customers, FIUs and FIPs about key consent related events e.g., whenever a consent artefact is revoked by the customer, the associated FIU and FIP must be notified about it. Finally, the AA must provide its customers an interface using which they can view and manage consent artefacts associated with them and, optionally, an interface for the customers to view their aggregated financial information.
AA Client	The Account Aggregator Client is an authorized client that interacts with the AA service. It may be implemented as library, SDK or might interact via direct authorized AA API calls. The client may operate in the customer’s environment and provide the necessary customer interactions for requesting the financial information based on the customer’s consents. The AA client could be a web based application, a mobile based application offered by the AA or a SDK/library embedded in another application. The AA is the owner of the AA client.
FIP	The FIP provides information to the AA about the nature of financial

	information of customers held by it. It also provides the actual financial information (in encrypted form) in response to consented requests from the AA. The FIP must maintain logs of all account aggregation queries received from AAs. It must service queries only from authorized AAs. The FIU interacts with the Central Registry and keeps its public key information updated in that registry.
Central Registry	The Central Registry provides the public key certificates of FIPs and AAs, that are utilized for digital signatures and authenticating requests from the corresponding entity.
Customer	The Customer maintains and account and interacts with the AA to link accounts and provides electronic consent.
FIU	The Customer may designate an FIU as the recipient of the Financial Information when requesting consent artefact creation to AA. The FIU needs to maintain the Customer's financial information provided to it securely in compliance with terms of the consent granted by the Customer.

2.2 High Level Architecture

The account aggregation ecosystem uses a layered approach, that decouple the FIU from the FIP via AA. `Account Aggregator` acts as an intermediary and helps connect the `FIU or the customer` to multiple `FIPs` through standardized API interfaces. The following diagram shows the various interfaces and system interactions in the account aggregation ecosystem.


FIP
{1..*}
A/C Linking and FI Access Notification
Interface Legend
API
SMS/OTP/Email Notification
Callback/Notification
FIP A/C Linking API
FIP Data Flow API
AA Notification API
Consent Request
Account Aggregator
{1..*}
Key Registry API
Central Registry
Pull of the available FI
AA Data Flow API
FI availability notifications
FIU Notification API
Customer
AA Client
FIU
{1..*}
The Central Registry provides the public key certificates of FIPs and AAs, that are utilized for digital signatures and certificates required for authenticating requests from the corresponding entity.

The customer interacts with the Account Aggregator for requesting services. The AA client component interfaces with the Account Aggregator either directly or via the API exposed by the AA to facilitates this interaction. The customer interacts with the Account Aggregator to link accounts and generate consent, all such interactions must happen directly between the customer and the AA through an application provided by the Account Aggregator. Such interactions for account linkages and consent generation must not happen via FIU or via an embedded SDK/library provided by the AA. The Financial Information may be made available to the customer via the AA Client application. In the architecture the FIU acts as the recipient of the financial information.

The central registry provides the necessary information about registered FIP and AA in the ecosystem, their corresponding certificates for facilitating the cryptographic functions etc. The central registry may evolve over period of time and may start out as static file. Every registered AA and FIP must use the registry to verify the digital signatures.

The architecture uses asynchronous mechanisms to enhance scalability and provide deterministic mechanisms to fetch consents and financial informations. The notification callbacks include handles for such deterministic calls enabling a decoupled operation from when the request is made, when recipients gets notified about the success and failure status and when the recipient makes a call to retrieve the consent and financial information data. Similar mechanisms are used between FIP and Account Aggregator as well as between Account Aggregator and FIU.

As shown in the high level architecture diagram above, the following Interfaces have been defined:

Interface	Summary
FIP A/C Linking API	This FIP API enables the AA to link FIP account(s) of the Customer with the AA account. Financial information can be fetched only from accounts that are linked with the AA.
FIP Data Flow API	The FIP API provides the interface to AA and enables them to collect the financial information for a customer programmatically. The information is collected based on a digitally signed consent artefact submitted in the request.
A/C Linking and FI Access Notification	This interface is a notification service operated by the FIP notifying the Customer about the A/C linking events and any FI data access request originating because of the account aggregation request. Change in the status of consent are also delivered via this interface.
AA Callback API	This is a callback interface hosted by AA to receive asynchronous status update notification from FIP on the aggregation request.
AA Data Flow API	The FIU uses this AA interface to retrieve financial information once Customer consent has been received.
Consent Request	The interface allows the AA to collect consent from the Customer and thus help validate that the Consent Request indeed came from the Customer.
Consent Management	The Consent Management I/F is hosted by each AA and enables management of the Consent Artefacts and their lifecycle.
Key Registry API	The Key Registry I/F enables AAs to discover new FIPs as they are registered in the AA ecosystem. It maintains the certificates associated with AAs and FIPs.
FIU Callback API	This is a callback interface hosted by FIU to receive asynchronous status update notification on the aggregation request.

These interfaces are further defined in the [Appendix].

2.3 Establishing Linked Accounts of a Customer

Before Customers can request financial information, they need to specify the accounts that they want to make available for account aggregation in the Account Aggregator.

This is an important step so that a filtered set of accounts, explicitly linked by the Customer is made available to the account aggregator. These explicitly linked accounts (with the respective account IDs) of the Customers is maintained by the AA.

2.3.1 Customer Address

Each Customer who has an account with the AA is identified by a unique Customer Address. It represents a handle for searching for AA account details. All AA account addresses are denoted as “account@provider" form. Address should only contain a-z, A-Z, 0-9, .(dot), - (hyphen).

<Customer_identifier>@<AA_identifier>

The Customer Address may be used by FIUs to establish link with customer’s account maintained by them and use it to identify customer’s consent and financial information associated with the customer. The construct is conceptually similar to that of the UPI ID.

2.4 Electronic Consent

The Master Direction [1] requires that the Account Aggregator shall provide services to a Customer based on the Customer’s explicit consent. The Consent is electronically sought from the Customer. The Consent Framework is central to the implementation of the AA architecture. The Electronic Consent in this specification uses the Consent Artefact, which comprises of the following sections:

- **Identifiers**: Specifies all the entities that are involved in the transaction: the Financial Information Providers issuing the information, the Financial Information Users accessing the information, the account aggregators, and the Customers. The identifier element may further include account or customer identifiers required to uniquely identify a Customer’s financial information maintained by the FIP.
- **Data section**: The Data Section comprises of fields describing the type of information that is being accessed and the access permissions associated with each of them. This section also describes the specific information that is requested, the duration for which information is requested (e.g., the past 6 months’ statement of an account), duration of storage by Financial Information User (referred to as “datalife”), the frequency of access, along with a set of pre-processing filters that can be used to further customize the information that is retrieved. Access permissions can be of four types:
    - The requester can either get VIEW access to the information, which implies that the FIU is not allowed to store the data or reuse it later.
    - The FIU or AA application can STORE the information and use it within the period defined in datalife. All information must be exchanged between the provider and the consumer in a secure fashion using either data

and/or channel encryption. Information must be destroyed after the datalife.

- The STREAM permission facilitates in-point streaming of information to the FIU.
- 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.

- **Purpose of access**: This may include information about the application domain (e.g., finance) and the application within that domain that is enabled through the financial information access (e.g., loan offer computation) and a free-form textual description.
- **Signature**: The Consent Artefact is digitally signed by AA as per the W3C recommendations [3] for XML format.

When a Customer requests for financial information, the AA collects the consent from the Customer. The AA creates two different Consent Artefacts for an information request from a single FIP account. One Consent Artefact authorizes the FIU/Customer to request aggregated information from the AA and the other Consent Artefact authorizes the AA to obtain information from that FIP for transferring to the FIU/Customer. The latter artefact does NOT mention details of the FIU that is requesting information. This is done in order to ensure anonymity of the FIU in information requests, which helps prevent differentiated service delivery by the FIPs.

Consent Artefact XML between Customer and AA

```
<?xml version="1.0" encoding="UTF-8"?>
<Consent xmlns="http://meity.gov.in" id="" createTime="YYYY-MM-DDThh:mm:ssZn.n"
startTime="YYYY-MM-DDThh:mm:ssZn.n" expireTime="YYYY-MM-DDThh:mm:ssZn.n" >

   <!-- Identifiers -->
   <FIP id= "" />
   <FIU id= "" />   <!-- Optional -->
   <AA id= "" />

   <Customer idType="" id=""/>
   <!-- Following element may repeat; captures multiple IDs for same Customer
   <!-- Following element captures Customer account at FIP -->
   <Account accountType="" id=""/>
   <!-- Data Block -->
   <Data-Items>
      <!-- following element repeats -->
      <Data name="" type="TRANSACTIONAL|PROFILE">
         <Access mode="STORE|QUERY|STREAM" />
         <!-- the duration for which information is requested -->
         <Duration unit="DAY|MONTH|YEAR|INF" value="" />
         <!-- how long can the information requester store data -->
         <Datalife unit="MONTH|YEAR|DATE|INF" value="" />
         <!-- frequency and number of repeats for periodic information access -->
         <Frequency unit="DAILY|MONTHLY|YEARLY" value="" repeats="" />
         <Data-filter>
            <!-- Data access filter, any encoded query string as per financial
information provider API needs -->
         </Data-filter>
      </Data>
   </Data-Items>

   <!-- Logging block -->
   <ConsentUse logUri=""/>
   <DataAccess logUri=""/>

   <!-- Purpose block -->
   <Purpose code="" refUri="">
      <!-- purpose text goes here -->
   </Purpose>

   <!-- Signature block -->
   <Signature> Signature of AA as defined in W3C standards; Base64 encoded
</Signature>

</Consent>
```

Consent Artefact XML between AA and FIP

```
<?xml version="1.0" encoding="UTF-8"?>
<Consent xmlns="http://meity.gov.in" id="" createTime="YYYY-MM-DDThh:mm:ssZn.n"
startTime="YYYY-MM-DDThh:mm:ssZn.n" expireTime="YYYY-MM-DDThh:mm:ssZn.n"
revocable="true|false">

   <!-- Identifiers -->
   <FIP id= "" />
   <AA id= "" />
   <!-- Following element may repeat; captures multiple IDs for same customer -->
   <Customer idType="" id=""/>

   <!-- Following element captures customer account at FIP -->
   <Account accountType="" id="" />
   <!-- Data Block -->
   <Data-Items>
```

```
      <!-- following element repeats -->
      <Data name="" type="TRANSACTIONAL|PROFILE|DOCUMENT">
         <Access mode="VIEW|STORE|QUERY|STREAM" />
         <!-- the duration for which information is requested -->
         <Duration unit="DAY|MONTH|YEAR|INF" value="" />
         <!-- how long can consumer is allowed to store data -->
         <Datalife unit="DAY|MONTH|YEAR|INF" value="" />
         <!-- frequency and number of repeats for access repeats -->
         <Frequency unit="DAILY|MONTHLY|YEARLY" value="" repeats="" />
         <Data-filter>
            <!-- Data access filter, any encoded query string as per financial
information provider API needs -->
         </Data-filter>
      </Data>
   </Data-Items>

   <!-- Logging block -->
   <ConsentUse logUri="" />
   <DataAccess logUri="" />

   <!-- Purpose block -->
   <Purpose code="" refUri="">
      <!-- purpose text goes here -->
   </Purpose>

   <!-- Signature block -->
   <Signature> Signature of AA as defined in W3C standards; Base64 encoded
</Signature>

</Consent>
```

2.5 Purpose

This section define purpose of the information usage. The refUri should follow the specification defined in [10].

- **code**: It is a unique number assigned to an identified purpose for which a customer consent may be sought.
- **refUri**: This refers to a URL where the purpose is further defined in a machine readable format.
- **text**: A brief textual description of the purpose.

