Technology Architecture Documentation for Digital Addressing Project

DATA FOR PUBLIC GOOD

Document Number: CDPG/FSID/2025/12V1.0 Date: 18/06/2025

Content

Glossary

Sr. no.	Term	Description
1.	Address Attribute Registries (AAR)	AARs are used by AIPs to fetch verified address attributes based on a DIGIPIN
2.	Authorized Address Validation Agency (AAVA)	AAVA carry out limited physical verification with the user consent on whether the information associated with the Digital Address corresponds to the actual locatable place
3.	Address Information Agent (AIA)	AIAs oversee user consent processes and offer a clear, intuitive interface that allows users to create, update, and manage their Digital Addresses. Acting on a user's behalf, AIAs work with AIPs to ensure that address information remains accurate and can be altered or revoked when necessary. They also deliver an authorization framework that grants AIUs access to address details solely under proper user consent.
4.	Address Information Provider (AIP)	AIPs maintain the digital address registry, which includes core address data and any associated verification details. They also track which Address Information Agent (AIAs) supports each Digital Address (DA). By keeping the registry current and secure, AIPs guarantee that only authorized parties can access accurate and up-to-date address information.
5.	Address Information User (AIU)	AIUs directly interact with users, offering services—such as deliveries or location-based support—that rely on the DAP's digital addresses. They access address details through the framework established by the Central Mapper (CM) and AIPs, always ensuring they obtain and honor appropriate user consent.
6.	Central Mapper (CM)	The CM is responsible for managing suffixes used by Address Information Providers (AIPs), maintaining a comprehensive registry of all DAP stakeholders, and enabling efficient discovery among them. By standardizing the structure of digital addresses and housing a complete stakeholder directory, the CM

		ensures interoperability and simplifies collaboration among various entities.
7.	Digital Address (DA)	The Digital Address is a unique and customized label (such as ***username@domain***) to represent the user's DIGIPIN and descriptive addresses.
8.	Digital Address Network (DAN)	Digital Address Network (DAN) is composed of multiple interconnected entities, each playing a specific role in the management and resolution of Digital Addresses (DAs).
9.	Digital Address Project (DAP)	A Digital Public Infrastructure (DPI) which is being designed to allow users to create, access, share, manage and use their address information.
10.	DIGIPIN	DIGIPIN is an open-source national level addressing grid that divides India into approximately 4m x 4m grids and assigns each grid a unique 10-character alphanumeric code based on latitude and longitude coordinates
11.	User	Person or an Organisation who uses Digital Address Service

1. Intended Audience

The document is intended for technical audiences such as domain experts, technical architects, project managers, etc.

2. Purpose and Scope

The Department of Post has identified the need to create the 'Technology Architecture Documentation for the 'Digital Addressing Project'. Center of Data for Public Good (CDPG), is a Program unit within Foundation of Science Innovation and Development (FSID), Indian Institute of Science (IISc), Bengaluru, India, has been identified as the responsible entity for the 'Technology Architecture Documentation' for this. The purpose of this document is to define the Technical Architecture for the 'Digital Address Project'

This document provides a clear and comprehensive view of the proposed DAP architecture. It highlights design principles, proposed interfaces, interactions and dependencies between different components.

3. Introduction

3.1. Motivation

Traditional addressing systems in India suffer from various inconsistencies in format - structural issues, missing information, multiple ways of representing the same information and a reliance on landmarks or localities. The existence of multiple places with similar names within a city and unmapped or informal settlements in rural areas further compound the problem. .

Integrating these styles of addresses with modern technology also poses significant challenges, thus hindering the adoption of automation, logistical optimization, advances in the GIS space etc. to improve delivery efficiency. Additionally, expanding traditional addressing to adapt to the growing demands of smart cities and the ever evolving digital landscape requires considerable infrastructural and administrative efforts.

Traditional addresses are used almost universally for e-commerce, postal deliveries, KYC in banks etc. The ambiguities introduced by these addresses cause issues during service or item delivery - delays, resorting to manual intervention with recipient, loss of items - leading to an increase of operational costs incurred by the service provider and a poor user experience for the service consumer. A significant source of frustration for service consumers is manual entry of address information on every new service they wish to use, and updating addresses on these services due to a change of residence or loss of landmarks [1].

To overcome the inefficiencies of the current addressing system, the Department of Posts (DoP) is developing the Digital Address Project (DAP)—a pioneering initiative designed to modernize India's addressing framework by incorporating GIS and allowing management and consent-based sharing of addresses

to service providers. The DAP achieves this through two key components: the digital postal index number (DIGIPIN) and the digital address ID (Digital Address).

3.2 DAP as an Address Management System

In support of such modernization, DAP should be seen as a comprehensive address information management system. The DAP shall be envisioned as the backbone for organizing, validating, and updating address-related data in a standardized, interoperable and secure format. As the system evolves, DAP should enable the integration of traditional and digital addresses by creating structured, address data that can be used across government and private entities.

This system would ensure seamless updates in case of administrative changes, support last-mile delivery even in remote or informal settlements, and allow real-time access to verified address data.

3.3 DAP as a Digital Public Infrastructure

These two components; DIGIPIN and Digital Address are envisaged as the foundational elements of the Digital Public Infrastructure (DPI). These technologies have the potential to serve as critical enablers of a wide range of public and private services, much like Aadhaar and UPI. As a DPI, DAP must be designed with principles of interoperability, openness, scalability, and privacy at their core. This would allow seamless integration with other digital platforms such as financial services, e-commerce, and disaster management systems.

By institutionalizing DIGIPIN and Digital Address as part of India's DPI ecosystem, the government can ensure standardized and inclusive access to address-related services, foster innovation among service providers, and create a robust digital backbone to support the vision of a connected and digitally empowered India.

3.4 Design Principles for DAP

The framework outlined in this document operates on the following guiding principles:

- **Technology Agnostic:** The Digital Address (DA) architecture shall be designed to be independent of specific technologies, programming languages, or platforms. The architecture shall aim to facilitate seamless and secure electronic data flow among diverse stakeholders by remaining technology agnostic.
- **Reliability:** Systems within the DAP shall be engineered to prioritize reliability, ensuring consistent software operation over defined periods and environments. Minimizing the impact of system failures on interconnected systems and facilitating swift recovery are integral aspects of the design.
- **Scalable by design:** DAP components shall be designed to be scalable. A federated design approach is suggested where multiple AIUs, AIAs and AIPs can co-exist by design thus reducing the possibility of data bottlenecks.

Additionally, the architecture allows for the scalable expansion of individual components as and when needed.

- **Privacy by Design:** Privacy considerations shall be integrated into the design and engineering phases from inception. Data exchange mechanisms within the DAP shall be designed to respect user privacy, incorporating electronic consent mechanisms and maintaining a non-repudiable audit trail.
- **Security by Design:** Secure by design indicates that security is incorporated in design of all the components from the ground up. The DAP shall prioritise security at every level of software and system design. End-to-end data security, utilizing Transport Layer Security (TLS), ensures data-centric protection. All software components in DAP shall be secure by design and follow the security best practices in component design and implementations.
- **User-Centric Approach:** Emphasizing user's experience and usability, the DAP implementation shall simplify interactions and enhance access to data and services for users. In addition, DAP shall take into account the key stakeholders' namely AIA, AIU, AIP and CM's concerns, and simplify their interactions amongst themselves.
- **Consent-Driven Architecture:** Data sharing is contingent upon explicit consent from users, ensuring transparency and trust. DAP preserves the privacy of data by ensuring that the data is shared, created, managed, updated only if the consent is provided by the user.
- **Open APIs for Interoperability:** The system shall use standardized programmatic interfaces (Open APIs) to promote interoperability, functional extensibility, facilitating seamless sharing and access to digital resources across various devices, form factors, and networks.
- **Open source:** DAP shall be designed to be open-source. It shall use leading tools, technologies from the open source industry in development and shall not use any proprietary tools and services.
- **Cloud agnostic:** DAP shall be designed for cloud deployment and shall be capable of utilizing the state-of-the-art cloud infrastructure. In addition, DAP shall be designed to ensure that the platform can operate efficiently across any cloud infrastructure. By adhering to cloud agnosticism, the DAP can prioritize flexibility and interoperability, empowering stakeholders to deploy the platform seamlessly across various cloud environments without encountering compatibility issues.
- **Minimalistic by design:** DAP aims to be inclusive hence the APIs are designed to be minimalistic and domain agnostic.
- **Accountability:** DAP ensures accountability of transactions carried out by various stakeholders for all the transactions that require authentication and authorization
- **Unbundling:** Unbundling implies breaking up a complex task into smaller micro services or tasks. This enables efficient and robust design and implementations. DAP shall follow unbundling by breaking up the services into simpler interfaces into multiple microservices for ease of implementation and deployment.

- **Extensibility, modularity and service orientation:** The design of DAP shall be extensible, modular and shall incorporate service-oriented designs. This shall help in scaling up/down without affecting the other components and allows different components to be designed and developed independently.

4. DIGIPIN

The Department of Posts has undertaken an initiative to establish a Digital Public Infrastructure (DPI) for a standardized, geo-coded addressing system in India. As a part of this initiative, the Department has finalised DIGIPIN – the foundation layer of the DPI. This initiative seeks to provide simplified addressing solutions for seamless delivery of public and private services and to enable "Address as a Service" (AaaS) across the country. DIGIPIN is an open-source national level addressing grid developed by Department of Posts in collaboration with IIT Hyderabad and NRSC, ISRO and is a key component of the digital address ecosystem. The advent of DIGIPIN will mark a revolutionary step in India's journey towards digital transformation by bridging the crucial gap between physical locations and their digital representation.

DIGIPIN divides India into approx. 4m x 4m grids and assigns each grid a unique 10-character alphanumeric code based on latitude and longitude coordinates [2].

5. Digital Address

Alongside the DIGIPIN layer, the DAP proposes a user-friendly Digital Address Layer to enable users to create unique, customizable identifiers for their addresses to simplify management and sharing of their addresses — similar to how UPI IDs simplify banking.

5.1. Defining Digital Address

Digital Addresses (DAs) are human-friendly labels that encapsulate address information. A DA resembles an email or UPI address (e.g., *name@suffix*) and maps to two key components: a DIGIPIN, which encodes geospatial data of the location and a descriptive address for added context. The descriptive address may have its attributes structured in a well-known format that is machine readable. All systems storing and maintaining Digital Addresses will be required to use a particular descriptive address format. The format can be an attribute of the DA to ensure interoperability. Each DA may also include verification details, providing insight into the relevance and accuracy of the encoded address information. Each DA may also have optional validity information (valid until timestamp) which enables temporary digital addresses to be created by users. Users can manage, update, share, or revoke access to their Digital Address through a unified interface. DAs eliminate the need to repeatedly enter detailed address information and allow users to share location coordinates without recalling the full address and associated DIGIPIN. The entire system will be consent-driven, with strong privacy and user-control features detailed later [3]. The DA and the attributes when stored in AIP and shared with AIU shall have a standard format and schema to ensure interoperability amongst the DAN components.

5.2. Digital Address Format

In this section the definition of different formats for the digital address are proposed. The allowed character set for digital addresses are currently restricted to alphanumeric characters in ASCII. However, in future this may be expanded to include regional characters for inclusivity purposes. This is in alignment with the current UPI Address conventions[4].

Figure 1 shows a EBNF [5] syntax diagram visually defining the rules for constructing a digital address. A digital address consists of a **name** followed by the "@" symbol and a **suffix**. The name and suffix are composed of one or more words, which may themselves be separated by dots. A word is a sequence of valid characters, which can be lowercase letters (a–z), uppercase letters (A–Z), or digits (0–9).

When creating a Digital Address, the name portion of the address can be chosen by the User, while the suffix must be chosen from a pre-defined list of suffixes managed by the Address Information provider, which is described in the next section. The name portion of the address can also be system assigned and not chosen by the User, or it can be derived using the provided user information. The combination of name and suffix must be unique across the system.

This structured approach ensures that digital addresses follow a consistent, predictable format suitable for systems that require unique, alphanumeric identifiers.

