DHRUVA

Digital Hub for Reference & Unique Virtual Address

The Digital Address DPI: Policy Document

Department of Posts
Ministry of Communications

May, 2025

Table of Contents

Table of Abbreviations

Abbreviation	Full Form
AaaS	Address as a Service
AAVA	Authorized Address Validation Agency
ABDM	Ayushman Bharat Digital Mission
AIA	Address Information Agent
AIP	Address Information Provider
AIU	Address Information User
API	Application Programming Interface
CM	Central Mapper
DHRUVA	Digital Hub for Reference & Unique Virtual Address
DIGIPIN	Digital Postal Index Number
DPDPA	Digital Personal Data Protection Act, 2023
DPI	Digital Public Infrastructure
GIS	Geographic Information System
GNSS	Global Navigation Satellite System
KYC	Know Your Customer
NHA	National Health Authority
NPCI	National Payments Corporation of India
ONDC	Open Network for Digital Commerce
PIN	Postal Index Number
SDG	Sustainable Development Goal
UIDAI	Unique Identification Authority of India
UPI	Unified Payments Interface
UPRN	Unique Property Reference Number
UPU	Universal Postal Union

PREFACE

Addresses are a critical component of communication. Over time, they have evolved to take different formats, from informal references such as landmarks, to developing street names and door numbers. Beyond its immediate utility in enabling communication between two or more parties, addresses now serve a wider role in the day-to-day functioning of society. In many countries, including India, the workflow of delivering services and benefits to people has increasingly shifted to doorstep delivery, enhancing accessibility and overcoming barriers to equitable access and economic and social inclusion.

Despite the centrality of address information in everyday life, frictions exist in how such data is managed, shared and used across India. These challenges stem from multiple factors, including the country's vast cultural and linguistic diversity, the use of inconsistent address formats, and the fragmentation of address data across siloed systems. To overcome these barriers, India requires a unified, interoperable approach to address management – one that enables flexible representation of addresses, places user interest at its core, supports innovation, and facilitates wide usability. Recognizing address information management as a key component of public infrastructure, the Government of India proposes to develop a digital public infrastructure (DPI) that supports the traditional addressing system by enabling users to depict and share their addresses in a standardized and geo-coded format. It enhances address precision, reduces errors in communication, and simplifies service delivery.

This Policy Document provides detailed insights into Digital Hub for Reference & Unique Virtual Address or DHRUVA – the proposed DPI for address information management in India, including the design principles, key interfaces, and the legal and policy safeguards necessary for its safe and effective functioning. The Policy Document affirms the Government's commitment to privacy by design, user-centricity and transparency in the development and implementation of DHRUVA. Further, by prioritizing interoperability and minimizing access barriers, DHRUVA aims to catalyze innovation.

Given the widescale and cross-sectoral benefits which DHRUVA can deliver, this Policy Document is being released for public consultation. The Government invites feedback from the public, industry, civil society, and subject matter experts to ensure that DHRUVA reflects diverse needs, fosters inclusive adoption, and upholds constitutional and legal safeguards.

Unlocking the Power of Address Information for a Digital and Inclusive India

Overview

Address information plays a foundational role for both public and private sector service delivery, and in enabling improved user experience. In a rapidly digitizing and urbanizing society, precise and reliable address information is essential for inclusive growth, efficient governance, and improved quality of life. India's current addressing system, long constrained by legacy formats, inconsistent standards, and overreliance on informal landmarks does not align with the growing demands of a digital economy. The absence of a standardized, scalable, and digital-first infrastructure results in inefficiencies, risk of exclusion, and missed opportunities.

There is a clear and urgent need to treat address information management as a core layer of public infrastructure, one that is designed, governed, and maintained at par with other foundational systems such as digital identity or payments. This requires rethinking not just the technical representation of an address, but the institutional and governance frameworks that support it. It calls for an approach that transcends outdated addressing conventions, towards a user-centric digital architecture with institutional and governance features that prioritizes user privacy and supports innovation across sectors. A modern address management ecosystem must also empower individuals to manage, use and share their address information with trust and agency. It must enable equitable access to public services and unlock system-wide value, without compromising on user autonomy and security. This document sets out the pathway for building such an ecosystem by reimagining the role of address data in shaping a more inclusive and responsive digital economy.

Vision

To establish a standardized, interoperable geocoded addressing system that supports secure, consent-based and seamless sharing of address information, empowering users with meaningful control over their address data.

Mission

1. To recognize address information management as a core public infrastructure essential for effective governance, inclusive service delivery, and improved user experience.
2. To develop an address data sharing and management ecosystem that supports seamless integration across public and private sector.
3. To promote user autonomy through secure and consent-based sharing of address information, that can support innovation and user convenience and promotes ease of living.
4. To foster a collaborative ecosystem of public and private actors co-creating user-centric solutions built on a secure and trusted digital address infrastructure.

Introduction

An address is structured information that allows the "unambiguous determination of an object for purposes of identification and location"[1]. It represents a location in a form that can be understood and interpreted for the purposes of navigation, delivery, and governance in modern society. It is a fundamental component of public infrastructure, playing a crucial role in postal operations, navigation, service delivery, governance and economic activity. The Universal Postal Union ('**UPU**') has recognized that address infrastructure forms an important basis for society's functioning, and that addresses can help in the development, support, and implementation of critical national policies. Due to its non-rivalrous, non-excludable nature, and its positive externalities which enables the delivery of both public and private services, the UPU argues that address infrastructure qualifies as a public good and should be treated as an essential component of national infrastructure and planning[2].

Address information is increasingly relevant to India's development trajectory. In India's rapidly digitizing and urbanizing context, address information plays a significant role in the interaction of citizens with the Government and markets. However, address data remains an underexplored domain and is often treated as a secondary input rather than a primary enabler of development. A robust, structured and digitally enabled addressing system has the potential to unlock significant efficiency gains across sectors, promote inclusion and can be a key enabler for Viksit Bharat. India's digital transformation has been anchored in its ability to leverage technology to build scalable public infrastructure layers to address foundational gaps, such as Aadhaar for identity, Unified Payments Interface ('**UPI**') for digital payments, and the Ayushman Bharat Digital Mission for health data management ('**ABDM**')**.** Address reform is the next step in this journey, which can help strengthen public administration, improve service delivery, and enable a more connected, inclusive, and efficient economy**.**

In this regard, there has been growing recognition that address is not merely a back-end enabler of service delivery, but a critical component of public infrastructure that can support existing priorities while opening up new pathways for inclusive growth and digital governance. For instance, the National Geospatial Policy (2022) acknowledged geospatial data as a critical national infrastructure and information resource, with wide-ranging social and economic value.[3] Together, these efforts signal a broader shift in policy thinking which treats address as an active attribute to be designed, governed, and utilized for public value.