Following are some examples of the purposes that the system will support.

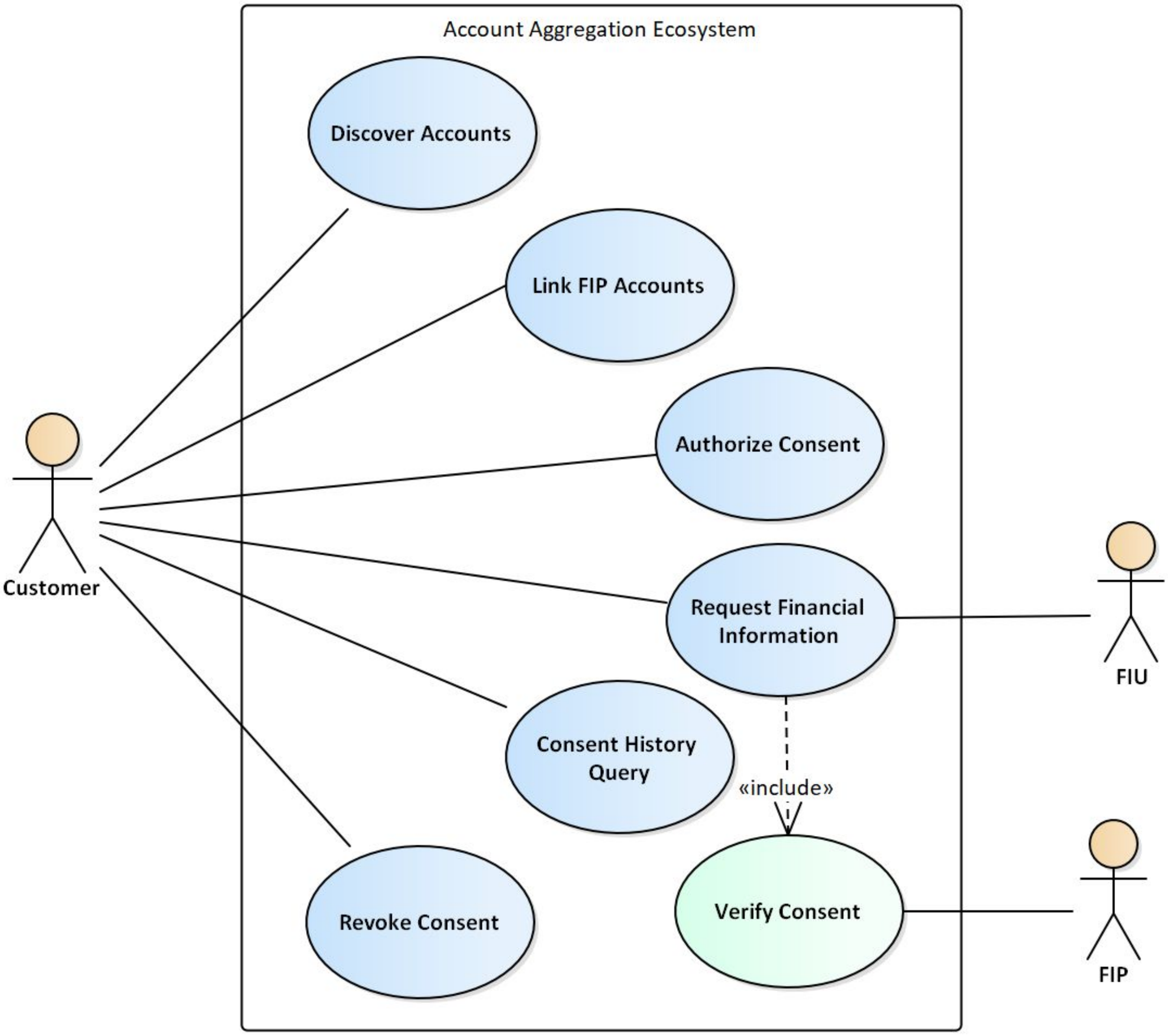
Code	field	value
101	refUri	https://api.rebit.org.in/aa/purpose/101.xml
	text	Wealth management service
102	refUri	https://api.rebit.org.in/aa/purpose/102.xml
	text	Aggregated statement
103	refUri	https://api.rebit.org.in/aa/purpose/103.xml
	text	Customer spending patterns, budget or other reportings
104	refUri	https://api.rebit.org.in/aa/purpose/104.xml
	text	Explicit consent for monitoring of the account against a covenant

Standards set of purposes will be published as a part of the technical standards. Please see Appendix [Section 6.4] for details on how to register a new purpose code.

3 Use Cases

The Account Aggregator ecosystem would support the following minimal use cases.

High Level Use Case Diagram



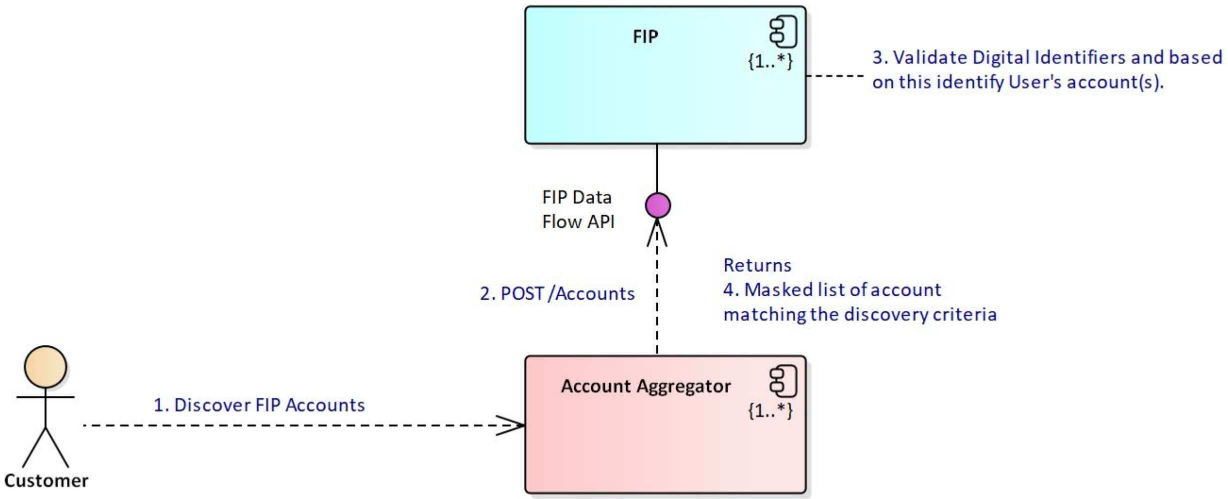
3.1 Discover Accounts

In this use case, a Customer initiates linkage of the FIP accounts their account maintained at AA. The AA, based on input from the Customer, passes a verified digital identifier such as a Mobile Number, Aadhaar Number, or PAN. to the "`POST /Accounts`" API of the FIP to obtain a list of masked accounts. The discovery happens in the AA domain and does not require Customer authentication in the FIP domain.

The Customer may choose to subsequently link these discovered account(s) to their account at the AA. The linking of account, is a prerequisite for consents to be generated. Customer consent can only be generated for linked accounts.

The discovery relies on identifying a Customer's account(s) based on a set of passed matching digital identifiers and their corresponding mapping with the accounts of the

Customer held by the FIP. Multiple identifiers may be passed for the discovery process but the request must include at least one verified strong identifier. Mobile Number and Aadhaar are examples of verifiable strong digital identifiers. The following diagram illustrates the operation of the "Discover Accounts" use case:


FIP
{1..*}
3. Validate Digital Identifiers and based on this identify User's account(s).
FIP Data Flow API
2. POST /Accounts
Returns
4. Masked list of account matching the discovery criteria
Account Aggregator
{1..*}
1. Discover FIP Accounts
Customer

Summary	This Use Case allows the Customer to discover their FIP accounts
Pre-condition	● The Customer has logged into the AA application ● The Customer has at least one strong verified digital identifier
Actor	Customer
Main Flow	1. The Customer initiates an account discovery process across one or more FIPs. a. The AA must ensure that at least one strong identifier is present in the request. b. The AA application may ask Customer to optionally select `FITypes` and/or account types for further filtering in the account listing. 2. The AA will use the `POST /Accounts` API to receive the masked account details of the Customer. 3. The FIP will validate the passed verified identifiers and return list of accounts with masked account details back to AA. 4. The AA displays this information to the Customer for subsequent account linkage. 5. The use case ends.
Alternate Flows	**Alt.1**: Account at FIP not discovered

	In this case, the AA responds to the FIU with the reason code and explanation. For such FIPs the AA may provide choice to the customer to enter additional identifiers such as Account Number/Folio Number/Customer ID etc and then retry the account discovery process.
Post-condition	A list of masked FIP accounts and corresponding `accountRefId` is provided to the AA that the Customer can then choose to proceed and link with her AA account. The customer shall then proceed to authenticate herself with that FIP account to link the same with her AA account.
Security and Audit Requirement	In the Account Discovery request, the AA must mark all identifiers it has verified, that includes strong identifiers, weak identifiers and custom non-verifiable functional identifiers that the Customer provides. The FIP must only respond if at least one of the verified strong identifiers match the record of the customer.
Comments	Aadhaar is considered a strong identifier. The AA may choose one of the available methods of verifying the Customer Aadhaar number. Furthermore, the mobile number and emails can be verifier using OTP and code verification mechanisms. PAN number can be verified against the income tax department, NSDL or UTIITSL [11]. For masking, all digits except for the last 4 digits of the account number must be masked. Mobile numbers are typically masked to show only the last 5 digits. See section [5.4.1].

3.1.1 Account and Identity Validation

The discovery happens in the AA domain. The customer must have an account in the AA domain. The AA must provide provisions for the customer to verify, if they haven't already verified during authentication, their Mobile Number, Aadhaar Number, and PAN Card. Also see section [5.2.2] on Digital Identifiers.