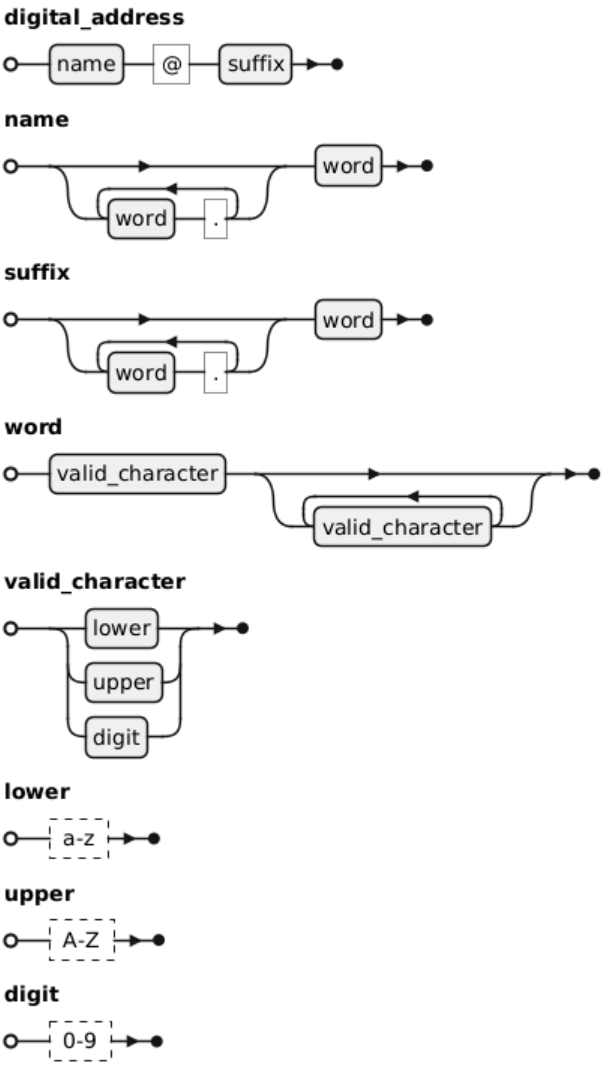


Fig.1 Syntax for the Digital Address

5.2.1. System-assigned vs. User-defined Digital Addresses

Individual AIPs may choose to allow users to choose the name part of the Digital address or have it be generated by the AIA based on information provided by the User (similar to UPI IDs where users are nudged to use their mobile numbers as their UPI IDs). AIPs can also choose to have system-assigned addresses - where the AIA assigns a random name to the DA to be memorable and inoffensive, giving users no choice to create their own DAs. A comparison of both styles of address assignment is given below.

Dimension	System assigned DA	User defined DA
Privacy preserving	System-assigned DAs can be created such that no private information of the User is leaked with the name and suffix combination.	Users cannot be stopped from including sensitive information in the name part of their DA. This may raise privacy concerns.
Memorability	Using a combination of random numbers or English alphabets in the DA may be difficult for a User to remember. Using a combination of short words from a non-offensive English word list may solve the latter, but there is no guarantee that all strata of society will make DAs of that nature easy to remember.	Users can choose memorable and personal names when creating their DA.
Monetization opportunities	There is no scope for monetization of certain name and suffix combinations.	Users may pay for certain unique name and suffix combinations that are personal to them.

5.3 Components of Digital Address Project

Below is a description of the key stakeholders and components in the Digital Address Project (DAP), illustrating how each role contributes to a secure and user-friendly ecosystem:

1. **Central Mapper (CM):**
   The CM is responsible for managing suffixes used by Address Information Providers (AIPs), maintaining a comprehensive registry of all DAP stakeholders, and enabling efficient discovery among them. By standardizing the structure of digital addresses and housing a complete stakeholder directory, the CM ensures interoperability and simplifies collaboration among various entities. As the DAP evolves, there is scope for multiple Central Mappers to be organized in a federated parent-child structure, where the parent Central Mapper allots certain suffixes to its child Central Mappers, so that suffix management can be distributed.

2. **Address Information Users (AIUs):**
   AIUs directly interact with users, offering services—such as deliveries or location-based support—that rely on the DAP's digital addresses. They access address details through the framework established by the CM and AIPs, always ensuring they obtain and honor appropriate user consent.

3. **Address Information Providers (AIPs):**
   AIPs maintain the digital address registry scoped by suffixes, which includes core address data and any associated verification details. Digital Address (DA) suffixes are assigned to AIPs by the Central Mapper (CM). An AIP is responsible for managing DAs created with their assigned suffixes. They also track which Address Information Agent (AIAs) supports each Digital Address (DA). By keeping the registry current and secure, AIPs guarantee that only authorized parties can access accurate and up-to-date address information. In certain scenarios, the AIP may act as an AIU to independently provide services to the users. For instance, the Department of Post can be an AIP while also using the information stored with them as an AIU providing delivery services. In such scenarios the normal consent workflows may be bypassed. However, if a certain AIP acting as an AIU needs to resolve a DA which is managed by a different AIP, then the normal consent workflows are applicable.

4. **Address Information Agent (AIAs):**
   AIAs oversee user consent processes and offer a clear, intuitive interface that allows users to create, update, and manage their DAs. Acting on a user's behalf, AIAs work with AIPs to ensure that address information remains accurate and can be altered or revoked when necessary. They also deliver an authorization framework that grants AIUs access to address details solely under proper user consent. A user may also choose to change the AIA associated to a DA through a migration process.

Together, these four components establish a robust foundation for the DAP, prioritizing privacy, accuracy, and interoperability in the provision and use of digital addresses.

5.4. Digital Address Attributes

The following table lists out some of the suggested attributes associated with a Digital Address. These attributes are stored by the AIP in their digital address registry. The attributes listed can be expanded or omitted as per the requirements of individual AIPs catering to different sectors and use cases.

Attribute	Description
Digital Address	The full digital address according the format specified above

DIGIPIN	The geocoded location information of the Digital Address
Descriptive Address	Fields containing the postal address attributes such as building details, street details, city, district, state, pincode etc.
Descriptive Address Format	The identifier of the format in which the descriptive address attributes are structured
Verifications	Fields containing the verification and the quality metrics of the location information such as physical verification information, confidence scores etc.
Validity Information	Fields specifying whether the digital address has any validity information such as an expiry timestamp, one time usage etc.
Reachability	Fields specifying any reachability characteristics of the location such as accessible to cargo vehicles, pedestrian friendly etc.
……	SCOPE FOR EXPANSION

Table 1: Attributes of a Digital Address with a scope for expansion

5.5. Digital Address Types and suggested business models

Digital Addresses may be classified into different types where the classification is made depending on the suffix and the associated AIP that may manage the suffix. Each type of DA can inform a business model for their associated AIPs that would be essential for the long-term sustainability of the DAP.

The types of DAs listed in Table 2 are intended as an example. The precise way DA types and associated AIPs will emerge will be determined by many techno-economic-regulatory factors. The technical architecture outlined in this document permits many different models.

Table 2 lists out the different potential Digital Address types, the example suffixes that each DA can have, the nature of the AIP who may administer the suffix associated with the DA, the business model the AIP may choose to use to be financially viable and the assignment policy the AIP may choose to use to assign DAs to Users respectively.

The choice of words for suffixes is to be decided by the DAP governance entity. SOPs may be created to determine how a new suffix is introduced and the steps required for an AIP to assign a Digital Address with that suffix. The DAP governance entity might specify operational policies to avoid words that may lead to privacy leaks when used in a Digital Address. The suffixes listed in Table 2 are only examples and may not be used in practice.

Digital Address type	Examples of suffixes	Nature of associated AIP	Business model of the AIP	Digital address assignment policy
National	*@gov, @dop, @mot*	Public sector authorized	Funded by govt	Validate addresses based on org affiliation
State	*@ka, @tn, @police.ka*	Public sector authorized	Funded by govt	Validate addresses based on org affiliation
High Value	*@home, @work, @office, @school*	Private sector (licensed from CM)	Revenue from licensing, payment to the CM	Have you paid?
Organizational	*@iisc, @xyzcompany, @indianrailways*	Private sector, academic, PSU	Payment to CM	Privately managed. Usually based on org. affiliation
Everyman	*@pincode, @passportoffice, @bankname, @aadhaaroffice*	Public or private sector	Service to customers, free offering	Member of bank, name choices may be structured or may be limited
Service provider	*@amazon, @swiggy*	Private sector	Assigned to customers to improve their efficiency. Payment to the CM	May be based on membership (e.g. Amazon Prime)

Table 2: Suggested Digital Address types

In order for the DAP to be financially sustainable, the Central Mapper and AIPs need to strategize and explore monetization options for certain flows in the DAP system. For e.g.

- The CM can lease out suffixes to private sector AIPs for a number of years at some monetary value. This may not be possible for sensitive suffixes such as *@gov* or *@goi*. Instead the CM may choose to allocate such suffixes to trusted AIPs who are able to adhere to strict operational guidelines and policies issued by the DAP governance entity.
- AIPs may allow Users to pay for popular or personal name values when creating their DAs
- AIPs may also charge AIUs a small amount for every DA resolution. The amount itself would be insignificant to an AIU when compared to the benefits that the DAP and DAs would provide to an AIU's service

5.5.1. Considerations on a uniform suffix

It may be desired to have a uniform suffix for all DAs created for branding and awareness purposes. However, this approach does not align with the present technical architecture. Suffix resolution as a concept would no longer be applicable since there is only one suffix and the CM's role in the DAN expands to more than just a suffix-to-AIP 'routing system'. With only one suffix, the CM would have to contain information of each and every DA created and the AIP it is associated with. This new role of the CM has potential security, storage and scalability concerns. Having multiple suffixes in the system not only negates the aforementioned concerns, but also carries the potential for monetization as highlighted in this section.

Instead, it is proposed to create a bespoke AIP that manages the suffix '*@indiapost*' or '*@dop*' early on in the development of the DAP to encourage Users to create their first DA with that suffix. Also, the governance entity in charge of the Central Mapper may choose to append a tag to every suffix. For e.g., all suffixes may include the tag .dop (*@home.dop*, *@work.dop*, *@xyzcompany.dop*) to denote the involvement of the Department of Post in the DAP.

5.6. Digital Address creation

Digital Addresses may be created and managed by the User using the AIA as a facilitator to the AIP. The user may have an existing interaction with AIP and be prompted by the AIP to create a Digital Address. If a User agrees, the AIP can redirect them to the appropriate AIA. Digital Address Creation is a multi step process. The steps for the creation of Digital address is shown in Fig. 2 and described below

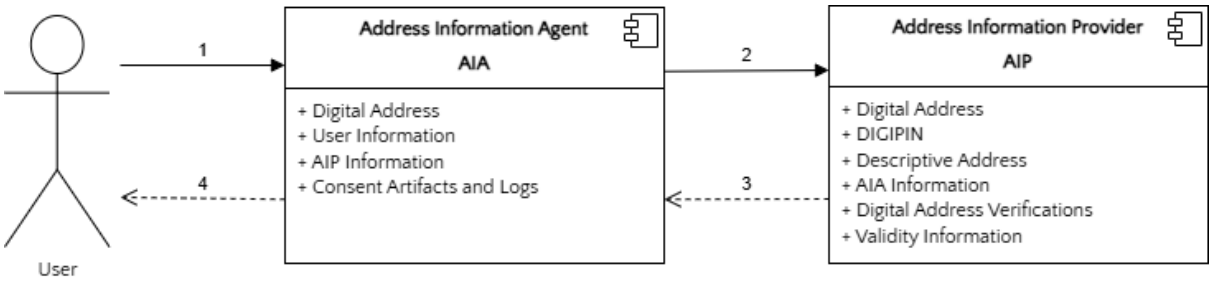


Fig. 2: Simplified DA Creation Flow

1. **Request from the User → AIA**: The User authenticates with its chosen Address Information Agent (AIA) and submits a 'Create Digital Address' request. The response specifies the desired DA label (***<name>@<suffix>***) and may optionally include preliminary location details or preferences. The AIA verifies the User's identity, checks local policy constraints (e.g., naming rules, block-lists), and prepares a consent artifact that records the User's authorization for this registration. The AIP may maintain machine-readable policies that must be satisfied to get a DA with a particular suffix. The AIA can enforce said policy and ensure that the User satisfies all conditions specified by the policy before proceeding to the next step.

2. **AIA → AIP: Registration submission**: Next, the AIA forwards the request to the Address Information Provider (AIP) that owns the target suffix. The message conveys:
    - the requested DA label,
    - the AIA's own identifier so future updates can be channelled through it, and
    - address attributes

    The AIA also includes proof that valid consent has been captured and logs the outbound transaction.