1. Addressing System in India | A Case for Reform

1.1. The Addressing System in India

India's addressing system is a complex blend of administrative formats, informal practices and user-generated descriptions. The Postal Index Number codes ('**Pincodes**'), which were first introduced in 1972 for the purpose of mail sorting, are now widely used in addressing.[4] While the postal address format (linked to administrative boundaries such as village, taluka, district and Pincodes) used by the Department of Posts, Ministry of Communications, Government of India provides a basic framework, there is variation in how addresses are expressed in rural and urban areas. Urban addresses typically include a house number, street name, locality, and city, but this structure can also vary widely depending on regional conventions and legacy planning patterns. In rural and peri-urban areas, addressing is often descriptive, using landmarks and proximity references in place of standardized formats. Separately, service providers, such as e-commerce and navigation applications have introduced their own addressing methods, such as auto fetching and Global Navigation Satellite System ('**GNSS**') pins, to facilitate address discovery, and delivery. These parallel systems coexist in a fragmented but functionally interlinked ecosystem.

1.1.1. Challenges of the Existing Addressing System in India

Despite its functional resilience, India's addressing ecosystem remains fragmented, largely informal, and dependent on local knowledge. While this has allowed communities to communicate address information in informal formats and adapt to diverse geographies, it also means that the knowledge remains localized and protected from optimization, precision, interoperability, or digital integration. The limitations of this almost 'ad-hoc' approach have become increasingly evident as digital infrastructure for delivery of services increasingly becomes central to governance and commerce, and across sectors like logistics, public welfare, emergency responses, and for urban planning activities such as provision of civic amenities. As a result, the need for a more structured, machine-readable, and user-friendly addressing layer has become more imminent.

This foundational gap between convention and adaptation has exposed several structural and functional limitations in the prevailing addressing practices, which are highlighted below:

Dependence on Administrative Boundaries: Descriptive addresses rely heavily on administrative boundaries, such as a city, district, State etc. When administrative boundaries are altered, or there is a name change, a corresponding change in the address follows. However, residents may continue using outdated administrative identifiers, resulting in errors or delays in service access. These challenges become a matter of concern for citizens while applying for official documents, or for benefits under a location-specific scheme.

Challenges with Pincode Precision and Coverage: Based on the Department of Posts' estimates, the area covered by a Pincode in India varies, from a few sq. kms to thousands of sq. kms, with an average cover of around 170 sq. km per Pincode. This extensive coverage of area per Pincode may impact the precision and accuracy for last mile deliveries, particularly in densely populated urban areas, or sparsely populated rural areas. Further, persons may not be aware of a change in the Pincode, which is the result of the opening of a new post office in an area. The use of outdated or incorrect Pincodes can pose challenges for the post office to service their customers and also leads to user inconvenience.

Linguistic Fragmentation and Translational Inconsistencies: India's rich linguistic diversity influences addressing practices as well. While this reflects cultural and linguistic convenience, it impedes the use of this information for administrative and logistical purposes. People who are not conversant in the local language will face the additional hurdle of having to rely on translations, phonetic spellings, or non-standard transliterations, all of which potentially increase the room for error.

Incompatibility with Machine-Readable Systems: Addressing systems in India are descriptive and they rely on narrative conventions, local knowledge, and spatial approximations that are optimized for human interpretation. Supplying address information in the same format to a digital interface does not improve addressing accuracy or result in standardization. Prevailing address formats are therefore poorly suited for integration with digital platforms, which have become the primary vehicle for service delivery across public and private sectors. Therefore, meaningful digitalization of processes and automation of services that rely on address information is hindered.

1.1.2. Impact of the Existing Addressing System on India

Issues with the existing addressing system in India, highlighted above, have cross-cutting implications. As a critical part of the public infrastructure, address information shapes the contours of who is seen and served, especially where speed, accuracy, and scale are essential. The limitations of the addressing system discussed above have consequences across governance, inclusion, and economic participation.

Disrupted Delivery of Services: In the absence of a consistent and standardized addressing system, services such as postal delivery, e-commerce, logistics, and utilities encounter challenges in reaching end-users. These inconsistencies directly impact operational efficiency and beneficiary convenience.

Increased Operational Costs: The lack of a standardized and machine-readable addressing system increases operational costs and inefficiencies. For instance, sorting of articles received in post offices for delivery is a labour intensive and time-consuming process, vulnerable to human error. Additionally, where sequencing of items for delivery of articles is done manually, similar issues persist. In the absence of a standardized automated address validation at the time of postal booking, even a minor ambiguity in address details may lead to processing delays and misrouting. Without a digitalized system to track and optimize delivery routes, there is suboptimal use of resources, leading to inefficiencies.

Delayed Response to Emergencies: Accurate and precise location information is vital for emergency response and care. Landmark based addresses are often unreliable (for reasons discussed above), especially during natural disasters when reference points may be damaged, altered or displaced. This leads to delays in reaching affected individuals and delivering critical care.

Hindered Access to Essential Services: In remote or under-served areas without standardized addressing formats, households may lack a clearly expressed address with an identifiable location. This impedes the ability of service providers to effectively serve such areas. Consequently, the residents in such areas face the prospect of potentially being excluded from access to essential services (like emergency medical services) and economic opportunities.

Systemic Inconsistencies leading to User Inconvenience: Without a standardized approach to addressing, each sector currently collects and manages address data in silos, using inconsistent formats that are incompatible across systems. End users are burdened with repeatedly furnishing the same address information, often in different formats, while service providers lack the tools to validate, reuse, or coordinate that information efficiently.

These bottlenecks not only result in inefficient use of resources but also hinder effective, citizen-centric public administration. A 2018 study estimated that the inefficiencies caused by a poor addressing system may cost India between $10–14 billion annually, approximately 0.5% of GDP.[5]

1.2. The Need for a System to Manage and Use Address Information

The challenges and inefficiencies highlighted above may be attributed to the lack of a shared system for writing, managing and using address information, which can otherwise enable precise, interoperable and reusable address data. Addressing this gap requires a unified, technology-enabled ecosystem that allows for structured address data collection, management and seamless sharing across platforms while upholding privacy and ensuring compliance with applicable laws.