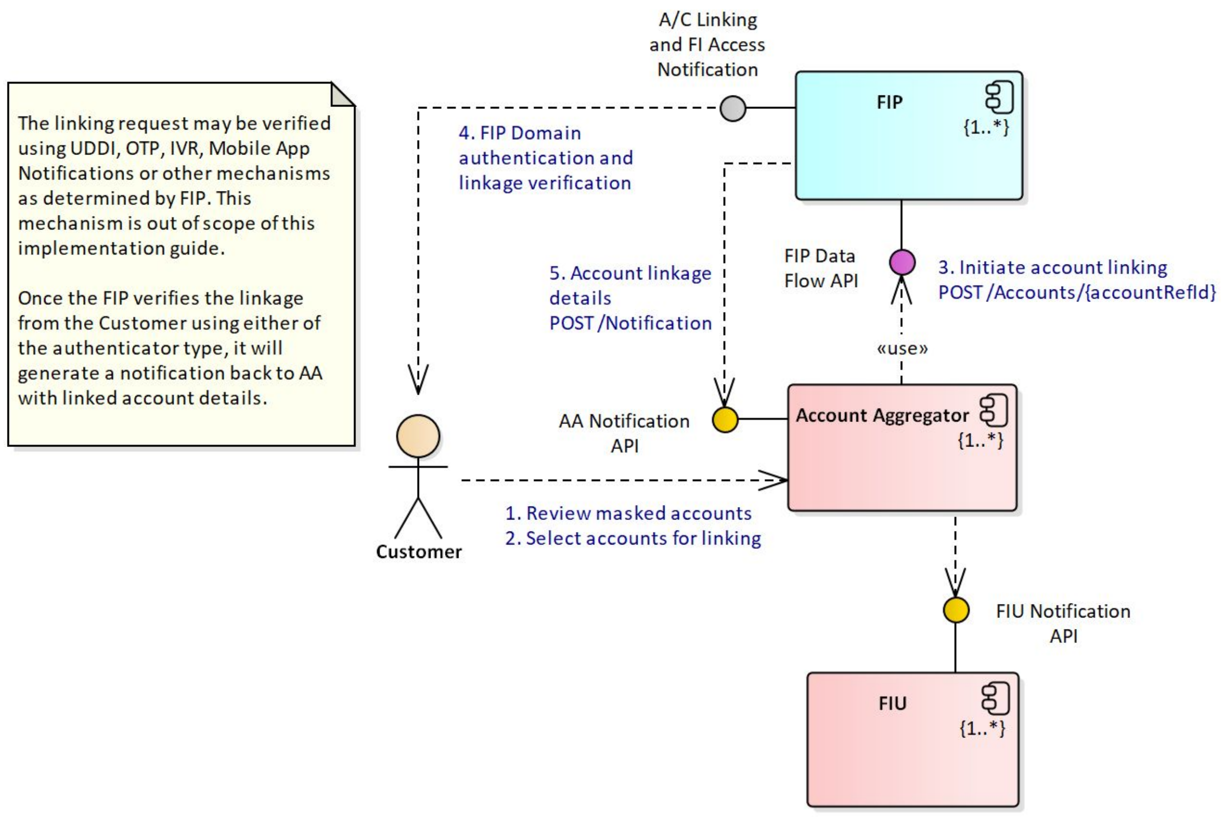
3.2 Link FIP Accounts at AA

This use case describes how a set of accounts are linked to the Customer's AA profile. The consents can only be created for accounts which the Customer has explicitly linked in their profile. Customer authorization in the FIP Domain is required to complete the linking of the accounts.

There are two kinds of authenticators that the FIP may support:

1. **FIP Direct Authenticator**: The authenticator obtains confirmation through an interaction directly with the customer.
2. **FIP Authorization Token-based Authenticator**: In this case, a token (e.g., a short-lived one-time password) is issued to the customer, which the customer can then supply to the AA for subsequent forwarding to the FIP. This provides a confirmation to the FIP that the customer has approved the linking request to AA.

The diagram below shows a mechanism that could be implemented by the AA and FIP to facilitate this.



The linking request may be verified using UDDI, OTP, IVR, Mobile App Notifications or other mechanisms as determined by FIP. This mechanism is out of scope of this implementation guide.

Once the FIP verifies the linkage from the Customer using either of the authenticator type, it will generate a notification back to AA with linked account details.

Once this linking is successfully completed (i.e. the User is authenticated by the FIP), the `accountId`, `accountType`, `customerId` and `FIType` will be made available at AA and stored in the Linked Accounts of the Customer.

3.2.1 Link Account

Summary	A customer initiates the FIP linking requests [see section 2.3] from the AA application.

Pre-condition	● The Customer has an account at the AA ● Verified Customer's mobile and/or email address may be required for enabling OTP messaging from the FIP ● The discovery of Customer's accounts has happened as specified in the previous use case
Actor	Customer
Main Flow	**Token-based Authenticator** 1. The Customer has a masked list of accounts to initiate the account linking process in the AA application 2. The Customer selects the masked accounts to be linked in her profile. 3. The AA application requests FIP for these masked accounts to be linked. 4. The FIP sends OTP details corresponding to specific accounts of the customer at FIP 5. The Customer enters, the OTP on the AA screen. 6. The AA forwards this OTP detail back to FIP. 7. Once the FIP confirms the OTP it sends a notification to AA application with the details of the linked account. 8. The AA updates the linked accounts details. 9. The use case ends.
Alternate Flow	**Direct Authenticator** 1. The Customer has a masked list of accounts to initiate the account linking process in the AA application 2. The Customer selects the masked accounts to be linked in her profile. 3. The AA application requests the FIP for the masked account(s) (using the `accountRefId`) to be linked. 4. The Customer authentication and verification happens in the FIP domain. 5. Once the FIP verifies the link account request with the Customer, the FIP sends a notification to the AA application with the details of the linked account. 6. The AA updates the linked accounts details. 7. The Customer is presented with the updated linked profiles. 8. AA may send notification to the FIU application and the Customer may switch context to the FIU application. 9. The use case ends.
Post-condition	Once this linking profile, i.e. the FIP account linkages are established for the Customer, the AA will enable Consent Artefacts creation for these linked accounts.
Notes	

Security and Audit Requirements	All account linking activities should be logged. The linkages should be established based on explicit interaction between the FIP and the customer.

3.2.2 Delink Account

Account delinking can happen in one of the two ways:

- Account delinking initiated at AA
- Account delinking at FIP, such as in case of customer request to FIP, account closure and other internal events in the FIP domain.

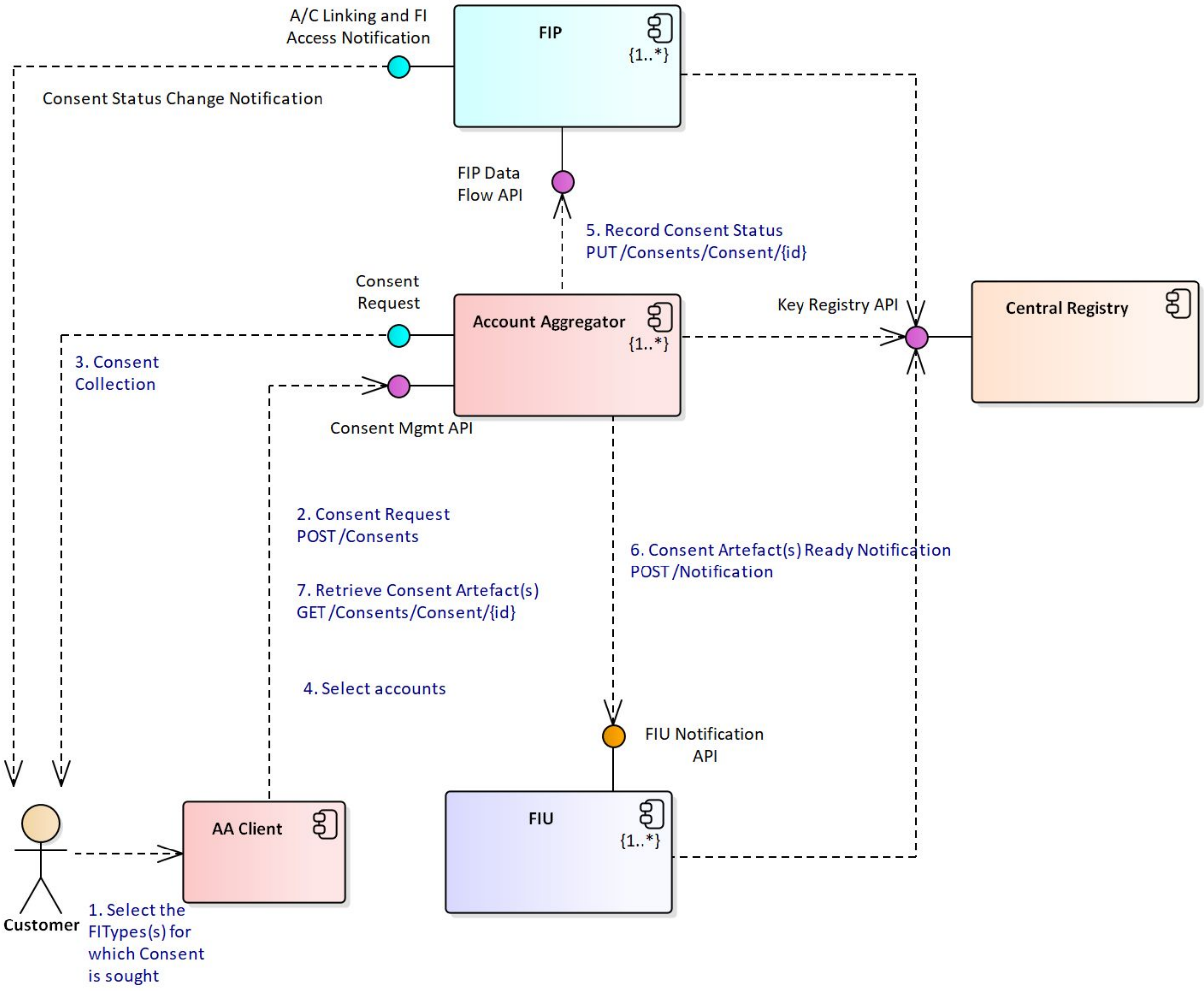
When the linked account is delinked, all the Consent Artefacts associated with this linked account are revoked and FIU and FIP are notified. The delinking action is performed on the AA application screen.

Summary	AA registered account customer using the AA application initiates the FIP delinking request.
Pre-condition	● The customer has account at AA ● The customer's email and mobile are verified by the AA ● The customer is able to provide identifier(s) that can help FIP identify the account associated with the customer. This could be Aadhaar, PAN, CIN or the unique account number. ● The customer's mobile and/or email address may be required for this initial registration for enabling OTP messaging from FIP ● The discovery of customer accounts have happened as specified in the previous use case ● The customer has already linked the accounts
Actor	Customer
Main Flow	1. The customer initiates the account de-linking process in the AA application 2. The customer selects the account(s) to be de-linked in her profile. 3. The AA application notifies FIP for these delinked accounts. 4. The AA updates the de-linked accounts details. 5. The AA may send notification to the FIU application and customer may switch context to the FIU application. 6. The use case ends.

Alternate Flows	The customer requests account delinking at FIP In this case, once the FIP updates its record, the FIP sends a notification to the AA and AA proceeds with removing the account delinking process. AA will notify the customer of such change.
Post-condition	The AA will revoke the consents previously created against this account. New consents can't be generated for this de-linked account.
Notes	
Security and Audit Requirements	All account de-linking activities should be logged. The OTP must be sent to a verified address (verified mobile number or the email address). All records for the historical consent artefacts must be maintained in compliance with the IT Act.

3.3 Create Consent Artefact(s)

The customer's Consent Artefact is important for enabling request of FI from the FIPs. AA can only request for FI from FIP once it has obtained the consent from the customer. AA is the Consent Manager and manages the entire lifecycle of the consents. This use case illustrate the mechanism for obtaining the consent based on a customer interaction with the AA application.


A/C Linking and FI Access Notification
FIP
{1..*}
Consent Status Change Notification
FIP Data Flow API
5. Record Consent Status PUT /Consents/Consent/{id}
Consent Request
Account Aggregator
{1..*}
Key Registry API
Central Registry
3. Consent Collection
Consent Mgmt API
2. Consent Request POST /Consents
7. Retrieve Consent Artefact(s) GET /Consents/Consent/{id}
6. Consent Artefact(s) Ready Notification POST /Notification
4. Select accounts
FIU Notification API
AA Client
FIU
{1..*}
Customer
1. Select the FITypes(s) for which Consent is sought

The AA acts as the Consent Manager in the account aggregation architecture and interacts with the customer to obtain Consent. The FIP is the consumer of the consent and provides information based on the Consent Artefact submitted to it by the AA. Furthermore, FIP maintains the most up to date status of the pertinent Consent Artefacts.

The Consent Generation Request may include `FIType(s)` and other filtering criteria to improve the account selection on the AA for Consent Artefact(s) generation. The Consent Management always happens in the AA domain.