    The user would supply their location via their mobile device or computer to the AIP via AIA. The AIP can then convert the lat-long to a DIGIPIN (using the approaches outlined in the DIGIPIN document).
3. **AIP → AIA: Registration acknowledgement**: The AIP checks for label availability, applies its internal validation (length limits, reserved names, geospatial sanity), and, if all tests pass, commits the new record to its registry. The stored entry links the DA label to the User (via the AIA) in addition to the DIGIPIN and descriptive address. The AIP then returns an acknowledgement containing the unique DA identifier, a timestamp, and any additional metadata (e.g., recommended caching strategies).
4. **AIA → User: Confirmation**: On receipt, the AIA updates its own ledger—capturing the DA label, the User reference, the associated AIP, and the consent artifact ID—then notifies the User of successful creation. The confirmation typically includes the live DA, a summary of the stored address information, and guidance on how the User can manage or revoke the address in the future.

5.7 Digital Address resolution

Digital address resolution is the act of accessing the real world location information and the other attributes associated with a digital address so that the components and services can accurately find, validate, and interact with that location.

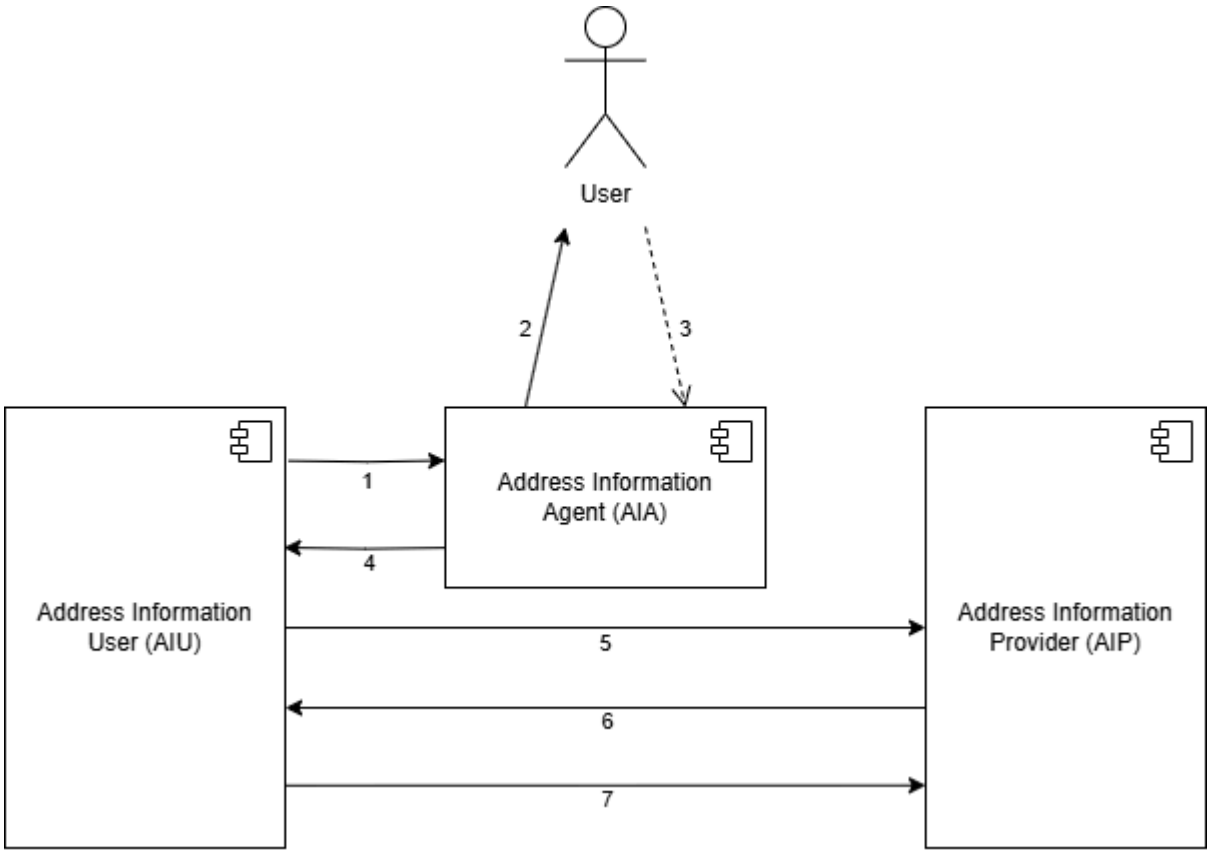


Fig. 3: Simplified DA Resolution

1. **Resolution request** - The AIU sends an initial resolution request to the AIA, asking it to obtain the geospatial details behind a specific Digital Address (DA). This request carries the DA and the AIU's credentials but no authorization token yet. During the resolution request, the AIU specifies the purpose for which they want to use the User's address data (e.g. parcel delivery). They may also request for certain attributes to be returned during resolution. E.g. to see if a User is in a certain AIUs service coverage range, the AIU may only require the locality address attribute when resolving the address.
2. **Consent request** - On receiving the request, the AIA reaches out to the User to confirm that the User is willing to let this particular AIU resolve the DA. This step constitutes the formal solicitation of consent.
3. **Consent response** - The User reviews the request, authenticates with the AIA, and grants (or denies) consent. During the request review, the User can decide what address attributes can be shared with the AIU and determine if the AIUs purpose for their address information is satisfactory.
4. **Authorization token creation** - When consent is granted, the AIA records the decision and issues a signed, time-bound authorization token to the AIU that binds the User, AIU, DA, and intended purpose. This is then shared with the AIU.
5. **Resolution request forwarding** - Armed with the authorization token, the AIU forwards the original resolution request—now augmented with the token—to the appropriate AIP that hosts the DA's suffix. Note that certain DAs may not require

consent for resolutions based on conditions specified by the concerned AIP. If an AIU determines that the DA they are trying to resolve does not need consent, they may directly contact the AIP without going through the previous steps.

6. **Resolution response** - The AIP validates the authorization token, retrieves the stored address information (DIGIPIN and any descriptive address), and returns it directly to the AIU. The response may include metadata such as freshness and caching limits.
7. **Confidence score feedback** - After completing its service, the AIU optionally sends a feedback payload—delivery accuracy, error codes, or other quality signals—back to the AIP. The AIP aggregates this data into a confidence score that helps refine address-verification logic and flags DAs needing re-validation.

Frequent consent requests for a particular AIU and DA prior to DA resolution may be a source of frustration to a User. To solve this, Users may choose to give preemptive long-term consent to certain AIUs to avoid these frequent consent requests. Preemptive consent can be revoked at any time by the User. The flows for preemptive consent creation and revocation are outlined in Appendix-III.

6. Proposed Technical Architecture of the Digital Address System

The technical architecture of the Digital Address Project (DAP) is envisioned as a decentralized Digital Public Infrastructure (DPI) with clearly defined roles and responsibilities for all stakeholders. It leverages established industry standards and best practices to promote interoperability. Furthermore, by embedding the principle of privacy by design, it ensures that any collection of sensitive information is handled responsibly and includes appropriate consent management mechanisms.

6.1 Interactions of different components

The diagram in Fig. 4 depicts the core interactions in the Digital Address Project's federated ecosystem.

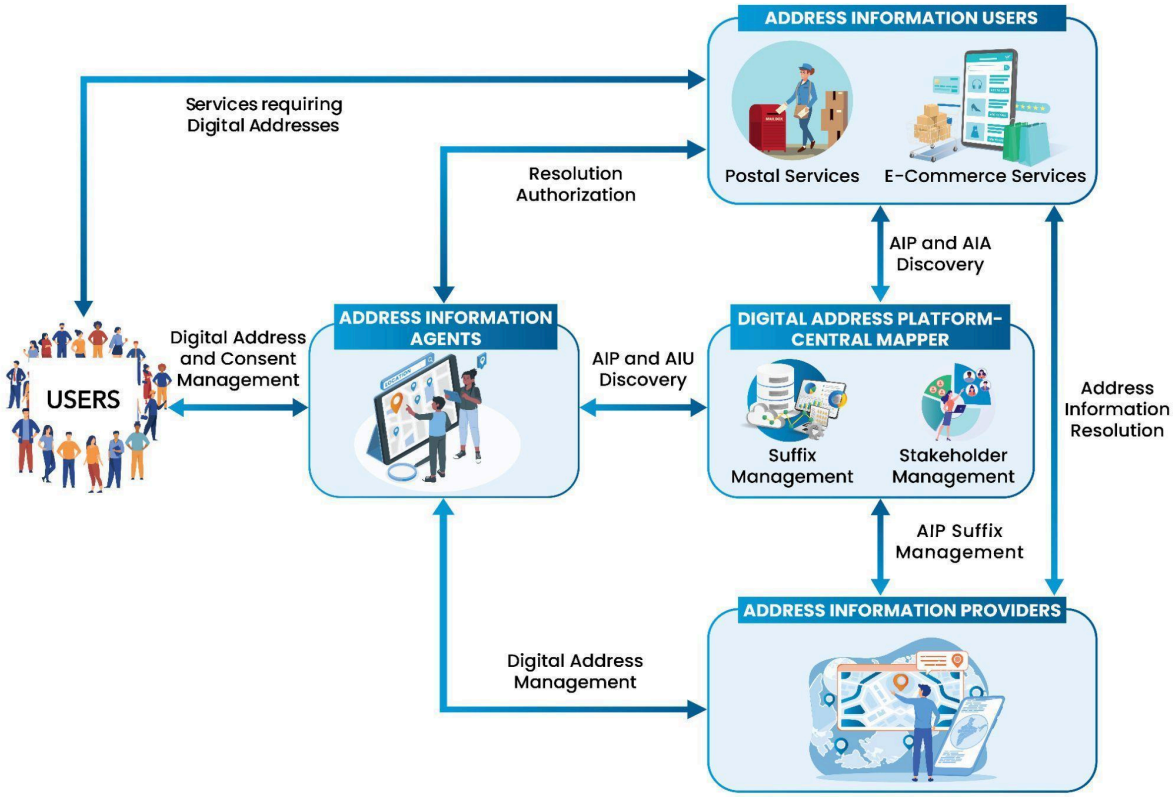


Fig. 4: Digital Address Network Interactions

At the centre is the Central Mapper (CM), which performs two coordination roles: ***Suffix Management***—delegating namespace ownership to individual Address Information Providers (AIPs)—and ***Stakeholder Management***—maintaining a live directory of all AIPs, Address Information Agents (AIAs), and Address Information Users (AIUs). When an AIU such as an e-commerce or postal service needs to handle a Digital Address, it first consults the CM to discover (***AIP and AIA Discovery***) which AIP hosts that address and which AIA can supply the authorization token required for resolution. AIAs also query the CM to discover peer AIPs and AIUs, ensuring interoperability across the network.

Users interact primarily with the AIA, where they create or update Digital Addresses and manage consent for data sharing (***AIP and AIU Discovery***, ***Digital Address and Consent Management***). The AIA, acting on the user's instructions, carries out ***Digital Address Management*** with the relevant AIP—registering new addresses, attaching DIGIPINs or descriptive text, and storing consent artifacts.

When a user requests a service from an AIU (***Services requiring Digital Addresses***), the AIU must resolve the Digital Address to real-world coordinates. It therefore asks the AIP for the address information, but the AIP releases data only after receiving a valid authorization token. That token is obtained through the AIA ↔ AIU ***Resolution Authorization*** exchange: the AIU proves it has the user's permission, and the AIA vouches for the consent. Once authorized, the AIP returns the address details to the AIU (***Address Information Resolution***), enabling the AIU to fulfil the user's service

request—such as delivering a package or scheduling a postal pick-up. The detailed stakeholders interaction flows are discussed in Appendix-III

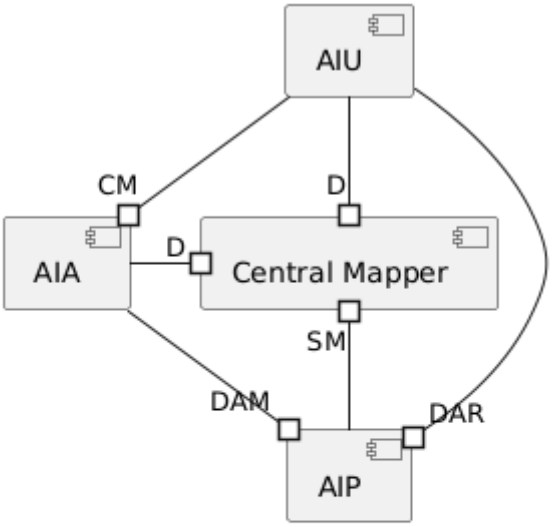
In summary, the CM provides discovery and namespace governance; the AIA safeguards user consent and manages address records; the AIP stores authoritative location data; and AIUs consume that data to deliver real-world services—all linked by clear, policy-driven interfaces.