The gains from such a reform will be manifold. Standardizing addresses and providing a digital infrastructure for address information management is expected to have a direct beneficial effect on both governance and service delivery as discussed subsequently in this document. Beyond operational efficiency and user convenience, such a system would trigger cross-sectoral collaboration. With this background, addressing system reform, therefore, is not simply a matter of technical or administrative necessity - it will lead to the establishment of a foundational layer upon which equitable access, responsive and efficient governance, and seamless service delivery can be built.

Various countries have also recognized the need for standardizing and reforming the addressing system through a technology-based approach, reinforcing the importance of a robust address information management system as a part of national infrastructure. The National Address Database in the United States of America,[6] and the Geocoded National Address File in Australia[7] employ geocoding of addresses based on the underlying latitude and longitude coordinates of a given location. In Ghana, GhanaPost GPS has been designed as a mechanism for generating alphanumeric identifiers for addresses based on geospatial coordinates, by dividing the entire territory of Ghana into blocks of approximately 5m * 5m.[8] In certain countries, addressable locations are assigned unique identifiers. In the United Kingdom, under the National Address Gazetteer, a Unique Property Reference Number ("**UPRN**") is assigned to every addressable location in the country.[9] Similarly, in Estonia, all addresses are assigned a unique alphanumeric identifier, which is stored in a database along with the descriptive address.[10] These initiatives differ in terms of the modalities of what and how address information can be stored, accessed or shared, depending on applicable legal systems and national priorities in different countries.

However, the common denominator of all such initiatives lies in the benefits that standardization in address information management and digital infrastructure affords to service providers, end users and the Government. For instance, in the United States of America, the National Address Database seeks to support a broad range of government services such as postal, emergency services, prompt healthcare response and delivery, last-mile broadband delivery, school districting etc.[11] On similar lines, the National Address Gazetteer is geared towards ensuring efficiency in delivery of emergency and postal services, and ensuring optimal allocation of resources.[12] In Ghana, GhanaPost GPS is being envisaged as a solution for providing targeted delivery of emergency services, as well as providing a uniform addressing system for streamlining access to financial services and opening bank accounts.[13] In a nutshell, the global experience highlights the increasing emphasis on a technology-based, structured address information system to deliver cross-sectoral benefits.

For India to unlock the aforesaid potential, such an addressing system must comply with the core principles discussed below:

- The system must be based on a common technical standard that allows for interoperability across platforms in different sectors. This is important to develop a consistent and standardized approach to addressing that can be easily adopted by multiple stakeholders.

- End-users must have meaningful control over their address data, which must be processed only with the informed consent of the user. Users must have control over who can access their address information and have the option to revoke such access.

- There must be strong safeguards to ensure the privacy and security of the information shared over the system. The system must be compliant with applicable laws such as the Digital Personal Data Protection Act, 2023 (‘**DPDPA**’).

- The architecture must be future-proof, allowing the system to expand and adapt to new use cases without requiring major structural changes. It should support innovation and application development across a wide range of participating entities.

- The system should be developed through a collaborative approach that brings together public institutions and private innovators. This will help in building a system which addresses cross-sectoral needs, prevent data silos, and foster interoperability.

- The system must be designed to serve all users equitably, ensuring access to digital technologies is not a barrier to participation.

- There must be institutional and governance structures with clear responsibilities, transparent processes, robust accountability measures, and accessible grievance redressal mechanisms, which are backed by law. This is essential to building user trust and ensuring the long-term legitimacy of the system.

1.3. The Case for a DPI Approach

A system to standardize and manage address information can be modeled in different ways, with each model varying in terms of the user control, adaptability, openness to innovation, and operational details they offer. In the private sector, proprietary address information management systems have evolved for varied purposes such as e-commerce, navigation, etc. While these systems offer high functionality within their respective ecosystems, they typically operate as closed, proprietary networks, with limited interoperability posing high entry barriers for new entrants and inhibited reusability outside the system. Limitations on scalability may also arise, impeding accessibility and inclusivity for users. On the other hand, certain jurisdictions have adopted a national-level, centralized model of address information management. For instance, in the United Kingdom, the National Address Gazetteer maintains descriptive addresses along with the unique identifier UPRN in a central database.[14] Jurisdictions like South Africa[15] maintain a database of address information while the United States follows a model where aggregated address information from individual States is maintained at the level of the Federal Government.[16] However, except for Ghana, none of the jurisdictions examined above allow users the ability to generate a user-defined label or identifier associated with the address. Instead, a top-down approach is generally followed, where either descriptive address information is stored centrally, or a unique identifier is assigned or managed centrally. While these approaches have proven effective within their contexts, they may not be suitable for India where geographic and socio-economic diversity requires a more flexible, user-centric approach. Further, such models may not be suitable for peer to peer sharing of address information at the level of the user.

In addition, some models place restrictions on the sharing of address information. Jurisdictions like the United Kingdom only allow for sharing of address information contained in the National Address Gazetteer within the public sector only,[17] thus hindering the ability of the private sector to capitalize on and build upon an ecosystem for generation and sharing of structured address information. In Australia, where the address data is made available freely, the use of such address data by third parties is subject to license conditions.[18]

As these examples show, adopting any of the models in totality may not align with India's approach towards digitalization and bringing about a transformation in both governance and the service delivery sector, although it is essential to be informed by the potential advantages that each model has to offer. An address information management system for India must be designed to support flexible address representation, place the user at the core of the ecosystem, support innovation and ensure wide usability, thereby facilitating seamless flow of structured and accurate address information. Therefore, it is important to adopt a system of standardizing and managing address information that aligns with these principles and parameters.

In this regard, the objectives and vision of a robust address information management model can be best fulfilled through a Digital Public Infrastructure ('**DPI**') approach. As defined in the 'Report of

India's G20 Task Force on Digital Public Infrastructure', 2024 ('**G20 Report**'), a DPI is "a set of shared digital systems that should be secure and interoperable, and can be built on open standards and specifications to deliver and provide equitable access to public and / or private services at societal scale and are governed by applicable legal frameworks and enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms."[19] In India, DPIs already exist in different sectors, such as the UPI for financial services, the ABDM in the health sector, and AgriStack in the agricultural sector.