During a Consent Generation Request for a particular purpose at a particular point in time, each FIP account selected by the customer on the AA application will result in the AA generating a pair of Consent Artefacts, one authorising data sharing between AA and FIP and another authorising data sharing between AA and FIU. Each of the Consent Artefacts in the pair has their own unique identifier.

Summary	In order to perform the account aggregation for the customer, the FIU will request the AA Consent Flow API method “`POST /Consents`” to generate a digitally signed consent artefact. This use case defines the mechanism for obtaining consent from the customer and creation of the Consent Artefact(s). Valid Consent Artefact(s) are required to request for Financial Information from the FIPs.
Pre-condition	● The customer has created his Customer Address with the account aggregator ● The customer’s FIP account linkage has been performed on the AA ● The Consent Artefact(s) request may be initiated from either the AA application or the AA Client.
Actor	Customer
Main Flow	1. The customer selects the `FIType(s)` for which Consent is sought. The AA client either prefills a cached “`Customer Address`” or asks the customer to enter it. 2. Based on the selection of the `FIType(s)`, the AA client makes a request to the AA for the Consent Artefact(s) specifying the purpose for which the consent is sought using the “`POST /Consents`” API call on the AA Consent Management interface. 3. The AA initiates a Consent Collection process in the AA domain 4. The customer selects the linked accounts for which the consents can be generated. 5. The AA generates the Consent Artefact(s) and updates the corresponding FIP(s) with the status of the consent using the “`PUT /Consents/Consent/{id}`” method. 6. The AA application may generates a consent completed notification back to the FIU using the “`POST /Notification`” API on the FIU. 7. The FIU may then retrieves the consent artefacts from the AA using the “`GET /Consents/Consent/{id}`”. 8. The use case ends.
Alternate Flows	
Post-condition	Consent Artefacts are generated.
Notes	The AA client or FIP can request the Consent Artefact(s) using the “`GET /Consents/Consent/{id}`” API on the AA. The AA must validate the FIP and AA client and only respond with Consent Artefact that corresponds to these entities.

	The “`GET /Consents/{consentHandle}`” method provides a mechanism for AA client to obtain list of Consents Artefact(s) id generated in the “Consent Creation” request and their corresponding status.
Security and Audit Requirements	1. The Consent Artefact(s) are digitally signed. 2. The FIP maintains the status (active, revoked) of the Consent Artefacts. 3. All Consent creation requested must be logged.

3.4 Request Financial Information

FIP must provide the requested information to the AA only after validating the consent artefact, which involves verifying the embedded signature and checking for timeliness of the request. Since the requested financial information is time-dependent in nature, the request must specify the time instant for which information is being requested. This time instant must either be the same as the current time or an instant in the past. For example a request for information made at 12pm 31st October, 2018 may ask for information as it stands at that time, or it could ask for information as it existed at a past instant, say at 12pm, 30th October, 2018. This time instant for which information is requested is referred to as the ***capture time***. The FIP is expected to furnish information as it existed at the capture time, assuming that the capture time specified in the request is the same as the time at which the request is received by the FIP or is prior to the time at which the request is received.

Information needs to be provided by the FIP to the AA in a timely manner in accordance with the SLAs defined in the Master Directive or the FSR.

Consent Artefact Verification and Validation

Consent Artefact must be verified when FIP receives it from AA. Verification steps consist of:

1. Verify the credentials of the AA
2. Verify Consent Artefact is issued by authorised customer
3. Verify that the Artefact is valid, is in active state and contains all mandatory information

Consent Artefact is verified if, and only if all the verification steps are passed.

Consent Artefact must be validated every time information is requested based on the consent. The artefact is deemed valid if:

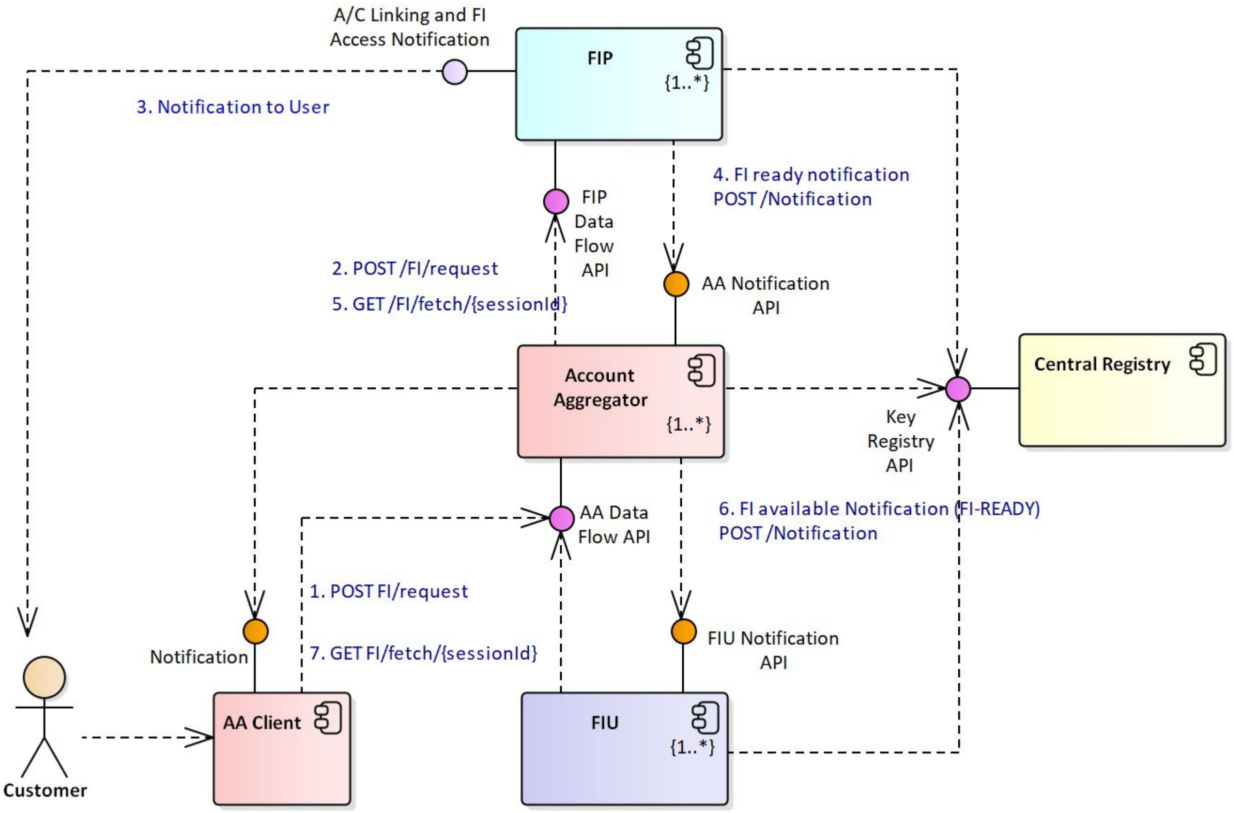
1. The capture time given in the request lies between the start time and the expiry time of the artefact and is either the same as the time at which the request is received or is prior to the time at which the request is received.
2. Consent has not been revoked based on the Revocation List maintained by the FIP (details of which have been specified in the section on Consent Revocation)

Types of Information Transfer

Information can be shared in two ways:

- **One Time**, where a customer requests for information to be shared exactly once. After the consent artefact has been created and approved, the AA client can request for information using a set of active consent artefacts. The AA verifies and forwards that request to the appropriate FIP as specified in the artefact. The FIP verifies the artefact and responds to the request. The information is then forwarded by the AA to the requesting entity.
- **Periodic**, where a customer or the AA client requests for periodic sharing of information. In case of periodic sharing request, AA, on behalf of the customer requests FIP periodically to share information. If the consent artefact provides permission for n information requests at specified time intervals, the AA would issue n data requests to the FIP, each with a different capture time. The information is then shared in the same way as described in the One-Time Data Transfer method.

In both cases, the AA is allowed to make multiple information requests with the same capture time and the same consent artefact. This may be required to compensate for any loss of information previously transmitted to the requesting entity. As long as the consent artefact is valid, the FIP must respond to the information request.



3.4.1 One-time fetch

Summary	The AA client requests for financial information once.
Pre-condition	• The customer has linked her respective FIP accounts as described in 2.3 and in use case 3.2. • The Consent Artefact(s) for the aggregation request has been created
Actor	Customer
Main Flow	1. The AA client makes a request for financial information using identifiers of previously created Consent Artefact(s) maintained in the customer's profile. The AA client includes the encryption parameters and the target recipient in the request using the "`POST /FI/request`" API. 2. The AA verifies the Consent Artefact(s) provided by the AA client: a. Verifies the status of the Consent Artefact(s) in its records. b. Verifies that all accounts are still linked for the customer. For accounts that are no longer linked,

revokes the Consent Artefact(s) and notifies the FIU and FIP.

  c. Verifies the FIU-AA Consent Artefact(s) against the Customer Address specified in the consent.

3. For each FIP from which financial information needs to be aggregated
    a. The AA constructs the financial information request, including the Consent Artefact and the encryption parameters and makes a request to the FIP, with a callback notification URL.
    b. The FIP verifies the Consent Artefact:
        i. Verifies the Digital Signature of the Consent
        ii. Verifies the integrity of the Consent Artefact
        iii. Validates the content of the Consent Artefact against the linked account reference.
        iv. Extracts and construct the encryption key for responding to the financial information request
        v. Verifies the validity time of the Consent Artefact
        vi. Verifies that the Consent has not been revoked.
    c. If the verification at FIP fails, goto **Alt.1** use case.
    d. The FIP constructs the financial information, encrypts it using the “encryption key” and notifies AA.
4. The AA fetches the encrypted financial information from the FIP upon notification.
5. The AA tracks status from all FIP(s) from which it is requesting aggregation.
6. During the aggregation process, the AA notifies AA client/FIU about the status update on the financial information collection from various FIP(s).
7. Once requests from all FIP(s) is completed (either success or failure), it constructs a response notification back to the recipient (FIU) with details to fetch the financial information
8. The FIU upon receiving the aggregation completion request, fetches the financial information from AA.

	9. FIU pulls the aggregated financial information and the customer is notified about the financial information availability. 10. The use case ends.
Alternate Flows	**Alt.1**: Verification at FIP fails 1. The AA is notified about the failure. 2. The AA records this in the audit log. 3. Depending upon the error conditions, the AA may revoke and archive the Consent Artefact. 4. The FIU is notified
Post-condition	● The FIU has obtained the aggregated Financial Information. ● The AA purges the aggregated financial information once the request is complete.
Security and Audit Requirements	The AA client runs in an environment separate from AA. The AA should not generate cryptographic keys on their environment for fetching the FI data.
Notes	Real-time response from FIP is expected. The asynchronous responses will have timeouts.