6.2 Digital Address Network

The Digital Address Network (DAN) is composed of multiple interconnected entities, each playing a specific role in the management and resolution of Digital Addresses (DAs). These entities include AIAs, AIPs, CM and AIUs and implement interfaces for: Discovery (D), Consent Management (CM) and DA Management (DAM) . All DAN components may also expose administrative, operational, and management interfaces beyond the core DAN scope.

Below is a function of the DAN interfaces and is shown in Figure 5:

1. Discovery (D)
    a. AIU → Central Mapper – An Address Information User (AIU) looks up which AIP owns a given suffix or DA.
    b. AIA ↔ Central Mapper – An Address Information Agent (AIA) likewise queries the Central Mapper to discover AIPs when managing or resolving Digital Addresses.
2. Suffix Management (SM)
    a. Central Mapper ↔ AIP – The Central Mapper allocates and updates namespace suffixes, keeping every Address Information Provider (AIP) in sync with the authoritative suffix registry.
3. Digital Address Management (DAM)
    a. AIA → AIP – Acting on a user's behalf, the AIA registers, updates, or deactivates Digital Addresses within the appropriate AIP registry.
4. Consent Management (CM)
    a. AIU ↔ AIA – Before an AIU can access address details, it obtains an authorization token from the AIA; the AIA captures or verifies the user's approval and issues the token.
5. Digital Address Resolution (DAR)
    a. AIU → AIP – With a valid authorization token, the AIU requests the AIP to resolve the Digital Address into its underlying location information, enabling the AIU's service workflow.



Op	Interface Description
D	Discovery
SM	Suffix Management
DAM	Digital Address Management
CM	Consent Management
DAR	Digital Address Resolution

Fig. 5 : Digital Address Network (DAN) interfaces

6.3 Key User Interfaces

DAP will expose the following interfaces for the users

Digital Address Assignment : Users will be able to create Digital Addresses for their own addresses via AIAs.

Secure and Consent-Based Address Data Sharing : Users will be able to share their Digital Addresses with consent to other Users and to AIUs to avail services.

Digital Address Management : Users will be able to manage their Digital Addresses via AIAs. Users can update and modify the DIGIPIN and descriptive addresses linked to their Digital Addresses, manage consent to their Digital Addresses and perform other tasks permitted by the AIA and AIP.

Secure Address Verification and Accuracy Checks: AIPs may facilitate verification of DIGIPIN and descriptive address before creation of a Digital Address by using authoritative address information sources.

Address-Based Service Discovery : AIPs may facilitate discovery of services based on the suffixes they manage. For e.g., an AIP that manages the suffix ***hospital*** and mandates that only hospitals can obtain a DA with this suffix can allow discovery of hospitals by listing all Digital Addresses containing the ***hospital*** suffix.

Legacy Address Integration : AIPs and AIUs can facilitate migration of traditional addresses into Digital Addresses with the consent of the User.

Cross Platform Integration : There is a scope for DAP to integrate with the existing DPIs on a case to case basis.

Strong grievance redressal : Users will be able to file grievances in case of any issues encountered when interacting with AIAs, AIPs and AIUs. Note that these grievances must be related to the operations of the DAP and not related to the service delivery of the AIUs.

6.4 Design Choices of the Digital Address Network (DAN)

- Digital addresses suffixes are unique : Every suffix should be managed by a single AIP.
- User data is handled by AIA : The user shall interact only with the AIA
- Modularity of DAN components : The DAN components viz AIU, AIP, AIA and CM shall operate independently and will only interact when needed.
- Flexible policies : The AIP shall have independent and flexible policies regarding allocating digital addresses to users.

6.5 Data Exchange component for Digital Address Project

At the core of the Digital Address system, there shall be a seamless, secure and consent exchange. The Data Exchange component must be able to handle the flow of data between various entities efficiently while addressing security and privacy considerations. Rather than consolidating data into a central repository, a Data Exchange must interconnect these disparate entities through standardized APIs and consent mechanisms, allowing for seamless access to information.

The interfaces and well-known concepts behind data exchanges will be relevant in the design and development of the Digital Address Project.

Key capabilities of an effective Data Exchange include:

- **Data Discoverability:** Ensuring stakeholders can easily discover relevant data
- **Standardization of APIs :** Creating consistent interfaces for seamless data access and interoperability.
- **Controlled Data Access:** Implementing secure data sharing policies to protect sensitive information.
- **Consent-Driven Data Sharing:** Promoting ethical data usage through clear consent mechanisms.
- **Anonymization and De-identification:** Safeguarding sensitive information to maintain privacy.

7. Security Considerations

7.1. Platform Security

Platform security refers to the security best practices to be followed during the development phase of DAP, and the infrastructure security on which the Digital Address Network (DAN) is deployed.

The development phase should include continuous security checks and practices to ensure that the source code of the DAN components is managed securely. This involves checking for common source code security vulnerabilities such as accidental inclusion of API keys and tokens in the source code repository, and regular usage of static code analysis tools which can help analyze source code or compiled versions of code to help find security flaws. Additionally the source code must perform input validation checks, output encoding checks, error handling and logging and other general coding practices. [20]

Infrastructure security includes following security best practices for the technical infrastructure deployment. This includes following any security requirements for data protection (encryption, robust caching policies etc.), communication security (TLS for all communication channels, parameter filtering for HTTP connections etc.), system configurations (updating all infrastructure components to the latest approved versions, using separate environments for development and production etc.), and database security (secure credentials, strong input validation etc.) [20]

Particular care should be taken to cover common critical security risks and to follow at least the minimum standards for application development and verification. [21] [22]

7.2. Security and Consent Mechanisms

As the DAP system is citizen centric, consent is a core idea in DAP. With the introduction of the DPDP Act, robust consent mechanisms are essential for any DPI handling Personally Identifiable Information (PII) to build trust.

In the Digital Address Project (DAP), Address Information Agent (AIAs) act as consent managers on behalf of users. They collect and maintain the approvals necessary for key operations involving each user's digital address, ensuring that changes occur only with explicit authorization. The primary consent-driven actions include:

- Creation of a new digital address
- Assignment of address information to an existing address
- Deactivation of an address no longer in use
- Resolution of an address (i.e., retrieving detailed location information)

By assigning the responsibility of consent management to AIAs, the DAP maintains a user-focused approach, reinforcing privacy and guaranteeing that users retain full control over their digital addresses.

7.2.1 User authentication

Address Information Agent (AIAs) must authenticate users to confirm that only the rightful owner can maintain and manage their digital addresses. This authentication process is essential for generating the necessary consent artifacts, which underpin secure address operations. Depending on the specific category and intended use of the digital address, AIAs may employ multiple authentication mechanisms, such as:

- Aadhaar-based e-KYC verification
- Password and One-Time Password (OTP) authentication
- PIN based verification

By offering flexible authentication options, AIAs ensure robust identity verification, enabling users to confidently create, update, and deactivate their digital addresses.

7.2.2 Consent artifact management

Each time an Address Information Agent (AIAs) gathers a user's approval, it generates a digital consent artifact which is a digital record of the terms of the consent which the user has agreed. This artifact records:

- the identities of the Address Information Provider (AIP), Address Information User (AIU), and the AIA itself
- the user's authentication details (e.g., Aadhaar transaction ID, OTP hash, or PIN-hash)
- the relevant Digital Address (DA)
- metadata describing the purpose, scope, and validity period of the consent
- a globally unique consent identifier (CID) that links every subsequent action to the original approval. The CID can be a string of random characters which is sufficiently long to ensure uniqueness

7.2.3 Supplementary consent records

To create a complete audit chain, the AIA also stores additional documents tied to the same CID:

- Revocation receipts generated whenever a user withdraws consent
- Event notifications issued on creation, modification, or revocation of consent
- Audit logs detailing every data-access event that relied on the consent artifact, including timestamp, requesting AIU, and data fields accessed

7.2.4 Lifecycle and usage

All consent artifacts and their associated documents are retained in the AIA's secure consent repository, protected at rest and in transit. The CID functions as the single source of truth for downstream operations—such as DA creation, update, deactivation, or resolution—allowing AIPs and AIUs to verify that:

- the user's consent is still valid for the requested operation, and
- the requested data use remains within the original scope and timeframe.

This architecture delivers a clear, auditable trail of accountability while ensuring users retain granular control over how their digital address information is shared and managed.

7.3. Audit Logs

Audit logs must be created and stored at each component as a result of a successful operation. These logs may be used to hold the various stakeholders accountable and legally liable in case of any misuse or mismanagement of data. For the sake of non-repudiation, all records must be digitally signed.

The type of log records that need to be maintained by each component are listed below:

- AIA
    - User registration record : When the User registers on the AIA
    - DA Consent created record : When the User has given consent for an AIU to resolve their DA - both for preemptive and long-term consent
    - DA Consent revoked record : When the User has revoked preemptive consent for an AIU
    - DA Attribute Modification record : When the User has updated any of the attributes of their DA
    - AIA Transfer record : When the User has migrated to a new AIA. Both the new AIA and old AIA must create this record.
- AIP:
    - DA Resolution record : When the AIP has resolved a DA to an AIU

8. Federated Architecture

The Digital Address Project technology architecture proposes to establish a Federated Architecture, defined in terms of its building blocks. The federated architecture shall facilitate streamlining of information flows across stakeholders in the ecosystem while keeping users, their privacy and confidentiality of data at the core.

Federation is an architectural approach that allows interoperability and information sharing between semi-autonomous de-centrally organized entities, information technology systems and applications.

A Federated Architectural approach for DAP is needed for enhancing the security and privacy of the personal identifiable information of the users while ensuring interoperability, open source approach and technological agnosticism.

8.1 Principles of Federated architecture:

The federated architecture is founded on a set of guiding principles. These principles are recommended for implementation [6]:

1. **Decentralized Data Storage**

All user address data shall be maintained by Address Information Providers (AIPs) in a

decentralized manner by the allotted suffixes adhering to the principle of minimality at each level.

2. **User-Centric Data Control**
Users shall have full control over the processing of their address data, including how and by whom it is accessed or used.

3. **Controlled Access via Consent-Driven Links**
Access to address data shall only be provided through authorized applications or entities, and strictly via secure links, subject to the user's explicit permissions and consent, as per applicable policies and regulations .

8.2 Comparison of Centralized vs Federated architecture

A comparison between a centralized and federated architecture is as below :

Dimension	Federated model	Centralized model
Governance & trust	Each Address Information Provider (AIP) and Address Information Agent (AIA) is governed by its own organisation. Users and relying parties can pick providers they already trust.	One operator exercises end-to-end control; every stakeholder must accept its policies.
Privacy & consent	Consent is issued to the user. The AIA that on-boards the user also mediates every disclosure between the AIU and the user.	All consent artifacts and resolution logs sit in one place.
Regulation & localisation	Regional AIPs/AIAs can comply with local data policies, language, and sector-specific rules while still inter-operating through the Central Mapper	A single operator must meet diverse jurisdictional requirements and will need to have the capabilities to resolve any conflicts which may arise.

Dimension	Federated model	Centralized model
Scalability & performance	Registries, consent ledgers, and resolution services are partitioned, so that network traffic is naturally distributed to reduce load on any single component and latency is lower for local calls.	Centralized models are at risk of global outages during peak events (e-commerce festivals, emergency alerts, etc.) and performance bottlenecks may need to be handled on an ad-hoc basis.
Resilience & fault isolation	An outage at one AIP or AIA affects only the addresses it manages; the rest of the ecosystem stays online.	A single failure can disrupt every DA lookup and every consent flow.
Innovation & competition	Multiple AIAs can compete on UX (e.g., vernacular apps, accessibility features, value-added analytics). AIPs can innovate on verification methods (GIS overlays, satellite validation, field surveys).	In a centralized model, the absence of competing providers can reduce the impetus to continually enhance user interfaces or validation processes.
Specialisation	Different AIPs can specialise in distinct strengths—some excel at high-precision urban mapping, others manage enterprise asset data, while still others curate authoritative nationwide datasets.	In a centralized model, a single operator must address a broad spectrum of requirements, which may limit its ability to serve specialized or niche needs effectively.
Risk & compliance	Liability and compliance workloads are distributed. If a given AIP is sued or fined, the rest continue unaffected.	All regulatory, cybersecurity, and operational costs pile up on a single entity—and any breach becomes systemic.
User choice & portability	Users can migrate to a different AIP or AIA if service quality drops.	Lock-in is high unless onerous data portability mandates are enforced.