The Hon'ble Prime Minister described the contribution of DPIs to inclusive growth as revolutionary, emphasizing that they must serve as bridges and not barriers.[20] This vision is reflected in India's globally recognized success in implementing the DPI based models in key areas. According to the G20 Report, a series of measures based on the DPI model, such as the introduction of UPI and Aadhaar-based identification and eKYC has laid the foundation of an inclusive digital economy. For instance, such measures have resulted in an increase in the proportion of adults in India having a bank account from 17% in 2009 to over 80% in 2017.[21] India's success story with the DPI approach highlights the DPI model's effectiveness in addressing long-standing structural challenges at population scale. For reasons discussed below, such an approach is well-suited for address management in India.

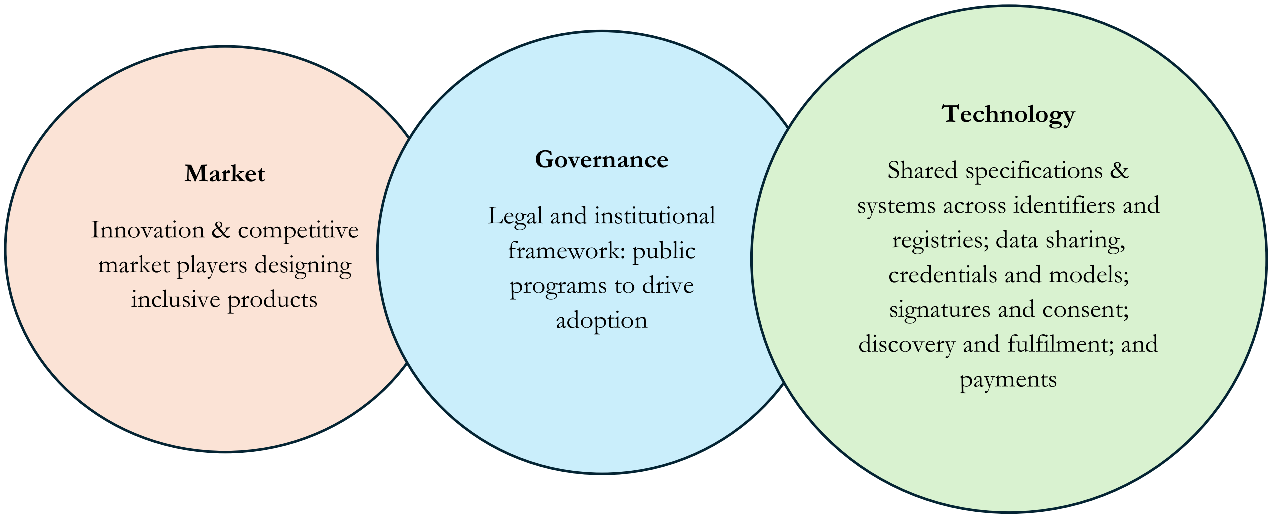
Market
Innovation & competitive market players designing inclusive products
Governance
Legal and institutional framework: public programs to drive adoption
Technology
Shared specifications & systems across identifiers and registries; data sharing, credentials and models; signatures and consent; discovery and fulfilment; and payments

Fig 1: Core Pillars of the DPI Approach

Source: Report of India's G20 Taskforce on Digital Public Infrastructure

Image Description: Three intersecting circles representing components of a digital public infrastructure model. The left circle labeled 'Market' reads innovation and competitive market players designing inclusive products. The centre circle labeled 'Governance' reads legal and institutional frameworks and public programs to drive adoption. The right circle labeled 'Technology' reads shared specifications and systems across identifiers and registries, data sharing, credentials and models, signatures and consent, discovery and fulfillment, and payments.

As set out in the G20 Report, a DPI is characterized by three basic elements: a shared technology design, robust and participatory governance, and market participation and innovation.[22] A DPI attempts to create an ecosystem that is built on open standards to ensure interoperability and is based on a federated architecture where data is stored at the primary point of collection, and not in a centralized repository. The building blocks in the architecture are assembled in such a manner that the entire ecosystem is evolvable and configurable and supports the building of tailor-made applications on top of the core skeletal infrastructure. As far as governance is concerned, the DPI must have a legal basis for its operation, with clearly defined institutional structures that delineate the roles and responsibilities of the participants. Compliance with the legal and regulatory structure is sought to be ensured by embedding obligations into code, such as limits on data flow within the ecosystem. Importantly, a DPI facilitates robust market participation, where the public and private sector can collaborate for effective and efficient delivery of services. A DPI approach for this solution can also mitigate entry barriers by reducing the cost of participation upfront. Risks which may have arisen out of monopoly pricing in the long run under a private sector-led model are thus assuaged under this model.

Such an architecture offers various benefits for address information management. The use of open standards enables seamless communication and coordination across systems, resulting in greater interoperability. This, in turn, enables the ecosystem to be flexible and amenable to newer use cases, thus fostering innovation. In addition, this makes it possible for a high degree of public-private collaboration, where the private sector can innovate within a regulated ecosystem.

Due to the focus on privacy and consent-based design, the user is afforded a greater degree of control over her address data in a DPI model. Further, due to the federated approach and the absence of a single point of failure, data security is enhanced to a large extent. This ensures that the user is placed at the front and centre of the ecosystem. Finally, due to its inherent flexibility, a DPI model ensures inclusivity and tailor-made solutions for users in order to bridge the digital divide and promote access to all, irrespective of disparity in technological access. All of these factors collectively, ensures that a high degree of legitimacy and trust in the eyes of the public can be achieved.

Thus, the DPI approach offers a balanced way forward that accommodates standardization and innovation, while preserving user rights and enabling collaborative growth. In India, the adoption of the DPI model has been instrumental in driving the nation's digital transformation, aligning seamlessly with its development agenda. By establishing foundational digital platforms like Aadhaar, the UPI, and DigiLocker, India has created an ecosystem that facilitates seamless delivery of services, promotes financial inclusion, and fosters innovation. This approach not only streamlines government-to-citizen interactions but also empowers private enterprises to build on these platforms, thereby stimulating economic growth and enhancing the ease of living. The success of these initiatives underscores the DPI approach's efficacy in creating scalable, interoperable, and inclusive digital solutions that cater to a diverse population.