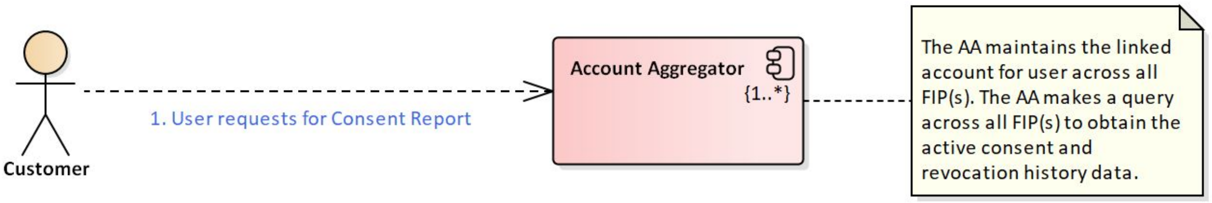
3.4.2 AA Initiated Financial Information periodic fetch

Summary	The AA will support periodic aggregation of the FI based on created consents and push a FI-READY notification to FIU or directly to an app installed in the Customer’s environment. The FIU or the application can then fetch the FI. This use case defines the flow for this periodic fetch. This AA initiated push notification enhances the Customer experience and enables the customer to obtain the FI data based on a configured scheduled.
Pre-condition	● Account linking profile is available on the AA ● Consents for periodic FI requests have been created ● Consent records status are maintained at FIP ● The Customer Address of the customer has been configured
Actor	AA
Main Flow	1. The AA initiates a pre-scheduled FI request based on set

	of keys received from the AA app or the FIP app and the corresponding consent artefacts 2. For each FIP from which financial information needs to be aggregated a. The AA constructs the financial information request, including the Consent Artefact and the encryption parameters previously sent by the FIU and makes a request to the FIP, with a callback notification URL. b. The FIP verifies the Consent Artefact: i. Verifies the Digital Signature of the Consent ii. Verifies the integrity of the Consent Artefact iii. Validates the content of the Consent Artefact against the linked account reference. iv. Extracts and construct the encryption key for responding to the financial information request v. Verifies the validity time of the Consent Artefact vi. Verifies that Consent has not been revoked. c. If the verification at FIP fails, goto **Alt.1** use case. d. The FIP constructs the financial information, encrypts it using the “encryption key” and notifies AA about FI data availability. 3. The AA tracks status from all FIP(s) from which it is requesting aggregation. 4. During the aggregation process, the AA notifies FIU about the status update on the financial information collection from various FIP(s). 5. Once requests from all FIP(s) is completed (either success or failure), it constructs a response notification back to the FIU with details to fetch the financial information, so aggregated. 6. The FIU upon receiving the aggregation completion request, fetches the financial information from AA. 7. FIU builds the aggregated financial information and notifies the customer about the availability of the financial information. 8. The use case ends.
Alternate Flows	**Alt.1**: Verification at FIP fails

	1. The AA is notified about the failure. 2. The AA records this in the audit log. 3. Depending upon the error conditions, the AA may revoke or discard the consent. 4. The FIU is notified
Post-condition	After the data is fetched by User/FIU the data will be purged by AA
Note	AA is never supposed to generate the cryptographic primitives and the encryption keys in their environment although the cryptographic primitives for the FI encryption can be generated in the customer's environment by an AA client.

3.5 Consent History

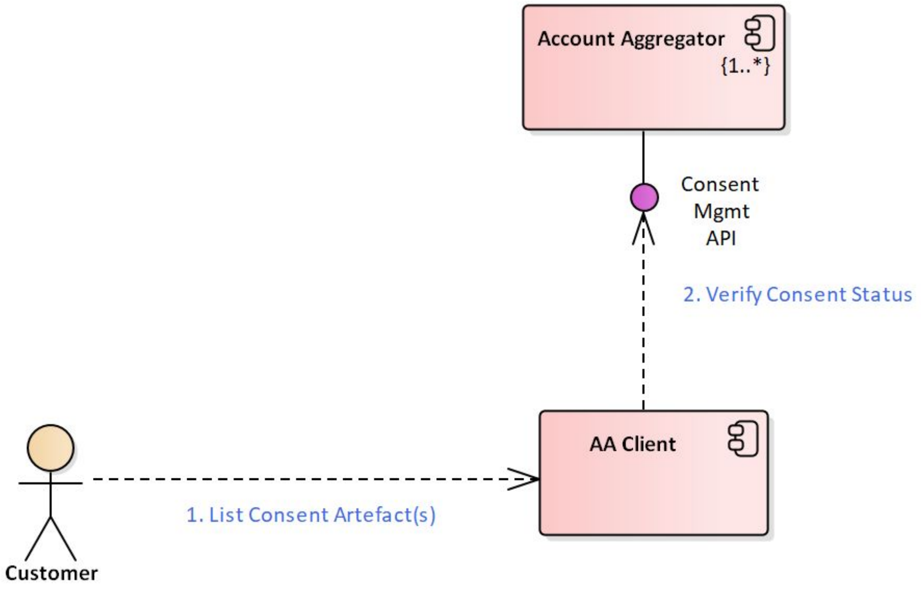

Customer
1. User requests for Consent Report
Account Aggregator
{1..*}
The AA maintains the linked account for user across all FIP(s). The AA makes a query across all FIP(s) to obtain the active consent and revocation history data.

Summary	The Consent Artefacts are created by the AA. The AA client maintains a copy of the Consent Artefacts to request aggregation and the FIP maintains the status of the Consent Artefacts against which it verifies the Financial Information requests. The AA mediates revocation of the Consent with the FIP. The customers may be interacting with multiple FIUs and AAs for Consent Artefact(s) creation. In this case it it important to provide the customers with the ability to obtain a comprehensive list of all Consent Artefact(s) associated with her profile. This use case describes how a comprehensive list of Consent Artefact(s) are provided to the customer. The customer may interact with the AA to get a comprehensive list of all Consent Artefact(s) across all the FIP with which there

	are linked accounts. All revoked and archived Consent History will also be made available to the customer.
Pre-condition	● Account linking profile is available on the AA ● The Customer Address of the customer has been configured
Actor	Customer
Main Flow	1. The customer logs into the AA application 2. The customer requests for the Consent log from the AA 3. The AA retrieves the customer's account linkage profile from its datastore 4. The AA presents a comprehensive list to the customer. 5. The use case ends.
Alternate Flows	**Alt.1**: FIP consents log: Customer uses the FIP application to see the consent that it maintains for the Customer.
Post-condition	History of all consents that have been created for the customer is displayed.

3.5.1 Alt.1: AA client consents log

The AA client specific maintained Consent Artefacts are displayed to the customer when using the application that has AA client functionality. This may be a subset of all consent that may exist for the customer across multiple AA clients that the customer might be interacting with, but presents a comprehensive list of all Consent related to the specific AA client. The following diagram shows the use case operation.

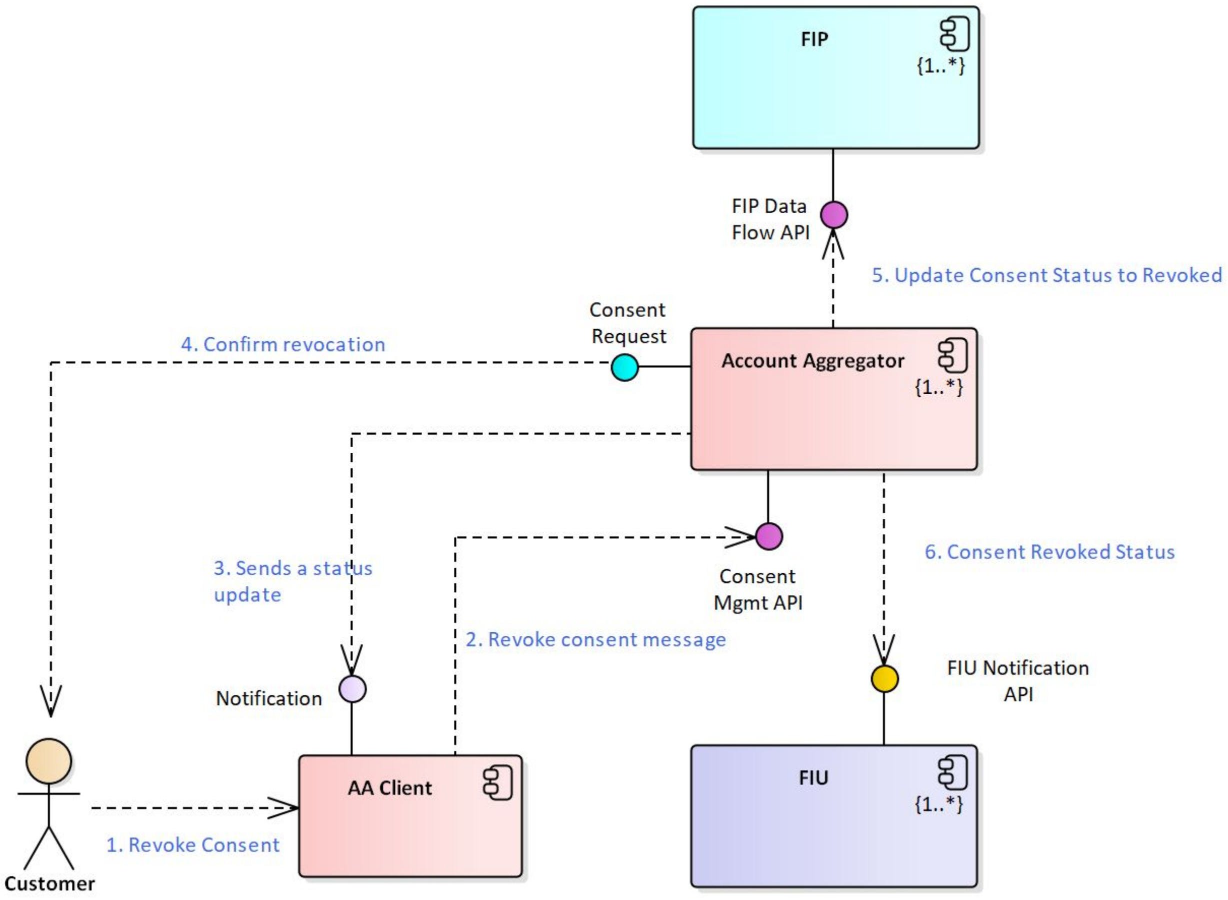


Summary	The AA client application may also provide the Consent History of the specific Consents that were generated from this application. This use case define the mechanisms for the AA client application to provide a listing of the Consents. Since the customer may use multiple AA client applications for different services, the AA client based "Consent History" will not be comprehensive list but may just be a subset. A comprehensive listing of the "Consents" may only be provided via the AA. This is an optional feature the AA client application may offer.
Pre-condition	● The customer is logged into the AA client application ● The "Consent Artefact(s)" for the customer have previously been generated on the FIU application
Actor	Customer
Main Flow	1. The customer requests consent history on the FIU application. 2. The AA client application loads the "Consent History" 3. It may verify the Consent Status for each of the Consent with the AA. 4. The AA client application displays the verified "Consent History" to the customer. 5. The use case ends.
Alternate Flows	None

Post-condition	Consent History of the Consent generated in the AA client domain is displayed to the customer within the AA client.
Note	

3.6 Revoke Consent

The AA enables the consent lifecycle management. An important aspect of the Consent Management is the Revoke, Pause and Resume the state of the consents. These state updates happen in the AA domain through interaction with the customer. In certain cases, for example, when a customer deletes their account with FIU, the FIU will initiate the Revocation of all consents associated with the customer's profile at AA.