Table 3: Comparison between a centralized and federated architecture

8.3 Role of Central Mapper in federated architecture

Federation does not mean "everyone speaks a different dialect." The Central Mapper standardises:

- Suffix delegation records (who owns ***.delhi.in***, ***.post***, ...)
- Discovery endpoints for AIUs and AIAs
- Global audit requirements (token formats, revocation events)

This thin layer provides **interoperability** while allowing execution details to remain local.

Summary : A federated lattice of AIPs and AIAs best matches DAP's goals of privacy, resilience, local compliance, and user empowerment, while a centralized model would create scale, trust, and regulatory chokepoints incompatible with a national digital-public-infrastructure mission.

9. Digital Address Verifications

Address Information Providers can provide additional value to the AIUs regarding the address data by provisioning for address verifications. There can be multiple address verification options which are dependent on the sector in which the AIU operates. These verifications can be automated processes or can involve extensive manual checks based on the usage requirements of the AIU.

9.1. Options for Verifications

9.1.1. Fetching address attributes from an Address Attributes Registry (AAR)

The AIP consults a trusted, regularly updated registry and receives standard details—such as the official locality, city, pincode, administrative boundaries of the DIGIPIN address information provided by the User. This trusted registry termed as 'Address Attributes Registry' (AAR) can be consulted during the Digital Address creation process, and at regular intervals in the future to update the standard address information received from the registry. The AAR is comparable to standardized address repositories developed internationally such as Geocoded National Address File (G-NAF) developed by Geoscape Australia[23], and the Estonian Address Data System[24]. The Fig.6 below outlines the flow when the Digital Address is first created by the User.

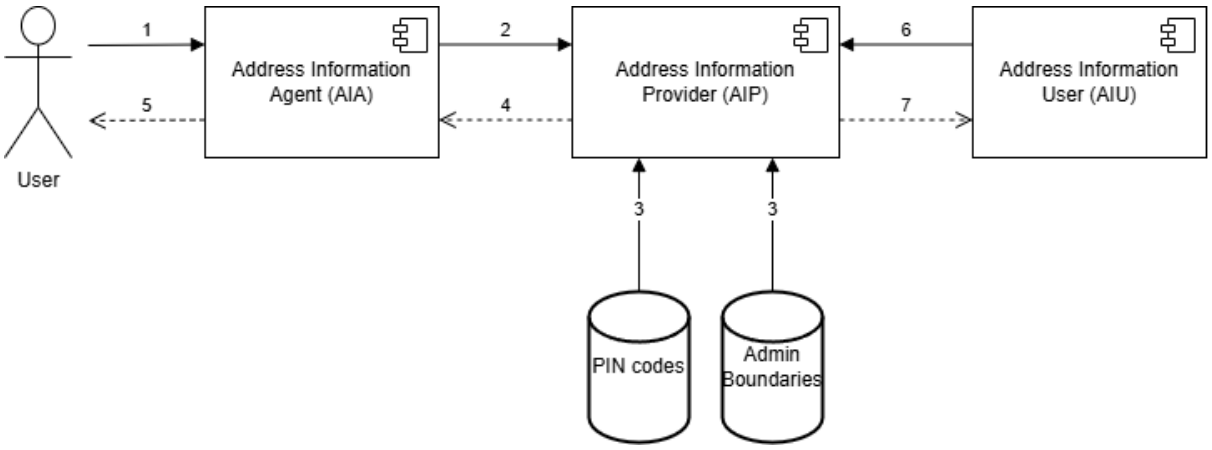


Fig. 6: Fetching address attributes from verified address attributes registries

1. The User creates the Digital Address and provides the DIGIPIN address information which is to be associated with the Digital Address to the AIA.
2. The AIA creates the relevant consent logs and updates the Digital Address at the AIP with the DIGIPIN information.
3. The AIP fetches the relevant address attributes from the AAR. These registries are authoritative and may be available in the public domain.
4. The AIP acknowledges the assignment of address information to the AIA.
5. The AIA notifies the user of the updated information.
6. An AIU who is interested in resolving a digital address presents the digital address with the relevant consents and authorizations to the AIP.
7. The AIP can fetch any updated address attribute information before resolving the request of the AIU.

9.1.2. Self-declared addresses with dynamic confidence scores

Users can supply their own address information. The AIP assigns a confidence score that rises or falls over time, using feedback from AIUs on whether service fulfillment was successful. A consistently smooth service record pushes the score higher, while repeated failures lower it. The steps for address resolution with dynamic confidence score feedback is shown in Fig.7.

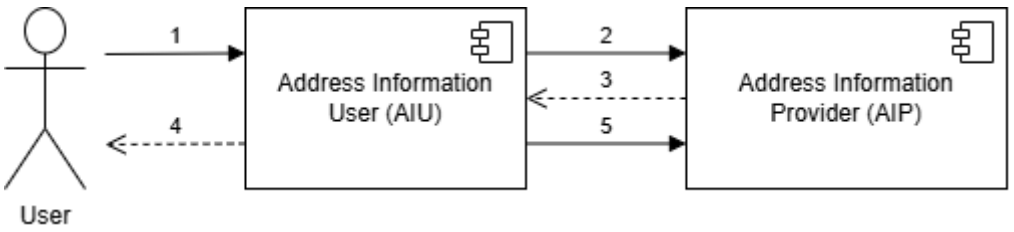


Fig. 7: Address resolution with dynamic confidence score feedback

1. The User approaches the AIU for some service fulfillment and provides the AIU with their Digital Address.
2. The AIU obtains the relevant consents and authorizations, and requests the AIP for resolving the Digital Address to obtain the address information.

3. The AIP verifies the request of the AIU and responds with the address information associated with the Digital Address.
4. The AIU fulfills the service request by the User using the address information provided by the AIP.
5. The AIU notifies the AIP regarding the accuracy of the address and the ease of fulfilling the service request, so that the appropriate confidence score can be computed.

Further information regarding the possibilities of computing the confidence score is given in section 9.2.

9.1.3. Physical verification by an Authorized Address Validation Agency (AAVA)

For the highest level of certainty, a certified field agent from an empanelled agency termed as Authorized Address Validation Agency (AAVA) [3] visits the location in person, confirms it on the ground, and the AIP marks the address as physically verified along with the metadata associated with the physical verification such as verification timestamp, the validity period of the verification, and any supporting information. The verification request can be initiated by either the User or the AIU based on the usage scenario of the Digital Address. AIPs can also choose to require physical verification in order to grant addresses under a specific suffix related policy. An illustrative example for an AIU initiated verification process is outlined in Fig.8 below.

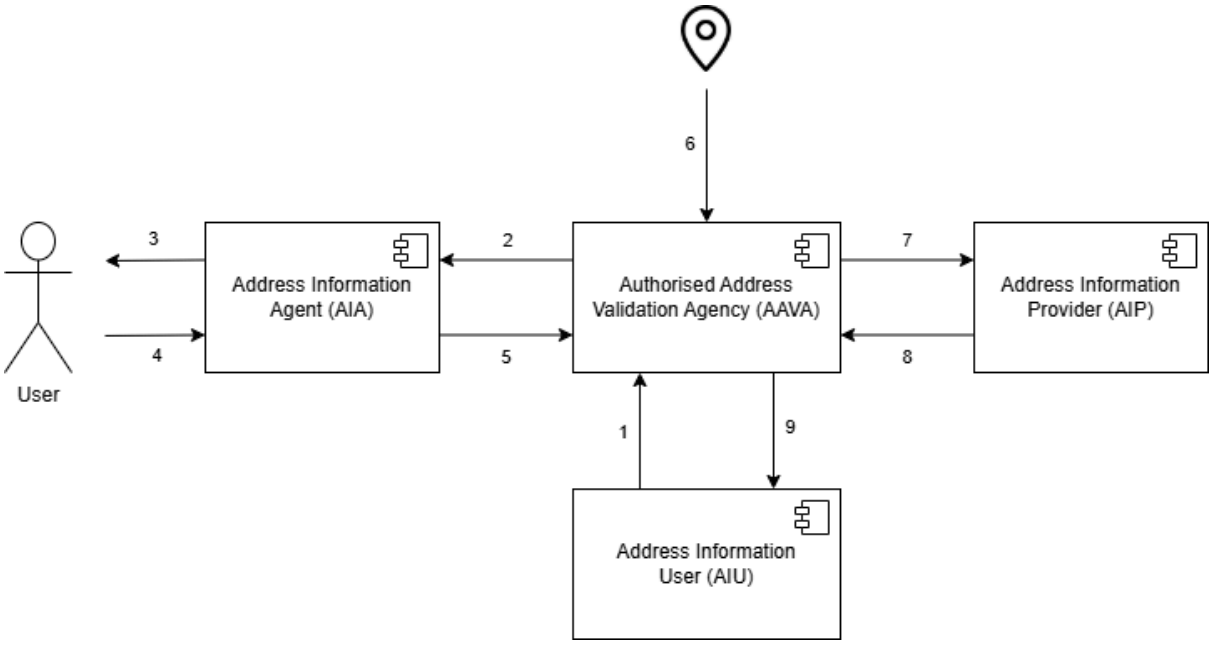


Fig. 8: Physical verification initiated by the AIU with the consent of the user

1. The AIU approaches an empanelled AAVA and initiates the physical verification of a Digital Address it has received for the purpose of service delivery to the User.
2. The AAVA notifies the associated AIA for initiating a User consent flow to perform the physical verification.
3. The AIA requests the user for consent for the verification process.

4. The User grants consent allowing the AAVA to perform the verification.
5. The AIA notifies the AAVA of the updated consent.
6. The AAVA performs the physical verification through a relevant out of band operation.
7. The AAVA notifies the AIP of the status of the physical verification including any extra metadata associated with the verification.
8. The AIP acknowledges and stores the verification information of the DA and makes it available for the AIU.

9.2. Confidence Score

The DAP also envisages setting a Confidence Score per Digital Address — assigning numerical ratings based on past successful deliveries. This option is highly valuable to sectors such as e-commerce, postal delivery, and related services. It would rely on regular user interactions to build incremental trust in the address authenticity, gradually increasing service reliability.

Confidence scores can be calculated at the AIP based on some feedback from the AIU after they have attempted the delivery using the address information from the DA resolution process. The confidence score represents an accumulative score from all the AIU deliveries. The method of calculating the confidence score can vary between AIPs.

As an example, one method can involve calculating the displacement of the delivery address information and the stated address information in the Digital Address. This displacement can be used to derive further insightful statistical scores of the address information in combination with additional parameters like the delivery timestamp and ease of delivery (successful delivery, delivered with difficulty, undelivered etc). Some example statistics are outlined below.

- Spatial deviation: Represents how tightly the deliveries cluster around the stated address. This can be used to infer if all the deliveries are consistently going to the same location.
- Centroid shift: Represents how far the delivery locations are from the stated address. This indicates if the stated address is pointing to the correct location overall.
- Success rate: Represents how successful the deliveries are over a period of time. Difficult deliveries and failed deliveries get assigned lower weights. This can be used as an indicator of how well the stated address works in practice.

All the above statistical scores would have to account for any changes in the address information either by resetting them or by using a time decay function to reduce the importance of older deliveries which occurred before the updated address information.

10. Way Forward

As the next step, we propose the development of a working prototype of DAP to ensure the soundness of the proposed architecture. This will serve as a functional prototype of the overall system and act as a validation instrument for the architecture, technical flows, stakeholder interactions, and guiding principles. This will allow progressive refinement of the proposed technical architecture.

As part of the first project milestones it is proposed to develop a prototype and include demonstrating the feasibility of the proposed solution, ensuring it is both practical and achievable within defined constraints. A key outcome at this stage is the development of a functional representation of the technology architecture, providing a clear view of how different components will work together. Consultation with industry stakeholders will play an important role in validating the approach, incorporating real-world insights, and aligning the architecture with current best practices and needs. Based on these consultations and ongoing analysis, the technical architecture will be updated, incorporating refinements and adjustments.

The second milestone focuses on the development and deployment of a Beta phase within a selected controlled environment such as a university campus. This phase shall aim to simulate real-world engagement by operationalizing key components that are AIPs, AIAs, AIUs, and the CM allowing for a realistic assessment of system interactions. The Beta phase will also serve to test the roles and interfaces of all stakeholders, ensuring that workflows, data flows, and user experiences align with intended designs. The objective is to identify key insights and solicit structured feedback from stakeholders, which will inform refinements and validate the foundational assumptions of the system before scaling to broader implementations.