Furthermore, India's experience demonstrates how a well-designed DPI can serve as a catalyst for achieving Sustainable Development Goals ('**SDG**s'), by bridging the digital divide and ensuring that the benefits of digitalization reach all segments of society. In the context of a DPI for standardizing and managing address information, it is envisaged that it can support progress towards the achievement of Goal 9 ("Industry, Innovation and Infrastructure") and Goal 11 ("Sustainable Cities and Communities"). As highlighted in the 'Introduction', the UPU recognizes address as an important part of national infrastructure for the society's functioning. Standardizing address information and enabling its seamless management and sharing, therefore, will work towards reducing entry barriers for both recipients of services and service providers seeking to reach untapped consumer groups. Subsequent parts of this document also highlight how this approach will support economic activities, which is a target set out under Goal 9. In the same vein, this approach can allow for better planning and execution of governance activities and play a critical role in disaster management and emergency response, which works towards creating sustainable cities and communities, thereby catalyzing the achievement of Goal 11.[23] Beyond these goals, it can support various other SDGs by enabling the delivery of welfare benefits and healthcare services. While the adoption of this model may have a more widescale impact given that the DPI approach will allow for further innovation led by market forces, its support for achieving SDGs is noticeable even at early stages of conceptualization. This positions the DPI model for an addressing system not just as a tool for technological advancement, but as a strategic framework integral to holistic national development.

2. DHRUVA - A DPI for Address Management

2.1. Introduction to DHRUVA

As discussed above, a DPI model is most suited to developing a technological solution to unlock the potential of address information for India. This section provides insights into the "Digital Hub for Reference & Unique Virtual Address" (**DHRUVA**), a DPI which is being designed to allow users to create, access, share, manage and use their address information.

DHRUVA is being designed by the Department of Posts to create a secure digital environment through which users can share accurate address information by leveraging a geo-coded framework. Its architecture can provide an alternative to the inefficient, costly, error-prone, and labour-intensive address information management practices mentioned in Section 1- with a simplified, digitalized process that boosts accuracy, user convenience and protects user information. By delivering this service through an open and interoperable architecture, DHRUVA creates an opportunity for structuring address information and creating efficiency in address information management across systems, akin to how barcodes standardized product identification information across systems of global commerce.

To deliver this service, DHRUVA is being developed as a technological ecosystem consisting of two key 'layers': the Digital Postal Index Number ('**DIGIPIN**') Layer and the Digital Address Layer ('**Digital Address**').

DIGIPIN is an open-source national-level standardized, geo-coded, interoperable addressing grid developed by Department of Posts in collaboration with the Indian Institute of Technology, Hyderabad and the National Remote Sensing Centre, Indian Space Research Organization. It is a 10-digit alpha-numeric code representing geographic coordinates (latitude-longitude), developed by creating uniform approximately 4x4 meter grids on India's territory. DIGIPIN uniquely identifies locations using geospatial data. Incorporating DIGIPIN as an additional address attribute to traditional addressing formats enables the leveraging of Geographic Information System ('**GIS**') capabilities, laying the foundation for future GIS-based digitalization of service delivery across various organizations in a cost-effective manner. The Department of Posts has already released the GitHub repository for the DIGIPIN grid. As a low-cost encoding solution developed on open protocols, the DIGIPIN layer is an efficient technological solution which is easy to adopt and implement.

In addition to the DIGIPIN layer, DHRUVA will also have a Digital Address layer ('**Digital Address**'). The Digital Address layer will be a user-centric, consent-based system built upon the DIGIPIN layer. It will allow users to generate unique and customized labels (such as username@domain) to represent their DIGIPIN and descriptive addresses and manage this information. Similar to how a UPI ID eliminates the need to accurately recall and rewrite one's account information every time while making a payment, the Digital Address will be designed to dispense with the need to rewrite address information repeatedly to avail of services. Moreover, since the Digital Address layer will be built on top of the DIGIPIN layer, users will also be able to share the geographical coordinates representing their address without having to recall the 10-digit alphanumeric code. Once a Digital Address is created by a user, it can serve as a single point of reference for users. Users will also be able to 'manage' their Digital Address - share, update their address information, or revoke their consent to sharing it through a unified interface. The ecosystem will be built to be entirely consent-based.

2.1.1. Objectives of DHRUVA

Establish a Unified Interface for Geo-coded Addressing: DHRUVA aims to introduce a foundational unified interface that enables the uniform encoding of addresses, by leveraging latitude and longitude coordinates for location identification. By doing so, it aspires to eliminate legacy inconsistencies and evolve to facilitate a unified standard for address representation in India.

Enabling Privacy, including by Design: Delivering privacy to users is not an afterthought in DHRUVA - it is foundational to the ecosystem, operationalized through its architecture, consent flows, and legal design. DHRUVA's objective is to provide a technological solution which aligns with the principles articulated in the Supreme Court's *Puttaswamy*[24] judgements and codified under the DPDPA. It embodies a "privacy by design" ethos: only data that is necessary is collected, all transactions are contingent on user consent, and control over address data remains with the user. This commitment to privacy manifests at multiple levels of its ecosystem. The technical architecture adopts a federated model which ensures that address data is not centralized but distributed, limiting vulnerabilities. The creation and use of Digital Address, including sharing of address information through this ecosystem, and its usage by the recipient will be through explicit user consent. Subject to applicable laws, users will also be able to update or withdraw their consent to share such information. At no point will address information be exposed to intermediaries beyond what the service requires.

Enhance Efficiency in Public and Private Service Delivery: Through a geocoded addressing system, DHRUVA aims to streamline service workflows, be it for last-mile deliveries, emergency responses, effective service request routing, or to facilitate KYC ('**Know Your Customer**') for amenable sectors. This enables optimized logistics and lowers costs across critical sectors that currently struggle as a result of legacy addressing standards.

Strengthen Decision-Making Through Address Intelligence: DHRUVA is expected to be an enabler of geospatial governance. By unlocking the power of geospatial intelligence, it enables informed decision-making on key governance priorities such as welfare distribution, citizen safety, and economic efficiency, including optimal resource allocation. In the case of area-specific welfare schemes in remote regions, for instance, shifting administrative boundaries or challenges in identifying beneficiary locations can hinder the disbursal of benefits. Through DHRUVA, beneficiaries will be able to share accurate and standardized address information, allowing better planning, more responsive workflows to ensure services reaches its intended recipients.