Summary	The Consent Artefact(s) once created may be revoked by the customer. The revocation status is maintained by AA and notified to FIP. A customer will have rights to revoke the consents previously

	created for her linked accounts.
Pre-condition	● The Consents have been created for the customer ● The customer is using the AA client. ● The customer has obtained list of of active Consent from the application
Actor	Customer
Main Flow	1. The customer selects option to revoke consent. 2. The Application context switches to AA application 3. The customer selects the consents to be revoked. 4. The AA asks customer for the Consent Revocation confirmation. 5. Once the customer confirms, the AA notifies the corresponding FIP about the Consent Revocation. 6. The FIP records the Consent's status as revoked and responds to AA. (It's important that FIPs maintain a list of all revoked artefact-IDs. This revocation list must also be shared with the Account Aggregators.) 7. The AA generates a notification to the FIU specifying that the Consent has been revoked. 8. The FIU intimates the customer that the Consent has been revoked. 9. The customer switches to the FIU application. 10. The use case ends.
Alternate Flows	**Alt.1**: Revoking the consent from the AA application When the Customer initiates the Consent revocation from the AA application, the AA generates the notification for the FIU, i.e. the FIU notifying it about the Consent revocation. **Alt.2**: Revocation upon AA account deletion When a customer's FIU account is deleted, all consents related to the customer's must be revoked. The FIU must trigger the consents revocation upon the customer's account deletion. All consents linked to the customer/FIU shall be revoked. In this case, FIU will trigger notification about customer account deletion to AA. The AA will revoke all of the customer's consents associated with this FIP. **Alt.3**: Revocation at FIP

	The FIP may revoke the consent upon customer request. In this case the FIP will send a revocation notification to the AA.
Post-condition	The FIP has recorded the Consent as revoked, the Consent can't be used for requesting the financial information from the FIP.
Security and Audit Requirement	The Consent Revocation calls will be logged for Audit trails. The AA client functionality for revocation of the consent must be provided by the AA.
Notes	The revocation notification is sent to both FIP and FIU.

4 Financial Information

The API specifications deals with encrypted data. The cryptographic primitives required for encrypting the data and the structure within which the encrypted and signed data is exchanged is generic and is agnostic of the representation of the data. This makes the API agnostic to the FI document structure and enables addition and evolution of the financial information representation indepent of the API versioning. It is however important that well defined data dictionary and standardized vocabulary is established for a common understanding of data representation between FIP and FIU/customer for an efficient exchange. This section provides primitives that will be used for exchanging customer's financial information between FIP and AA. A standard list of financial document formats that must be made available to the customer based on the customer's consent [1] is defined separately.

4.1 Data Schemas for specific FI

The Financial Information is delivered to FIU and customer as encrypted data. The FIU/AA application decrypts this data and processes it. This section defines a set of common data identifier constructs that the system will use. A list of supported FI schemas will be provided separately from this specification.

4.2 Document Specifications for Financial Information

The response containing financial information to a verified and valid consent request must contain FIP ID, Financial Information Type, and Document ID as part of the response. Further attributes like Timestamp, Consent Artefact ID, etc must also be included in the header.

- **FIP ID (`fipId`):** Each FIP will be provided with a unique identification (FIP ID) by the FSR so that all documents provided by them are accessible. It is likely that the list of unique codes will be derived via the FIP's domain URL whenever available and be published by the FSR with the ability to add new FIPs on a need basis. When URL is not available for a department, a unique (alpha) code may be assigned. Examples of FIP IDs are sbi.co.in for State Bank of India, nsdl.co.in for National Securities Depository Limited, CDSL for Central Insurance Repository Limited, etc. These codes must be unique across India and managed by the FSR.

- **Financial Information Type (`FIType`):** FSRs will decide and define the comprehensive list of Financial Information Types using pure alpha case-insensitive strings.

- **Session ID** (`sessionId`): All FI documents are generated against a session identifier.

4.3 Unsupported FI types

The system will support new financial information types which have not formally be defined in the specifications.

In situation, where an FIP integrates into the system, while a formal schema for a new `FIType` is not specified or not possible to specify, the document can still be delivered into the data section, with an referenced to a schema.

The schema could be embedded in the document with reference to the namespace.

5 Non Functional Requirements

5.1 Reliability Considerations

The systems must be designed to be highly available, scalable using a distributed architecture for vertical and horizontal scale, and high on performance.

The APIs must have high uptime and a public API Status Page must be provided by the AAs and FIPs that reports the same for each of the endpoints (along with other open data like average response time, latency, etc). Furthermore, the AAs and FIPs must implement the Heartbeat API for reporting their system uptime in real-time.

5.1.1 Failure Scenarios

This section explains how the various failure scenarios must be handled:

- Failure to Notify customer
    - In this scenario, when the Account Aggregator or FIP is not able to notify the customer on the status of the consent flow or data flow, a mechanism has to be put in place to notify the customer at a later stage. This can be achieved by reinitiating the notification message to the customer or by providing the customer an option to check the status through an application, or by providing a list of all consent flows and data flows (with status) in the application.

- Response from AA does not reach FIU
    - In this scenario, when the response sent by AA does not reach FIU, the FIUs should have a mechanism provided by AA to initiate a request to know the status of the consent flows and data flows.

- Response from AA does not reach FIP
    - In this scenario, when the response sent by AA does not reach FIP, the FIPs should have a mechanism provided by AA to initiate a request to know the status of the consent flows and data flows.

- Response from FIP does not reach AA
    - In this scenario, when the response sent by FIP does not reach AA, AA will wait for the response till the timeout period. FIP may have a mechanism to resend the response within the timeout period. If AA does not receive the response within the timeout period, AA will timeout the request and respond to customer or AA client with a timeout response.

- FIP is not available to AA

  - In this scenario, when the FIP is not available to AA, AA may have a mechanism to re-initiate the request to FIP.

- AA is not available to FIP:
  - In this scenario, when AA is not available to FIP, FIP may have a mechanism to re-initiate the request to AA.

- AA is not available to FIU
  - In this scenario, when AA is not available to FIU, FIU may have a mechanism to re-initiate the request to AA.

5.2 Security Considerations

5.2.1 Digital Identifiers

During the registration process with AA, the customer will need to established a set of validated identifiers. These validated identifiers enables the FIP with the discovery of the accounts that they may have for the customer. The NIST Digital Identity Guidelines [13] may be used to select and appropriate assurance level for enrollment and identity proofing.

There are three categories of digital identifiers, depending upon the verification mechanisms :

Type	Examples	Description
Strong Identifiers	Mobile, Email, Aadhaar	These identifiers can be verified by the means of OTP or biometric authentication and are thus considered strong identifiers.
Weak Identifiers	PAN	There is no strong mechanisms to verify that the PAN number that the customer has entered actually belongs to the customer (even though this can be manually verified).
Ancillary functional Identifiers	CRN, Account number, Folio Number	There does not exist a mechanism to verify this. These identifiers must be verified along with the Strong Identifiers, i.e., a combination of CRN and mobile number together is only verifiable in the FIP domain. The FIP should not respond only on the basis of CRN or Account Number but must verify the other Strong Identifier along with the CRN and Account number before responding with the

		masked account list.

The FIP should respond with its status of the identifiers as well. If the KYC process is performed by the FIP, then they may report these identifiers as “Strong Identifiers”.

Upon the registration, the customer also create a Customer Address [see section 2.3.1] and establish a Consent Approval PIN.

5.2.2 Customer Authentication between AA and FIP

During the Account Linking process, the customer needs to be authenticated with the FIP. The purpose of this authentication is to identify the customer who will authorize the linking of the accounts between AA and FIP. The authentication mechanism thus ensures the the right person is authorising the account linkage.

For the purpose of linking, the customer may be authenticated through any of the suggested mechanisms:

- **Approach 1**: Authenticate in FIP Domain
  The customer is redirected to the FIP and authenticates themself by entering their account credentials on the FIP interface. This redirection should happen via deep linking of the AA and FIP mobile applications and must NOT make use of Webview technology (for embedding the FIP Website in the AA app).
- **Approach 2**: Authenticate using OTP
  Customer provides Account ID of FIP and receives a one-time password (OTP) via SMS from the Financial Information Provider. The OTP SMS could be replaced by In-App Notification from FIP authorized App, TOTP, or Email. This code is then used to authenticate the customer.

There are multiple approaches to authentication and the appropriate one should be chosen based on interoperability across Account Aggregators and the Financial Information Providers, ease of implementation, security of User credentials and best possible User experience.

5.2.3 Using a secondary PIN by customer in the Consent flow

When using the Consent Approval process on the AA screen, the customer must enter the Consent Approval PIN. The AA should allow authenticated customers to change/reset the Consent Approval PIN.

5.2.4 Guidelines for API Security

Below we provide a list of security guidelines that must be followed for securing the Account Aggregator APIs. Good references for learning about managing security in REST APIs are:

- The OWASP (Open Web Application Security Project) REST Security Cheat Sheet: https://www.owasp.org/index.php/REST_Security_Cheat_Sheet
- Top 5 REST API Security Guidelines by DZone.com: https://dzone.com/articles/top-5-rest-api-security-guidelines

Here are our guidelines:

1. **Enforce HTTPS only:** All Account Aggregator APIs must enforce the use of TLS 1.1 or above in API calls and responses. This will ensure security and integrity of the financial information that is shared by Account Aggregators with requesting entities.
2. **API Keys:** API Keys should be used as the first line of defense against unauthorized API calls. API keys need to be set up before FIUs or FIPs can start making API requests to AAs.
3. **Digitally Sign API Requests:** All API requests must be digitally signed using industry-grade signature algorithms. Here are some guidelines to use when generating digital signatures in API requests
   a. Use latest cryptographic algorithms: 2048-bit RSA based signatures (e.g., RSA-PSS) or the latest elliptic curve based digital signatures (e.g., ECDSA) in groups which provide at least 256 bits of security.
   b. Use SHA-256 for hashing the requests when generating signatures. Make sure to hash query parameters in the URL as well as in the body of the API request (for PUT/POST APIs). Make sure to also include API keys as part of the content to be hashed.
   c. Use JSON Web Tokens or the W3C Signature Syntax for XML signatures to embed signatures in API requests. The digital signature should be embedded as a query parameter in the URL.
   d. Use OCSP Stapling for including public-key certificate chain information in API calls. OCSP is described here: http://www.entrust.net/knowledge-base/technote.cfm?tn=70825
4. **Digitally Sign API Responses:** The use of TLS V1.1 and above will ensure that API responses are sent in an encrypted and signed manner. For added security, it is recommended that AAs use public-key based digital signatures to sign responses. The same guidelines as in the case of API requests will apply.
5. **Rate limiting API calls:** In order to prevent denial of service attacks, API requests should be rate-limited by AAs. Appropriate error codes should be provided in responses in situations of request overload.
6. **Use validation methods:** Standard practices around input validations should be applied in order to prevent injection and other attacks. These include the following.
   a. Input Validation techniques
   b. URL Validation techniques
   c. Validate incoming content-types
   d. Validate response types

More information on validations is available in the OWASP REST Security Cheat Sheet.

7. **Use Output Encoding:**
    a. Security Headers
    b. JSON Encoding
    c. XML encoding
8. **Use HTTP response codes appropriately:** See examples in the OWASP REST Security Cheat Sheet for this.
9. **Maintain audit logs:** All API requests and responses should be logged locally by the AAs to ease detection of security threats and attacks.

Bug Bounty Programs may be organised to encourage the white-hat community to constantly monitor and proactively report possible threats to the AA APIs that could then be fixed leading to strengthened systems.

5.2.5 Customer Management and Customer Protection

Given the sensitivity of financial information, FIUs, AAs, and FIPs must put in place appropriate customer management and customer protection mechanisms:

- Customers must have provisions to lock and unlock their FIP and AA accounts for consented data access.
- Two Factor Authentication for customer of the AA is mandatory.

5.2.6 Fraud Detection and Analysis

The AAs and FIPs should put in appropriate monitoring mechanisms for Fraud Detection and Analysis. Logging is essential as that ensures traceability across systems. For example, unusual access patterns, too frequent access, over consenting, consent fatigue, and other such anomalies must be identified on a proactive basis.