The third milestone, marks the real-world pilot deployment of the system in a live operational environment. This phase is focused on enabling the end-to-end execution of core workflows under actual conditions, moving beyond controlled testing to practical application. The pilot shall serve to validate the system's scalability, assess its performance and user experience at scale, and identify any operational challenges. The key objective is to fine-tune procedures and configurations based on observed performance and practical realities. Additionally, the pilot shall incorporate and implement feedback from stakeholders gathered during earlier phases, ensuring that the system is optimized, user-aligned, and ready for broader rollout.

Building on the learnings from these three phases, a phased rollout strategy for the full-scale deployment of the system should be planned. This approach will enable controlled expansion across regions or stakeholder groups, ensuring stability, managing risk, and allowing for iterative refinements based on real-world feedback. Each phase will be guided by defined success metrics and readiness criteria, ensuring that the system scales efficiently while maintaining performance, security, and stakeholder alignment. A phased rollout also supports effective change management and smoother adoption across the ecosystem.

The proposed timeline for the Digital Address Project is shown in the figure below:

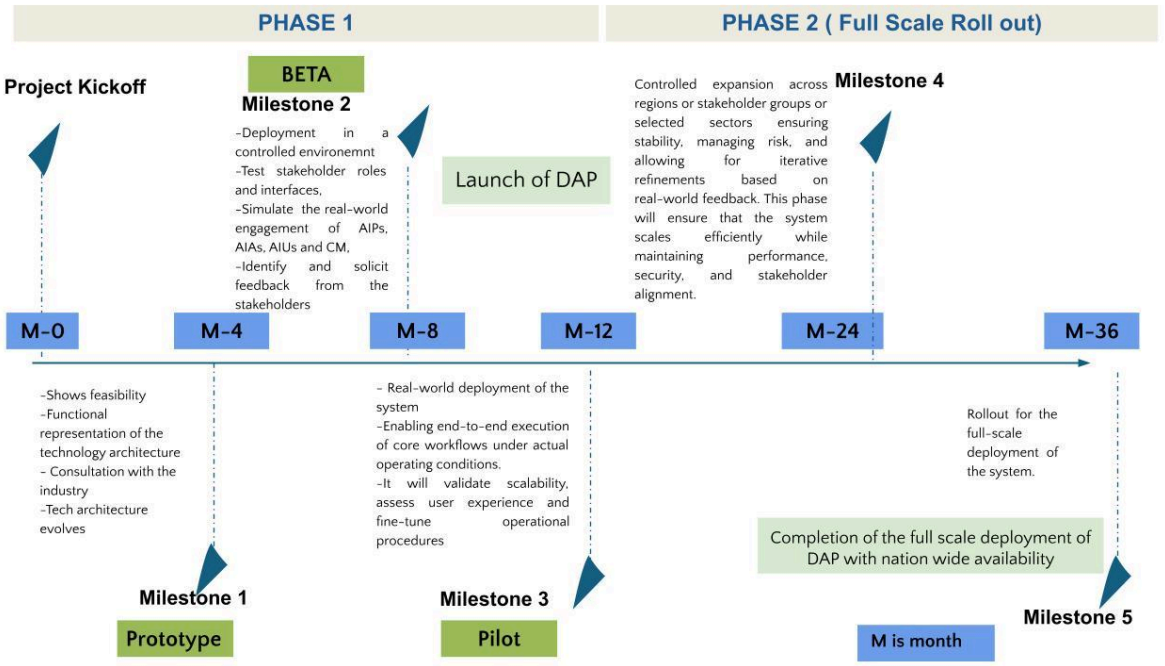


Fig. 9 : Proposed timeline for the Digital Address Project

The financial estimates for the PHASE-1 are shared in a separate document titled 'DAP_Financial_estimate_Proposed_timeline_Cloud_Cost_estimate_model'

Appendix-I : Open Source Licensing

When building Digital Public Infrastructures (DPIs), the choice of an open-source license is critical as it determines how the software can be used, modified, and shared. As DAP is envisaged as a DPI, this Appendix lists out the advantages and limitations of various commonly used open-source licensing approaches. Popular licenses like MIT, Apache 2.0, and AGPL have been considered. Each of these licences offers distinct advantages and disadvantages depending on the DPIs goals for openness, collaboration, and control.

AI.1. MIT License

The MIT License is one of the simplest and most permissive open-source licenses. It encourages adoption by lowering the barriers to integration. The MIT License is suitable for those initiatives which aim to maximize reach and usage. It does not enforce openness in derivative works, which may lead to proprietary forks that do not contribute back to the community [7].

Advantages:

- **Simplicity:** The MIT License is short and easy to understand, even for non-technical users
- **Flexibility:** It allows anyone to use, modify, distribute, and even sell the software without many restrictions
- **Broad Adoption:** Ideal for libraries or frameworks that developers can easily integrate into other projects

Disadvantages:

- **No Copyleft Protection:** Users can take MIT-licensed code, modify it, and use it in closed-source projects without sharing their changes
- **No Patent Protection:** Unlike Apache 2.0, the MIT License does not include explicit patent rights or protections

AI.2. Apache License 2.0

Apache 2.0 is a strong choice for cloud platforms commonly used in enterprise-grade software (like Kubernetes). A DPI cloud infrastructure, like the DAP for hosting government services could benefit from this license due to its patent protections. The Apache License is another permissive license but includes additional protections. It provides legal clarity with patent protection. Apache License does not enforce open-source contributions from derivative works [8] .

Advantages:

- **Patent Protection:** Grants users a perpetual, irrevocable license to any patents related to the software

- **Attribution Requirements:** Requires users to disclose significant changes made to the original code
- **Enterprise-Friendly:** Widely used by companies because of its legal clarity and protections for commercial use
- **Flexibility:** Like MIT, it allows proprietary use of modified versions of the software

Disadvantages:

- **Complexity:** The legal language is more detailed than MIT, which might require legal expertise to fully understand
- **No Copyleft Enforcement:** Similar to MIT, it does not mandate that derivatives remain open-source

AI.3. AGPL (GNU Affero General Public License)

The AGPL is a strong copyleft license designed to ensure openness in all forms of software use. AGPL's network interaction clause ensures that even hosted services must share their source code, fostering trust and accountability. Strong copyleft ensures openness across all derivatives and network-based uses, promoting transparency and community collaboration [9].

Advantages:

- **Copyleft Protection:** Ensures that any modifications or derivatives of the software must remain open-source under the same licence
- **Network Interaction Clause:** Closes the "SaaS loophole" by requiring that source code be shared even if the software is used over a network (e.g., web applications)
- **Community Collaboration:** Encourages sharing improvements with the community by mandating openness for all changes

Disadvantages:

- **Restrictive Nature:** Its strong copyleft provisions may deter adoption by companies or developers who want flexibility in using or modifying the code privately
- **Legal Complexity:** Understanding compliance requirements for network-based applications can be challenging
- **Limited Commercial Appeal:** Enterprises may avoid AGPL due to its strict sharing conditions, especially for proprietary SaaS offerings

The following table suggests the different Open source Licensing Schemes for DAP components

Component	Suggested Open-Source License
Address Information Provider	Apache License 2.0
Central Mapper	AGPL

Address Information Agent	Apache License 2.0
Deployment Scripts	AGPL

Table 4: Suggested Open-Source Licenses for DAP components

Appendix-II : Suggested technology stack

For the development of the Digital Address Project, we suggest the following technologies or any appropriate replacements.

Sr. No.	Component	Suggested Technologies
1.	Central Mapper	Kubernetes [10], RabbitMQ [11], PostgreSQL [12], Vert.x [13], Keycloak [14], ImmuDB [15], NGINX [16]
2.	Address Information Provider (AIP)	Vert.x, PostgreSQL, NGINX, ImmuDB
3.	Address Information Agent (AIA)	(*SDKs in various programming languages can be provided to allow AIAs to interact with the CM/AIPs. Implementers can choose to use any SDK that aligns with their language requirements. OpenAPI specifications for the AIA interfaces can also be developed.*)
4.	Address Information User (AIU)	(*SDKs in various programming languages can be provided to allow AIUs to interact with the CM/AIPs. Implementers can choose to use any SDK that aligns with their language requirements. OpenAPI specifications for the AIU interfaces can also be developed.*) Vert.x, PostgreSQL, NGINX, ImmuDB
5.	Monitoring and observability of components	Prometheus [17], Grafana [18], Loki [19]

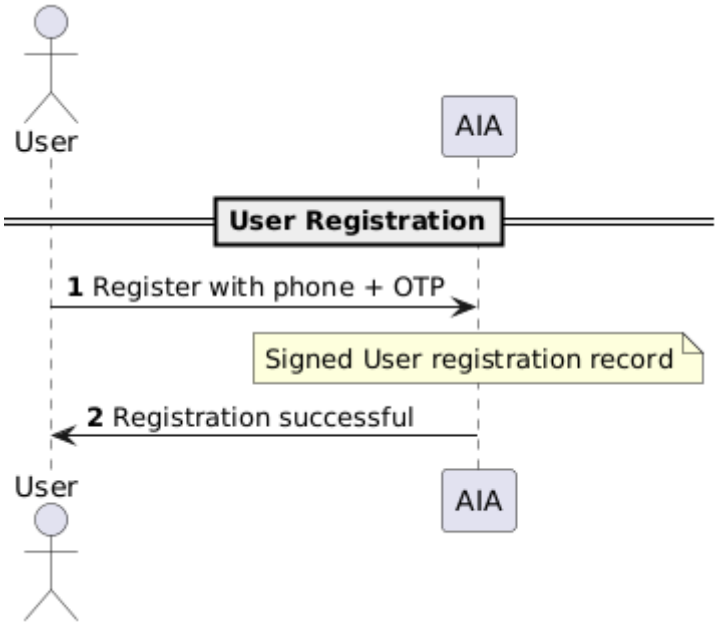
Table 5: Suggested technologies for DAP development and deployment

Note : Please note that these technologies are only suggestive and non-exhaustive and some of these technologies can be replaced by suitable alternatives.

Appendix-III : Detailed sequence diagrams of the DAP operations

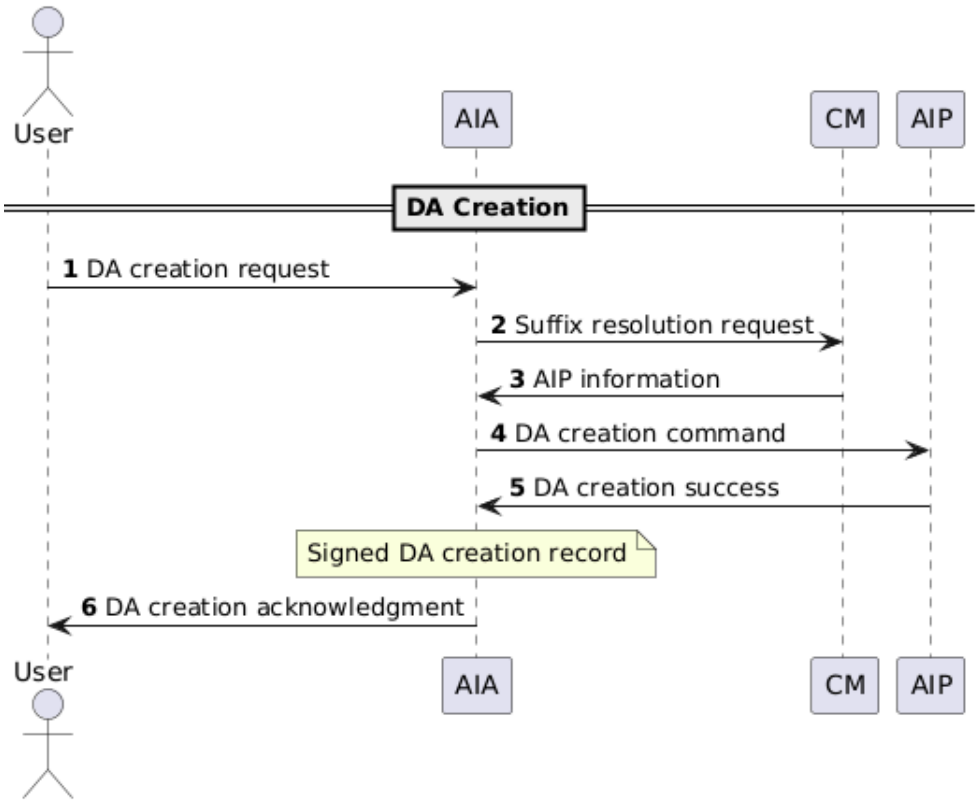
AIII.1. User Registration

The flow begins with the user initiating registration by submitting their phone number along with a One-Time Password (OTP) to the system. The AIA processes this request and generates a signed user registration record, which serves as proof of successful registration. This signed record is logged and returned to the user, completing the registration process with a confirmation of success.