Enable Ecosystem-wide Interoperability and Innovation: DHRUVA aspires to unlock new possibilities for address data related services in much the same way as the UPI has triggered an explosion of bundled financial services. By providing a foundational technological layer complete with published, open APIs and consent-based protocols, it aims to eliminate barriers to entry for new players. As a result, innovators can integrate high-quality, geo-coded address data, or address accuracy to expand their service offerings vertically and horizontally or offer new forms of services altogether to end users, and offer Address-as-a-Service ('**AaaS**'). AaaS is the array of services associated with address data management to support secure and efficient interactions between users, government entities, and private sector organizations. This approach incentivizes innovation, fosters competition, and invites cutting-edge solutions that may not have been accessible under conventional addressing systems.

***Support Inclusive and Equitable Development*:** Reliance on the geo-coded addressing framework will bridge the urban-rural divide by enabling the government to effectively reach geographically remote or underserved regions - an objective central to DHRUVA's mission. Rural areas, which may lack structured addresses making them difficult to serve both for public and private entities, are an important intended beneficiary of DHRUVA. Complemented with an accessible interface by design, such as minimal data entry points and representation in regional languages, DHRUVA aspires to ensure that all citizens, can access and benefit from digital governance and targeted public service delivery.

Facilitate Trust and Consistency in Digital Addresses: The DHRUVA ecosystem creates a well-structured network of key players with the user at its centre. By adopting a federated architecture operating on uniform protocols and common validation layers for assigning Digital Addresses, the ecosystem proactively delivers consistency and reliability at scale. These measures, delivered through open APIs will instill confidence for users, and across government and private domains, enabling high integrity, efficiently delivered services for all.

Promote Scalability, Public-Private Collaboration and Future-Readiness: DHRUVA is being designed to handle exponential increases in Digital Address creation, updates, and verifications over time. Its governance framework and modular design are poised to evolve with emerging technologies – fostering long-term sustainability and continuous updates that can integrate with allied technological solutions and DPIs, as well as ensure seamless collaboration between the public and private sectors. The key outcome of DHRUVA, a precise address information shared in a minimalistic format, makes it a potent feature for integration across digital platforms. The ecosystem is therefore being developed for wide-scale adoption across India.

2.1.2. Key Interfaces

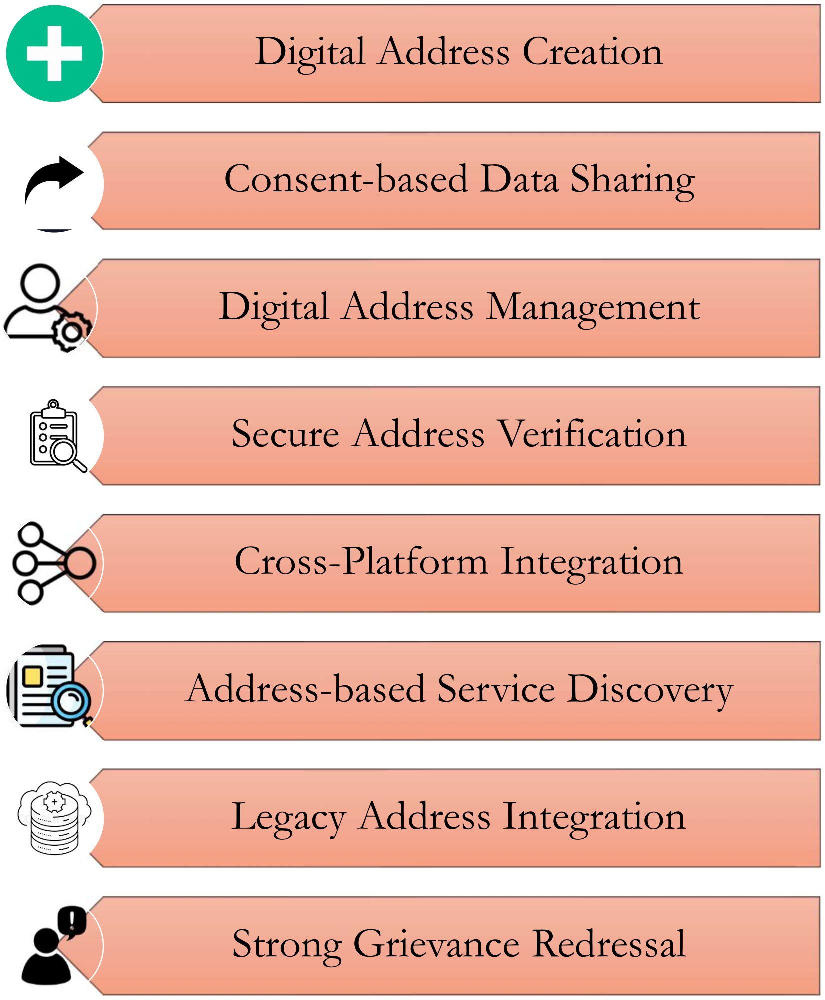
Digital Address Creation
Consent-based Data Sharing
Digital Address Management
Secure Address Verification
Cross-Platform Integration
Address-based Service Discovery
Legacy Address Integration
Strong Grievance Redressal

Fig 2: Key Interfaces for Users of DHRUVA

Image Description: A vertical list of eight key features of DHRUVA, each in a colored horizontal bar with an icon. The features are: Digital Address Creation, Consent-based Data Sharing, Digital Address Management, Secure Address Verification, Cross-Platform Integration, Address-based Service Discovery, Legacy Address Integration, and Strong Grievance Redressal.

DHRUVA is not conceptualized as a centralized platform, but a modular DPI that provides a diverse set of interfaces for streamlined address management and data exchange. Each interface functions as a core building block, allowing diverse stakeholders from everyday users to businesses and public sector agencies to securely access, validate, and share address information in a structured and efficient manner. In addition to sharing structured address information with service providers, DHRUVA also enables seamless peer-to-peer sharing of accurate address information among users in a secure manner. This enhances user convenience, in that users would not need to provide the full descriptive address in every situation, thus obviating manual errors in mistyping of textual addresses.

An overview of the key interfaces offered through DHRUVA can be found below:

Digital Address Assignment: The primary service offered by DHRUVA is the creation of Digital Addresses (e.g., johndoe@dhruva) which can communicate the descriptive address of the user (21, XYZ ROAD) and the DIGIPIN (latitude and longitude coordinates) to the recipient system. This ensures that every addressable point can be represented in a machine-readable, precisely geo-referenced format. The 'addressability' of a location is not contingent on rigid naming conventions or landmarks for referencing, since the geo-coded layer anchors each address to a definitive spatial reference. Therefore, DHRUVA offers the promise of enabling addressing of any location on the map of India.