5.2.7 Anonymity of FIUs when requesting information from FIPs

AA should not reveal the identity of the FIUs to FIPs in the process of requesting information from the FIPs. This is accomplished by the manner in which consent artefacts are generated in response to consent creation requests: for each request, two sets of artefacts are generated, one to support the flow of information from FIPs to AAs (these artefacts have no information about the FIUs that are requesting information) and the other to support the flow of information from AAs to FIUs (these artefacts enable *specific* FIUs to fetch information from the AAs, and thus have information about those FIUs). It is because of this separation in permissioning and data flows that FIPs are unable to learn the identities of FIUs who are requesting data from them.

5.2.8 Encryption of Financial Information

5.2.8.1 Data In-Flight Encryption

Information shared as part of the data flow will be secured using an encryption mechanism that ensures perfect forward secrecy. This means that even if any of the key materials stored at FIPs, FIUs or AA Clients (either long-term private keys or session keys) are compromised at a given point in time, data that was exchanged in the past (i.e. before that point in time) would not be possible to decipher. This is a strong guarantee of secrecy which is necessary to ensure for financial data.

We describe the mechanism here; corresponding APIs are in the appendix. The mechanism uses Diffie-Hellman Key Exchange (DHE). DHE is used in many Internet protocols (like SSH and TLS) for establishing shared secret keys between remote parties.

Encryption for AA Client

1. When making the request for data, AA client picks a set of Diffie-Hellman (DH) parameters, generates a DH key pair (dhsk(U), dhpk(U)) (which is a short-term public-private key pair) and generates a 32-byte random value, rand(U). It sends these values to AA, along with the data request via a digitally-signed API call.
2. AA ensures that the data request is in keeping with the terms of the artefact and, if so, it forwards the request to the FIP, again via a digitally-signed API call.
3. FIP checks that the consent artefact is valid (as above), that the data being requested is in keeping with the terms of the artefact and if so, it generates a fresh DH public-private key pair in the same group as specified by the FIU ((dhsk(P), dhpk(P)) and also a 32-byte random value rand(P). Using dhpk(U) and dhsk(P), it computes a DH shared key dhk(U,P) and using (dhk(U,P), rand(U), rand(P)) as key material, it computes a 256-bit session key sk(U,P) which is used to encrypt the data sent from FIP to FIU. FIP sends the public key dhpk(P), the nonce rand(P) and the encrypted data (encryption of the Financial Information to be sent under sk(U,P)) to the AA. To ensure integrity of the encrypted data, FIP also signs the entire payload (the encrypted information as well as the key materials i.e., the public key dhpk(P) and the value rand(P)) using its long-term private key before sending it to AA.
4. AA forwards the encrypted information and the key materials received to the FIU, after ensuring that the signature on these values is valid.

The DHE mechanism ensures that the shared key dh(U,P) can also be computed at the other end by the FIU using the values dhpk(P) (FIP's DH public key) and dhsk(U) (FIU's DH private key). For this reason, the FIP must accompany the encrypted data with dhpk(P) and rand(P) when sending it. All values must be digitally signed using FIP's long-term private key so that the FIU can verify the validity of the same.

At the end of the data flow, both FIU and FIP must delete all short-term key material that was generated in the process. This includes all DH key pairs, random nonces and the session key. This step is necessary for ensuring forward secrecy.

Encryption for AA application

The exact same flow would work except that all actions performed by the FIU would instead be performed by the AA app on the customer's phone. The following guidelines are to be followed in implementing the AA app, if the AA decides to offer the Financial Information aggregation functionality:

1. DHE key pairs must be generated localling on the customer's phone and the private keys from the DHE key pairs must never be communicated to the AA server.
2. The decryption of the customer's data must also take place on the customer's phone and the decrypted data (customer's financial information) must never be communicated to the AA server.
3. As stated above, the private keys must be deleted from the customer's phone at the end of the data flow.

The AA app should be implemented in a manner such that it can be easily verified (by an auditor) that the above three guidelines are followed.

Encryption for Periodic data access

For encrypting data in the case of periodic data access, FIUs and FIPs set up shared keys for a period of usage via a single exchange. A period is a series of multiple data accesses which is defined as follows: if the frequency of data access is WEEKLY or less frequent, the period should be set as 3 months; otherwise, the period should be set as frequency, multiplied by 12.

1. At the beginning of each period, FIU generates n key pairs (dhsk(U)[1], dhpk(U)[1]), … , (dhsk(U)[n], dhpk(U)[n]) where n is the number of data accesses in that period. It generates a random nonce rand(U) and sends the selected DH parameters, the value n, the n DH public keys dhpk(U)[1..n], the start-date and end-date of the period, the value rand(U) and the consent artefact to AA via a digitally-signed API call.
2. AA forwards the same, after validation, to FIP via a digitally-signed API call.
3. FIP stores the DH key pairs and rand(U) (and other fields).

For the "i"th instance of data access in a period (i ranging from 1 to n), FIP generates a fresh DH key pair (dhsk(P)[i], dhpk(P)[i]) and a random nonce rand(P)[i] and computes a DH shared key dhk(U,P)[i] and a session key sk(U,P)[i] using these values and the "i"th public key shared by FIU (i.e. dhpk(U)[i]) earlier. The data encryption and transmission then happens as usual, after which the DH keys dhsk(U)[i], dhsk(P)[i], and the session key sk(U,P) are deleted by the respective entities.

Choice of Diffie-Hellman parameters
DHE will be performed over Elliptic Curve Cryptography (ECC) groups. We recommend the use of Curve25519, which is used in DHE implementations in a lot of protocols like SSH and WhatsApp.

5.2.8.2 Data At-Rest Encryption

The customer data and metadata in AA must be encrypted using a symmetric key. These keys can be rotated from time to time and can be managed through a Key Management Service.

5.2.8.3 Controlling access to financial information by account aggregators

Financial information must only be accessible to the customer with whom the information is linked and account aggregators should not be allowed to view or store such information. Part of this objective is achieved via data in-flight encryption. Furthermore, if the account aggregator provides an app (a mobile app or a desktop app) through which the customer requests for FI, certain measures must be in place when implementing this app:

- The app may receive financial information from FIPs in encrypted form and decrypt such information, but it is not allowed to relay such information back over the network (e.g., it can communicate this information to a server maintained by the account aggregator).
- The app must follow strong API security guidelines as outlined in this document

5.3 Audit Considerations

All events (consent created, consent revoked, data requested, data denied, data sent, etc) in the consent flow and data flow and corresponding system requests and responses between FIUs, AAs, and FIPs must be digitally signed and logged to ensure immutability, non tamperability, and non repudiability.

AAs, FIUs and FIPs need to persist the logs for certain period of time so that they can be retrieved when necessary and this audit trail must be made transparency available to the customer. To ensure integrity, logs cannot be edited - they can only be appended.

5.4 Privacy Considerations

5.4.1 Data Masking and Identity Protection Guidelines

There are three levels of information access:

- Standardised Lookups
- Standard Financial Information Templates by Purpose
- Custom Financial Information

There are three levels of identity visibility:

- Hidden (Not Visible)
- Masked (Partially Visible)
- Completely Visible

Here are a basic set of data masking and identity protection rules that need to be followed to ensure that privacy is maintained:

- Tokenization: Account numbers, card numbers, phone numbers, personal identifiers (PAN, Aadhaar, etc.) should be tokenized using Virtual IDs issued by the FIU, AA, and FIP (as defined in the Customer Identifier section of the Consent Artefact XML).
- Data Masking - Masking Out: For instance, only the last four digits of a credit card number involved in a transaction may be revealed - XXXX XXXX XXXX 1564. Data Masking may be static, on-the-fly, or dynamic.

Note: A comprehensive list of data masking and identity protection rules may be further decided by the respective FSR, after which a Data Masking and Identity Protection Guidelines Document for Financial Information shall be published.

5.4.2 Data Portability Guidelines

The customer must be able to seamlessly transition from one NBFC AA to another by porting their NBFC AA account data and corresponding consent artefacts.

5.5 Consumer Experience Considerations

The user interfaces must be aesthetically designed, secure, honest, unobtrusive, understandable, useful, and an enabler of informed decisions.

The NBFC AA must provide mechanisms for customers to access the services via a desktop or laptop browser (web application), smartphone (mobile application), or feature phones. For ease of FIU integration, an SDK may be provided by the AA. New Customer Registration and subsequent linking of FIP accounts must take place in the environment of an AA (AA’s mobile app, web app, etc).

The AA must provide a User-friendly interface for customers to access a record of the consents provided by them and the FIUs with whom the information has been shared, recurring consent artefacts, and the ability to revoke (permanent) or pause (temporary) a consent artefact.

5.6 Developer Experience Considerations

In order to ensure easy and seamless consumption of these APIs by developers for the purpose of development (integration), it's important that the developer experience for the APIs exposed by FIPs and AAs be given prime importance.

The APIs should be developer friendly and at minimum the following considerations must be met:

- Developer Portal: It must be publicly accessible and must contain:
    - API Sandbox
    - API Documentation and Reference
    - Quickstart Guides
    - Open Source Libraries and SDKs

FIPs and AAs may further engage with developers via hackathons and other feedback channels like a Developer Forum or StackOverflow.

5.7 Grievance Redressal

There must be a dispute resolution mechanism in place by FIUs, AAs, and FIPs to route complaints digitally and redress grievances of the customer. This improves customer satisfaction and builds trust. Prompt and efficient service is essential to retaining existing customer relationships.

The customers may record their grievances / provide their feedback in writing, verbally, or digitally. SLAs must be put in place to ensure prompt response and necessary escalations in case of delays. Grievance Redressal can be further enabled through the use of detailed status and error messages in response to each request.

6 Appendix

6.1 Notifications

Appropriate Notifications have to be sent to all parties following any actions. Notification can be delivered through Email, SMS, Callback URLs, or In-app Notifications. Each notification can have different payloads and the payload of the event may vary based on the channel.

The following sections show the various account linking, consent and data lifecycle events for which the system will generate notification. The column M/O, specifies whether the customer should be sent a notification, where “M” means “Mandatory” and “O” means “Optional”. The other notifications to entities must be sent for auditing, logging and state management purposes.

6.1.1 Account Linking Lifecycle Events

Account Linking Lifecycle Events				
Notifications	**M/O**	**Sender**	**Receiver**	**Based on action performed by**
Account Discovery	O	FIP	customer	customer
Account Linked	M	FIP	customer	customer
Account Delinked	M	FIP	customer	customer

Static notification could be provided to the customers on their registered emails, mobile number or via in-app notifications.

6.1.2 Consent Lifecycle Events

Notifications	M/O	Sender	Receiver	Based on actions performed by	Payload contains
Consent Requested	M	AA	customer	FIU requested for consent	Time of request, FIU details
Consent Approved	M	AA	FIU	Customer approved the consent request	Time of request, customer’s details

				by FIU	
Consent Revoked	M	AA	FIU, FIP	Customer revoked the consent	Time of revoke, Revoker details, Reason for Revoke
		FIP	AA	FIP revoked the consent	Time of Revoke, Revoker details, Reason for Revoke
		AA	FIU, Customer	FIP revoked the consent	Time of revoke, Revoker details, Reason for Revoke
Consent Paused	M	AA	FIU, FIP	Customer paused the consent	Time of pause, Customer details, Reason for pause
		FIP	AA	FIP paused the consent	Time of pause, FIP details, Reason for Pause
		FIP	FIU, Customer	FIP paused the consent	Time of pause, FIP details, Reason for Pause
Consent Expired	M	AA	FIU, FIP		Expiry date

The first time a consent is created it will go into activated state.