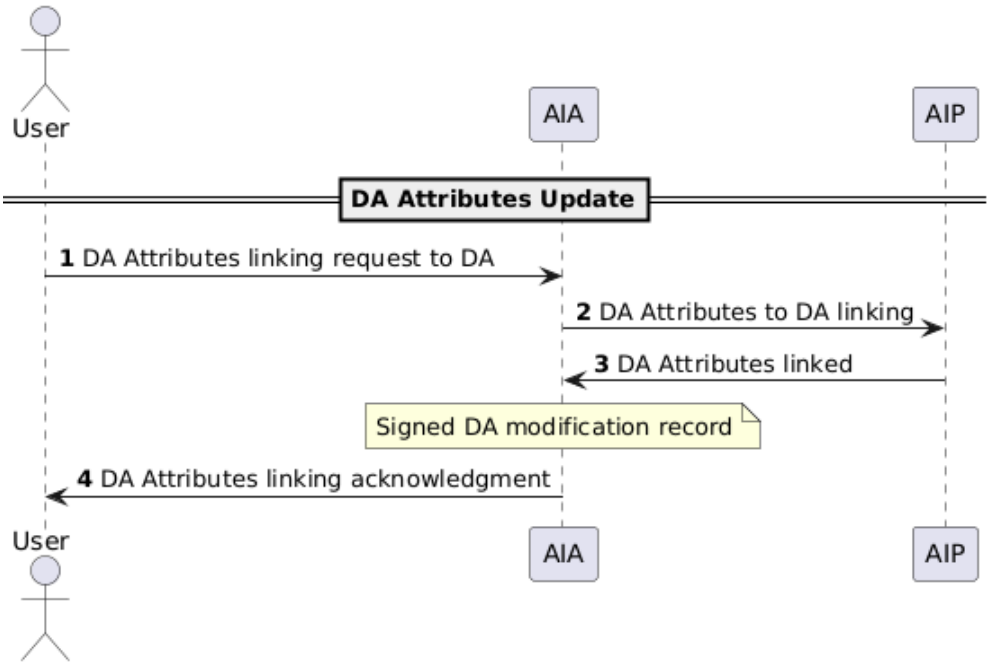
AIII.2. Digital Address Creation

The Digital address creation flow is initiated by the user sending a DA creation request to the AIA. The AIA resolves the required suffix information by querying the AIP through a suffix resolution request and receiving the relevant AIP information in return. Based on this, the AIA sends a DA creation command to the CM, which coordinates with the AIP to complete the creation. Upon successful creation, a signed DA creation record is generated and logged by the AIA. Finally, the user receives a DA creation acknowledgment, confirming the successful establishment of their Digital Address.



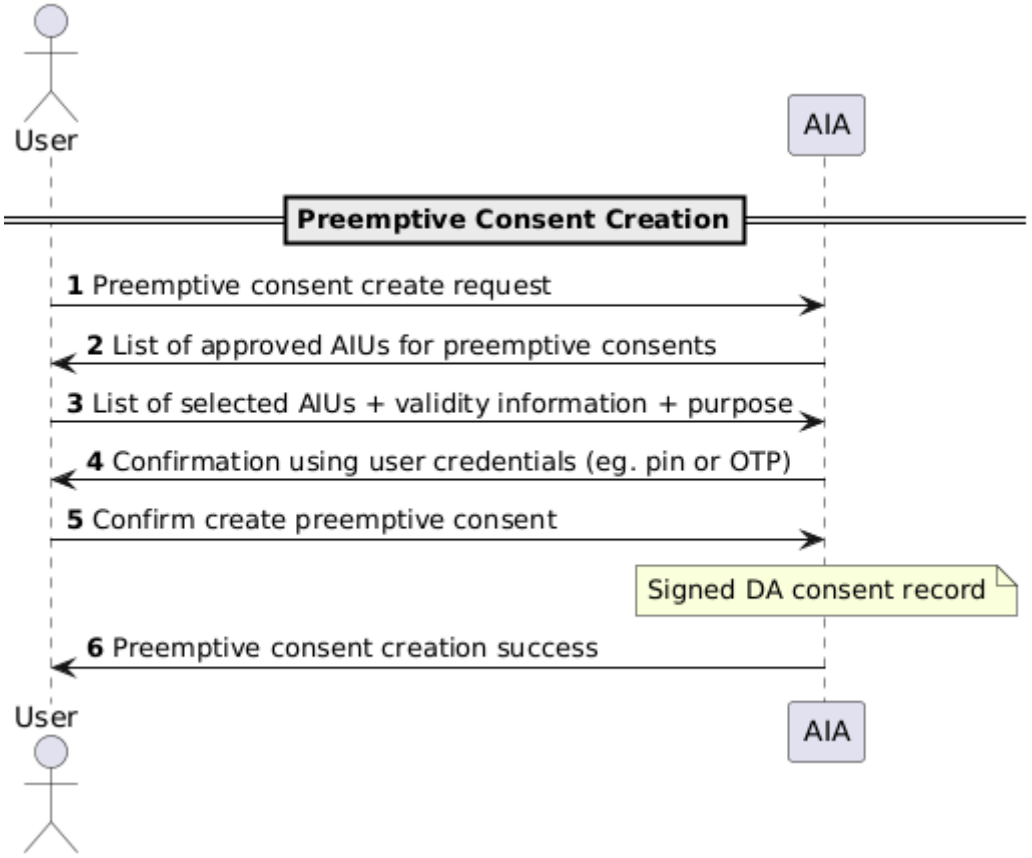
AIII.3. Digital Address Attributes Update

The flow begins when the user submits a request to update the attributes of an existing Digital Address. The AIA receives this request and forwards the updated attribute data to the AIP. Once the attributes are successfully updated, the AIP sends confirmation back to the AIA and a signed DA modification record is generated and logged by the AIA, which serves as a proof of the update. Finally, the user receives an acknowledgment confirming that the DA attributes have been successfully updated.



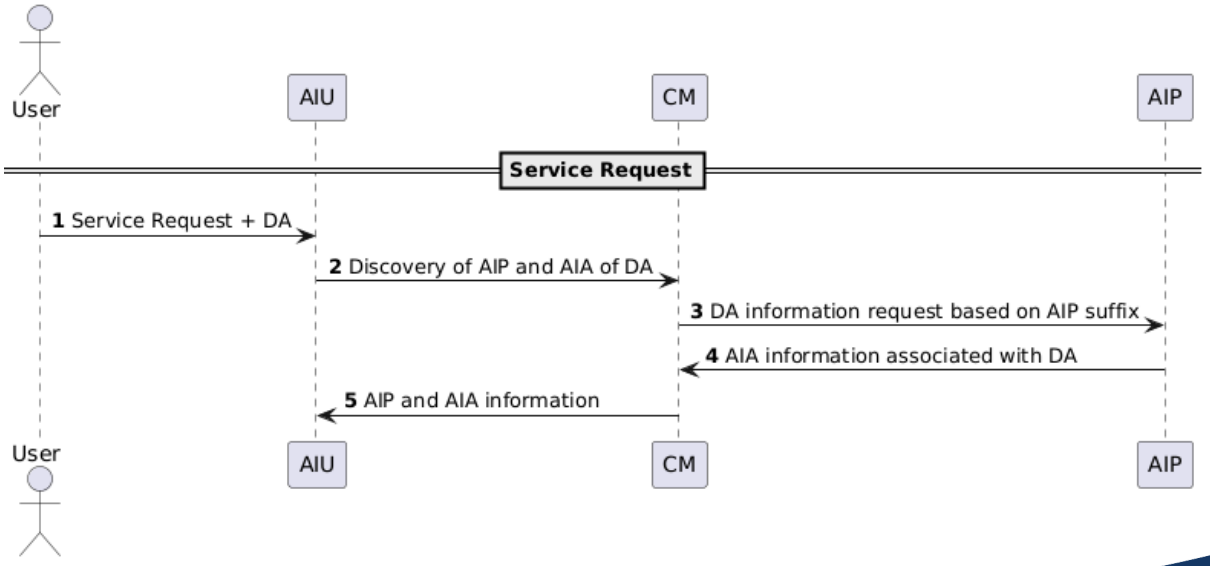
AIII.4. Preemptive Consent Creation

The Preemptive Consent Creation flow begins when a User initiates a request to create preemptive consent for their Digital Address for a particular AIU. The AIA responds with a list of approved AIUs eligible for such consents. The user selects specific AIUs, provides associated validity and purpose details, and then confirms the action using secure credentials such as a PIN or OTP. The AIA then finalizes the consent creation and generates a signed DA consent record. Finally, the user receives confirmation of successful consent creation.



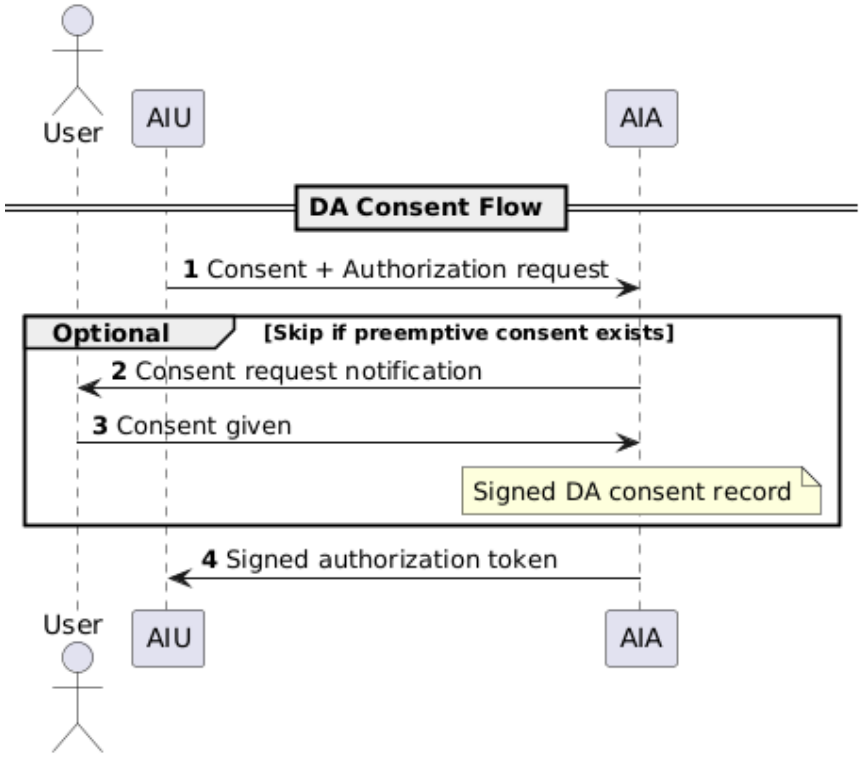
AIII.5. Service Request

The flow starts when a User submits a service request along with their Digital Address (DA) to an AIU. The AIU forwards this request to the CM to discover the associated AIP and AIA for the given DA. The CM queries the AIP based on the suffix of the DA to retrieve relevant information. In response, the AIP returns the AIA details linked to the DA. Finally, the CM provides the AIU with the necessary AIP and AIA information.