Secure and Consent-Based Address Data Sharing: Designed with user-centric principles, DHRUVA offers complete control to the user over their address information. It enables users to regulate when their address information can be accessed, and the duration for which it can be accessed through a consent framework, subject to applicable laws. In order to ensure workflow efficiency for all players, it is envisioned that necessary processes will be developed to ensure that the system minimizes the risk of incorrect information and safeguards against unauthorized access. It also enables users to revoke access to their Digital Address, meaningfully restoring autonomy over the information. Users can also update their address information, minimizing administrative overhead. By offering simplified address management, the system elevates transparency and user autonomy across different use-cases.

Dynamic Address Management: DHRUVA reimagines address information as a user-controlled data point. Instead of treating address as static and siloed records, it enables individuals to seamlessly manage their address data. Users can update, share, or revoke their address information through a unified interface. By enabling granular control, this interface enhances the utility of DHRUVA, making it more responsive to the diverse and evolving needs of users and increasing adoption across sectors.

Secure Address Verification and Accuracy Checks: Accurate address information is foundational to the provision of a wide range of public and private sector services, since it enables them to streamline logistics, reduce operational risks and costs associated with inaccurate addresses, and fulfil obligations like facilitating KYC requirements. Recognizing this, DHRUVA incorporates technical and governance features to ensure the precision, consistency, and authenticity of address data across its ecosystem. These protocols span standardized, interoperable data formats, geospatial anchoring through the DIGIPIN grid, and systemic checks for anomalies. To complement these safeguards, a legal framework for address validation is also being envisaged, wherein legally authorized entities may validate the accuracy of address and location information. Importantly, such validation mechanisms are designed to establish the authenticity of the address itself, without revealing or linking the identity of the individual residing at the location, thereby upholding DHRUVA's foundational commitment to privacy. Another type of validation which is being explored is a 'Confidence Score' - a quantifiable value, which gives insights about the accuracy and precision of the address and location data attributes in the Digital Address layer, as reported through a feedback mechanism. Together, these measures constitute the backbone of trust for all ecosystem participants and ensure that address information serves as a reliable and secure layer for digital service delivery.

Integration with Public and Private Services: DHRUVA is being designed for seamless integration with both private and public sector platforms and applications through standardized, interoperable, open-protocol APIs. Its 'plug-and-play' design enables existing applications to adopt its services with minimal effort, eliminating high infrastructure cost which would be usual for an overhaul of the existing address management systems. Such integration also enables the delivery of AaaS, allowing platforms to enhance their service delivery by leveraging standardized address data and offer other address-related capabilities and bundled services, unlocking catalyzing innovation across sectors.

Address-Based Service Discovery: DHRUVA enables the discovery of different points of service, including nearby healthcare facilities or other utilities, in a single query. By enabling the mapping of each Digital Address to precise spatial data, it allows for the efficient identification of service points and hotspots to provide civic amenities and helps e-commerce and logistics platforms determine the nearest delivery hubs. This will allow service providers to rapidly locate relevant points of interest for any given address due to its geocoded foundation.

Legacy Address Onboarding and Harmonization: India's landscape of conventional addresses is reliant on colloquial descriptors, which makes standardization across platforms difficult. By ingesting these legacy addresses and converting them into structured, geo-coded forms, DHRUVA preserves continuity for existing databases while simultaneously elevating them to modern, shareable formats.

Robust Grievance Redressal Mechanisms: To strengthen user trust, DHRUVA will allow for grievance redressal processes that are integrated with multiple contact points (such as mobile apps, emails, and call centres), to enable service providers to swiftly and transparently resolve user complaints and queries.

2.1.3. Key Design and Governance Principles

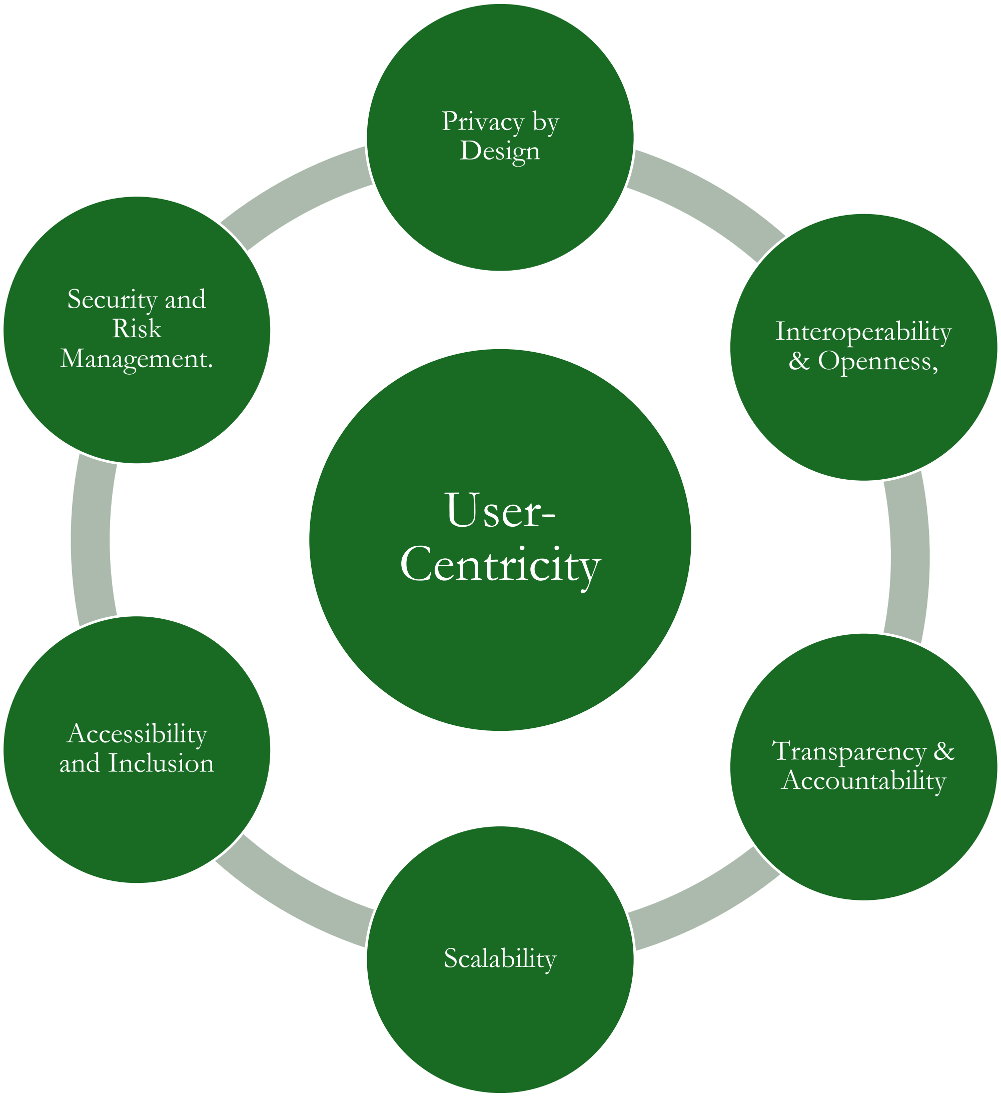
Privacy by Design
Interoperability & Openness,
Transparency & Accountability
Scalability
Accessibility and Inclusion
Security and Risk Management.
User-Centricity