6.1.3 Data Lifecycle Events

Data Lifecycle Events				
Notification	**M/O**	**Sender**	**Receiver**	**Based on action performed by**
FI Requested	O	AA	Customer	Customer
	O	FIP	Customer	AA
	O	AA	Customer	FIU
FI Ready	M	AA	Customer, FIU	AA
	M	FIP	Customer, AA	FIP

FI Denied	O	AA	Customer, FIU	AA
	O	FIP	Customer, AA	FIP
FI Purged	M	FIU	AA	FIU

6.1.4 Data Availability Notifications

Data Availability Notifications		
From	**To**	**Description**
FIP	AA	The requested data is generated and FIP notifies the AA to retrieve the requested data.
AA	FIU	For every FIP that the AA receives data in an aggregation process, it sends a notification to FIU.
AA	Customer	AA pushes the data to customer's data delivery destination and notifies the customer.

6.2 Summary of APIs by Entity

These API specifications cover all the entities within the account aggregator ecosystem to facilitate seamless integration between ecosystem partners.

Technical Specifications for API Digital Signatures
All API requests and responses must be digitally signed by the respective organization initiating the APIs. The digital signature should follow W3C standards for XML and IETF standards for JSON. It should include information about the public key of the entity creating the signature and the associated certificates or certificate chains required for signature verification. Certificate chains can be included as part of the signature (e.g., the W3C standard has the option of including certificates in the “KeyInfo” element of the signature) or a URI for the certificate chain can be provided. This approach ensures that when a public key changes, the updated key and certificate are communicated to the party that needs to verify the signature. CA public keys should be managed as in any digital signature application.

XML Format: Digital Signature XML element must adhere to the W3C Standards - https://www.w3.org/TR/xmldsig-core/

6.2.1 Central Registry - Financial Sector Regulator Metadata

The registry is maintained by each FSR (or a common entity nominated by the respective FSRs) for ensuring all licensed FIPs and AAs are identified, discovered, and trusted by the ecosystem. FIPs and AAs will need be given an account on the application where the registry is maintained for managing their profile, public keys, and other details. The registry would be made available at a publicly accessible URL.

Entity		**Central Registry**
Method	API Path	Description
Registry Query		
GET	/Registry	It allows ecosystem partners to fetch details about all the FIUs, FIPs and AAs registered with the regulator and obtain their respective certificates.

6.2.2 Account Aggregator

Entity		**Account Aggregator**
Method	API Path	Description
Consent Flow		
POST	/Consents	This API is intended for the FIU to obtain digitally signed consent artefacts. Once the customer approves the consent request, AA generates the digitally signed consent artefacts and shares them with the FIU.

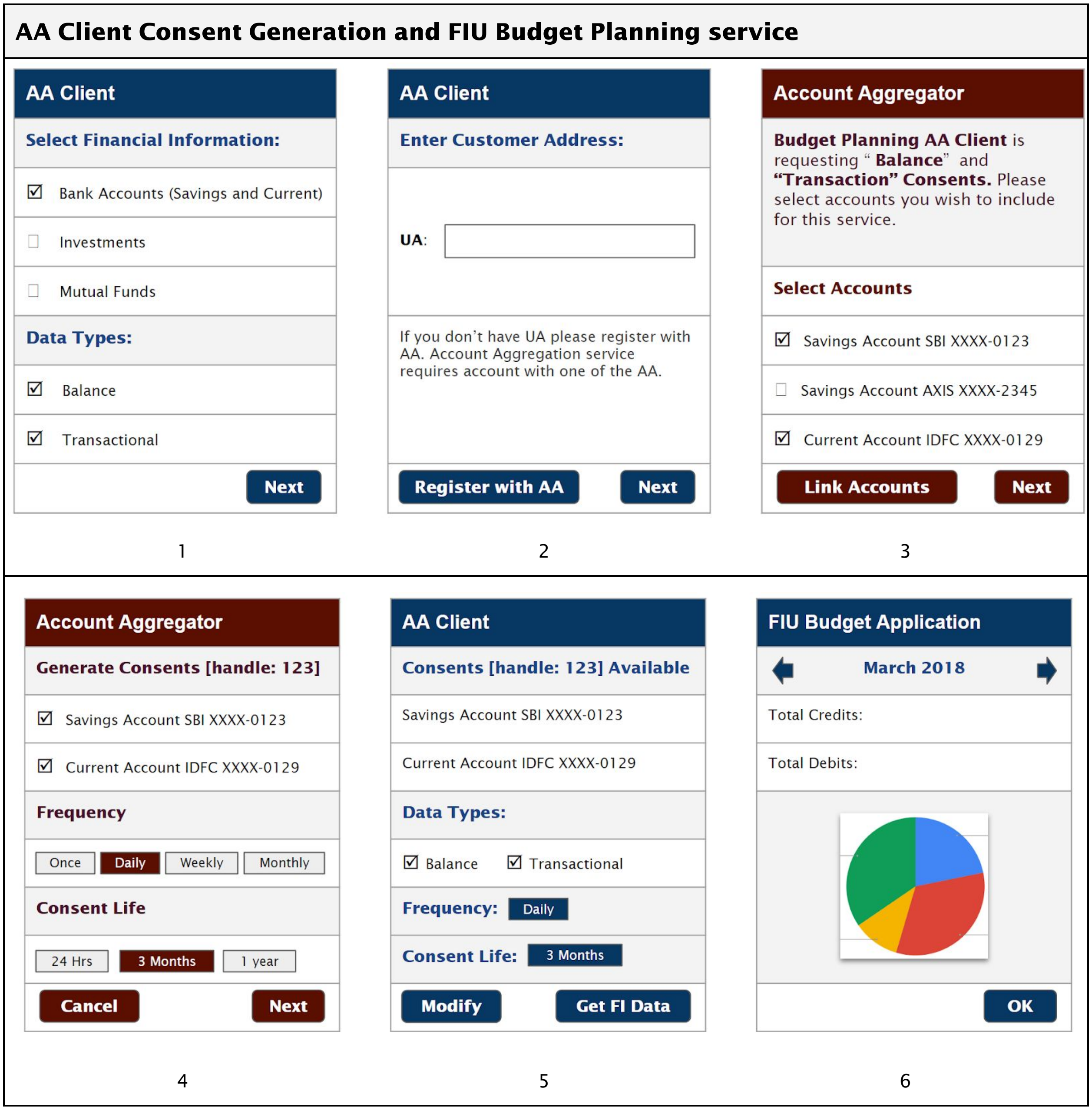
GET	/Consents/{consentsHandle}	Check status of a previously submitted Consent Artefacts creation request
GET	/Consents/Consent/{id}	This API is intended for fetching the consent artefact (and related information) associated with the given consent ID. The method will return only consents that have been created by the requester.
Data Flow		
POST	/FI/request	The FIU or the customer submits the Consent IDs of the consents required for fetching financial information from the FIP(s). A set of sessionIds are generated and returned. These SessionIDs enable the FIU or the AA client to fetch the information from the AA once available.
GET	/FI/fetch/{sessionId}	This API is used by the FIUs to fetch the financial information from the AA against a given SessionID. It is invoked after the FIU receives the <FI-Ready> notification from the AA.
Notifications		
POST	/Notification	This API is used by the FIPs and FIUs to submit notifications to the AA. In particular, this includes the notification (from FIPs) for availability of financial information in the data flow and the notification for account linking in the linkage flow. It also includes the notification for purging of data from FIUs.
Monitoring		
GET	/Heartbeat	This API is used by FIUs to check availability of AAs

6.2.3 Financial Information Provider

Entity		Financial Information Provider
Account Discovery and Linking		
POST	/Accounts	This method enables an AA to discover accounts belonging to a customer based on the customer's identifiers.
PUT	/Accounts/{accountRefId}	This API is used for establishing linkage (in the AA domain) of the customer's discovered account.
Data Flow		
POST	/FI/request	The AA submits the Consents for requesting the Financial Information from the FIP (and forwarding to the FIU or customer subsequently). A set of sessionIds will be generated, which would enable the AA to fetch the information once available.
GET	/FI/fetch/{sessionId}	This API is used to fetch the financial information from the FIP for a given SessionID. It is to be invoked after the AA has received the <FI-Ready> notification from the FIP.
Notification		
POST	/Notification	Notifies FIP of the Consent's status
Monitoring		
GET	/Heartbeat	This API is used by the AAs to check availability of FIPs

6.3 Example Application

The following functional example illustrates an usage scenario for the AA service.



AA Client Consent Generation and FIU Budget Planning service

AA Client

Select Financial Information:

☑ Bank Accounts (Savings and Current)

□ Investments

□ Mutual Funds

Data Types:

☑ Balance

☑ Transactional

AA Client

Enter Customer Address:

UA:

If you don't have UA please register with AA. Account Aggregation service requires account with one of the AA.

Account Aggregator

Budget Planning AA Client is requesting " **Balance**" and **"Transaction" Consents.** Please select accounts you wish to include for this service.

Select Accounts

☑ Savings Account SBI XXXX-0123

□ Savings Account AXIS XXXX-2345

☑ Current Account IDFC XXXX-0129

Account Aggregator

Generate Consents [handle: 123]

☑ Savings Account SBI XXXX-0123

☑ Current Account IDFC XXXX-0129

Frequency

Once [✓ Daily] Weekly Monthly

Consent Life

24 Hrs [✓ 3 Months] 1 year

AA Client

Consents [handle: 123] Available

Savings Account SBI XXXX-0123

Current Account IDFC XXXX-0129

Data Types:

☑ Balance ☑ Transactional

Frequency: Daily

Consent Life: 3 Months

FIU Budget Application

March 2018

Total Credits:

Total Debits:

In the example above, an authenticated customer is using an AA client application and wants to make the aggregated financial information available to the FIU service application.

(1) The customer starts the selection of financial information. The AA client may be customized to determine which `FIType(s)` and what kind of financial information types will the service need and accordingly present a screen to the customer.

(2) Once the customer makes her choices on screen (1) and clicks “Next”, the AA client asks for Customer Address associated with the customer’s account with AA. The customer enters her Customer Address and clicks “Next”. The AA client send a request to the AA. AA generates a `consentHandle` and provides to AA client for subsequent updates and status callbacks.

(3) The AA may use varieties of means, such as Push Notification (in case customer has installed and using the AA Mobile Application), Emails (in case the AA offers a web application) etc. The customer switches to the AA application for Consent generation. The AA application may use a variety of authenticators to enable customer to log in the AA application. Once logged in, the AA application presents a list of filtered linked accounts matching the `FIType(s)` requested by AA client.

(4) The AA builds a Consent generation confirmation screen for the customer to select the accounts to be included for the account aggregation service. The customer confirms the account selection and accepts Consents Artefact creations. For assurance, the customer may be asked to enter Memorized Secret [13], Lookup Secret or other form of second factor confirmation. The AA will notify the AA client/FIU about the successful Consent(s) creation using the callback notification interface of the AA client/FIU.

(5) The context switches to AA client application. The AA client application generates cryptographic primitives required for encrypted FI data retrieval and request AA for aggregating the FI Data. The AA will request aggregation of the data from the corresponding FIP using the Consent Artefacts. AA will notify the FIU application when FI data becomes available.

(6) The FIU will Fetch the FI data from AA once it receives notification that the data is ready. It will decrypt the retrieved FI data and provides the necessary views and services to the Customer.

The above examples are illustrative, the FIU and AA may present innovative UI/UX to enrich the experience of the customer. The FIU and AA application must provide adequate security through use of appropriate authenticators and use of secure authentication protocols.

6.4 Registering a Purpose Code

The following form may be used to submit the purpose registration code:

Code	<<will be assigned>>
Category	The category of service
Short Text	
Description	

Custom code range is defined between the range of [2001-9999]. If a FIU wants to use a custom code, it should register this code by emailing the SDO at sdo@rebit.org.in.