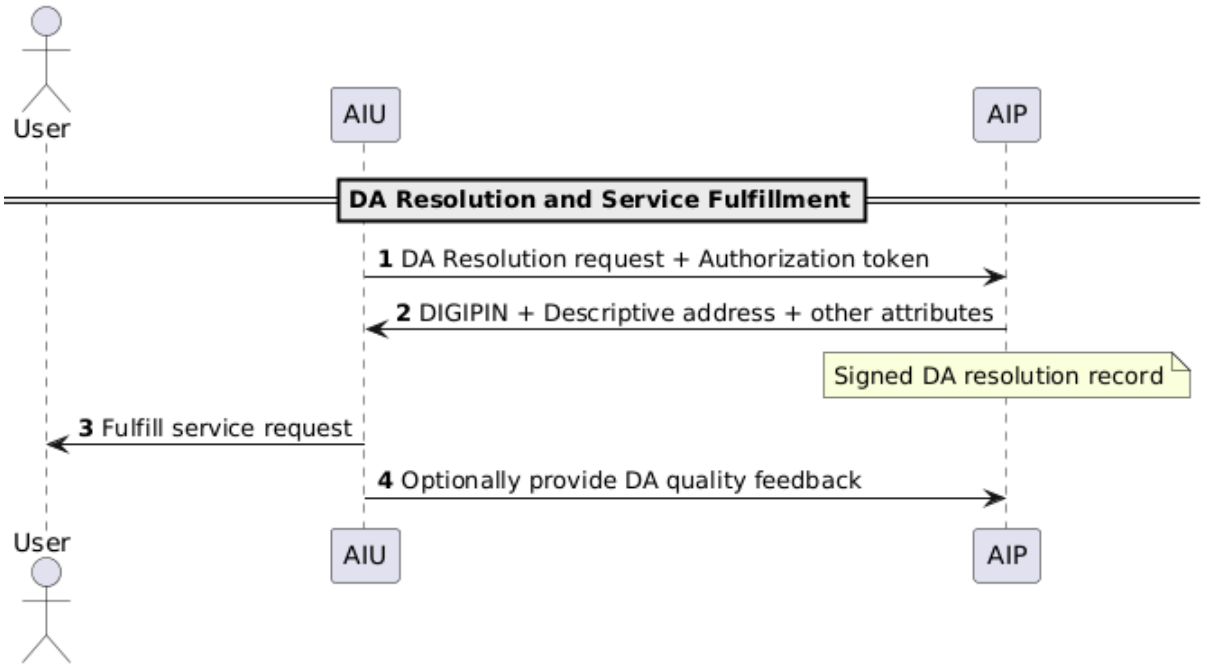
AIII.6. Digital Address Consent Flow

The flow initiates when an AIU submits a request for consent to resolve a particular DA to the concerned AIA. If a preemptive consent is not already in place, the system prompts the User with a consent request notification. The User then provides consent, which is logged by the AIA in the form of a signed DA consent record. Upon successful consent capture, the AIA returns a signed authorization token to the AIU. This flow ensures secure and auditable user consent for data access, while optimizing efficiency by bypassing redundant steps when preemptive consent is already granted.



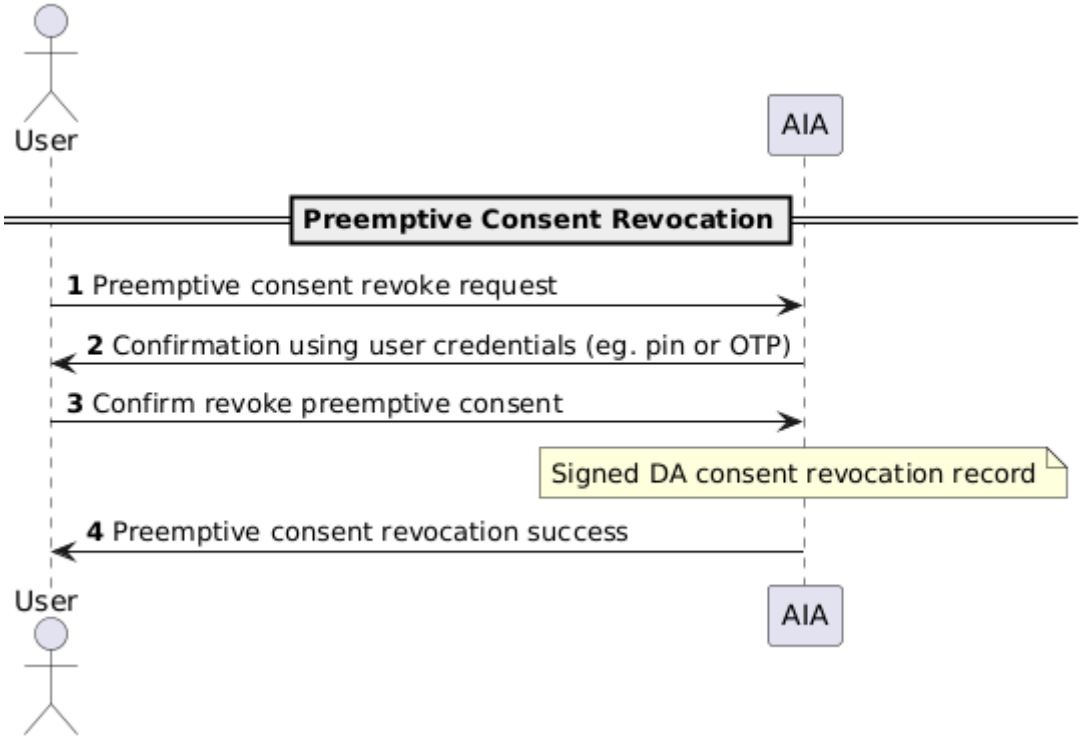
AIII.7. Digital Address Resolution & Service Fulfillment

The flow begins when an AIU sends a DA resolution request along with an authorization token to the AIP. In response, the AIP returns the resolved DA details, which include the DIGIPIN, a descriptive address, and other relevant attributes, along with generating and logging a signed DA resolution record to ensure accountability and auditing. With the resolved information, the AIU proceeds to fulfill the user's service request. Optionally, the AIU may also provide DA quality feedback to the AIP to help maintain or improve address accuracy. This process ensures secure, verifiable, and efficient resolution of digital addresses for service delivery.



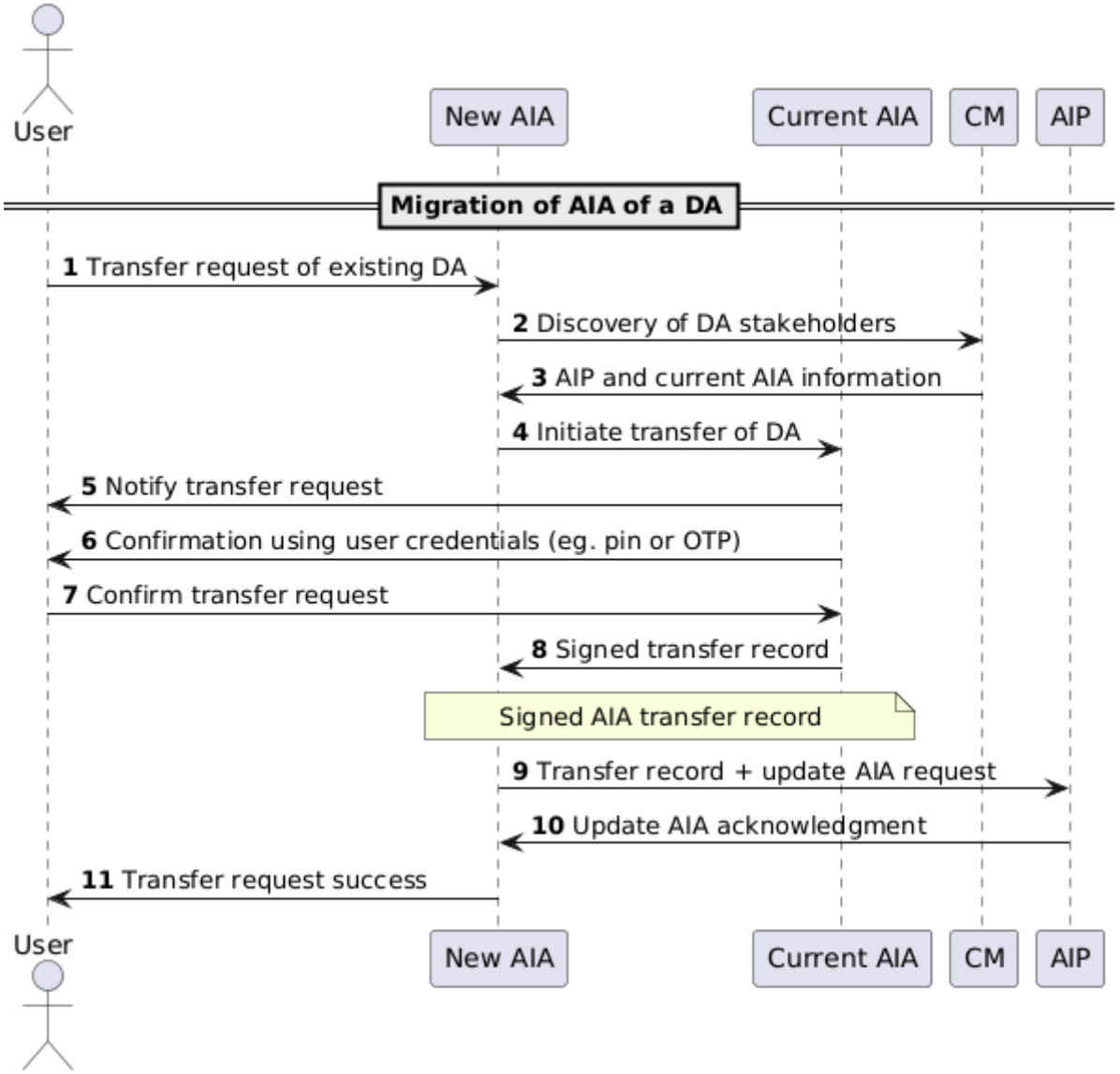
AIII.8. Preemptive Consent Revocation

The flow begins when the user initiates a request to revoke previously granted preemptive consent. The AIA responds by prompting the user for confirmation using secure credentials such as a PIN or OTP to verify intent. Upon successful verification, the AIA processes the revocation and generates a signed DA consent revocation record, ensuring tamper-proof logging of the action. The user is then notified of the successful revocation. This process ensures that users retain full control over their data sharing permissions, enabling secure and accountable withdrawal of prior consents



AIII.9. Migration of AIA of a Digital Address

The flow is initiated by the user submitting a transfer request for an existing DA. The new AIA begins by discovering the DA's associated stakeholders, retrieving information about the current AIA and the AIP. The transfer process is then initiated by the current AIA, and the user is notified. The user confirms the request using secure credentials (e.g., PIN or OTP), and upon validation, a signed transfer record is generated and shared with the new AIA. This record is sent to the AIP for updating the DA's ownership metadata. The current AIA acknowledges the update, and the new AIA confirms the successful completion of the migration to the user. This flow ensures a secure and traceable handover of control between AIAs while maintaining the integrity and authenticity of the DA's lifecycle.


User
New AIA
Current AIA
CM
AIP
Migration of AIA of a DA
1 Transfer request of existing DA
2 Discovery of DA stakeholders
3 AIP and current AIA information
4 Initiate transfer of DA
5 Notify transfer request
6 Confirmation using user credentials (eg. pin or OTP)
7 Confirm transfer request
8 Signed transfer record
Signed AIA transfer record
9 Transfer record + update AIA request
10 Update AIA acknowledgment
11 Transfer request success
User
New AIA
Current AIA
CM
AIP

References

1. Digital Address Project : White paper on Legal issues by VIDHI Centre for Legal Policy
2. DIGIPIN : https://www.indiapost.gov.in/VAS/Pages/digipin.aspx
3. Digital Address Project : Policy Document by VIDHI Centre for Legal Policy : https://www.indiapost.gov.in/VAS/DOP_PDFFiles/IP_30052025_Digipin_English.pdf
4. https://www.npci.org.in/PDF/npci/upi/circular/2025/UPI-OC-No-193-C-FY-24-25-Addendum-to-OC-193-compliance-to-UPI-technical-specifications-TRAN-ID.pdf
5. https://www.cl.cam.ac.uk/~mgk25/iso-14977.pdf
6. National Digital Health Blueprint : Ministry of Health and Family welfare : https://abdm.gov.in:8081/uploads/ndhb_1_56ec695bc8.pdf
7. Wiz.io - MIT Licenses Explained : https://www.wiz.io/academy/mit-licenses-explained
8. Apache License 2.0 : https://fossa.com/blog/open-source-licenses-101-apache-license-2-0/
9. What is the AGPL License? : https://fossa.com/blog/open-source-software-licenses-101-agpl-license/
10. Kubernetes : https://kubernetes.io/
11. RabbitMQ : https://www.rabbitmq.com/
12. PostgreSQL : https://www.postgresql.org/
13. Vert.x : https://vertx.io/
14. Keycloak : https://www.keycloak.org/
15. ImmuDB : https://immudb.io/
16. NGINX : https://nginx.org/en/
17. Prometheus : https://prometheus.io/
18. Grafana : https://grafana.com/
19. Loki : https://grafana.com/docs/loki/latest/
20. OWASP Secure Coding Practices Checklist : https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist
21. OWASP Top Ten : https://owasp.org/www-project-top-ten/
22. NISTIR 8397 Guidelines on Minimum Standards for Developer Verification of Software : https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=933350
23. G-NAF - Geoscape Geocoded National Address File : https://geoscape.com.au/solutions/g-naf/
24. Estonian Address Data System - https://geoportaal.maaamet.ee/eng/spatial-data/address-data-p313.html