Fig 3: Key Design Features of DHRUVA

Image Description: Circular diagram illustrating the key design principles of DHRUVA, with the principle of 'User-Centricity' at the center, surrounded by six interconnected outer circles representing key design principles: Privacy by Design, Interoperability & Openness, Transparency & Accountability, Scalability, Accessibility and Inclusion, and Security and Risk Management.

To ensure its successful implementation, a coherent set of guiding principles must lay a robust technical and governance foundation that prioritizes users, their rights, and their successful experience with the DPI. This will help in positioning DHRUVA for sustainable growth in the future. Defining these principles upfront will guide how DHRUVA is shaped, enhance trust, streamline stakeholder integration, reduce friction in adoption, align the ecosystem for evolving requirements, and ultimately facilitate effective governance across ecosystems into which DHRUVA is integrated.

The following core technical design and governance principles have been identified as essential for the successful implementation and sustainability of DHRUVA:

User-Centricity: DHRUVA is being designed around empowering users to control how their address information is shared, ensuring that all persons are able to access services which use address information, and that user convenience is maximized. The technical architecture of DHRUVA places the user at the centre, vesting all control to them through consent: users can grant, withdraw, withhold and modify consent to share their address information.

Privacy by Design: DHRUVA's ecosystem is being designed as a techno-legal artefact, which executes privacy through code. The underlying privacy principles which have been encoded across different layers and functions of DHRUVA - such as developing it as a data-blind mechanism to transfer address information, executing data transactions only through user-consent, and developing API protocols which preserve user privacy. To that end, the ecosystem is compliant with DPDPA and the judgement of the Supreme Court of India in *K.S. Puttaswamy v Union of India* [(2017) 10 SCC 1]. Principles such as data minimization, data retention, storage, purpose limitation, access, correction, and erasure, manifest through DHRUVA's features which users can access through the interface. It is also envisaged that the ecosystem will facilitate adequate legal recourse and grievance redressal mechanisms for users.

Interoperability and Openness: As a DPI, a key requirement of the ecosystem is that it should intuitively support private-public collaboration leading to innovation. Both the technical and governance framework of DHRUVA is being designed to support interoperability and openness. It is being designed on open protocols that will allow different platforms to "speak" to the ecosystem, and with each other through APIs. This functionality will ensure that information can be exchanged without any imposition of additional technical requirements on ecosystem participants, barring those necessary to ensure the safety of the information that is exchanged through it, limiting technical fragmentation. The institutional arrangement of DHRUVA and its legal framework is being situated in an industry-facing manner, supporting and replicating its technical openness. The standards and protocols for integration will be designed to enable seamless onboarding of platforms, ensuring broad access to its services while accommodating tech-neutral requirements. These integration thresholds will prioritize maintaining the integrity of the system, thereby preventing any systemic bias against select platforms or players and lowering the barriers to entry for new participants.

Transparency and Accountability: The values of transparency and accountability have been ingrained into the DHRUVA ecosystem's design. Technologically, the user exercises all control over their own information through a framework that obtains instructions through consent, as long as their data remains in the ecosystem. Transparency in the institutional arrangement, through clearly delineated roles of all entities participating in the DPI, ensures that their accountability to each stakeholder is unambiguous. Further information regarding the institutional arrangement and transparency guarantees can be found below in Section 3 of this document. This will be complemented with well-defined audit requirements, independent oversight mechanisms, and proactive grievance redressal procedures to ensure that the channels to exercise accountability remain accessible to all persons and entities.

Security and Risk Management: DHRUVA is being designed as a federated ecosystem rather than with a centralized repository, minimizing the points of vulnerability and ensuring that users retain control over their information throughout its lifecycle. The design and protocols include safeguards such as regular audits, appropriate compliance thresholds, and proactive monitoring mechanisms across the ecosystem and among integrated external actors. These measures collectively work to identify and address security risks in a timely manner and reduce systemic vulnerabilities.

Scalability: DHRUVA is being built to support scalability. The ecosystem's technology stack and legal and governance framework supports the onboarding and integration of a diverse set of sectoral players and users. Modularity and flexibility in its design, such as open API protocols, and regular feedback loops to foster collaboration will ensure that DHRUVA can respond quickly to technological innovations, policy shifts, and the evolving requirements of both the public and private sectors.

Accessibility and Inclusion: One of DHRUVA's primary objectives is to deliver addressability to every location in India. Remote locations or developing or underdeveloped regions are likely to be sites where addressing information is either too complex, or hyper localized resulting in isolation. The geo-coded layer circumvents users' needs to rely on context clues to accurately identify a location, ensuring that the institutional/regional knowledge which may be required for locating an address is eliminated. By default, this increases accessibility for service providers and enables them to expand the demographic and geographic groups they can offer services to.

In some ways, DHRUVA's Digital Address layer draws from the UPI model adopted in the financial sector, where users' inconvenience with recording and recalling banking information and sharing it was resolved by abstracting complex layers of information with one short string in a format (johndoe@okbank) with great recall value and minimal margin of error. It imitates this feature, ensuring that hurdles in sharing address information are eliminated. This has a direct impact on the inclusion of users who may face difficulty due to legacy addressing standards that require them to have access to literacy skills. Abstracted information, in a format with low requirements to possess recall value, will ensure that more users will now be able to access services by overcoming those barriers.

2.2. Benefits and Use-Cases of DHRUVA

Address information is a fundamental component of infrastructure, governance, and commerce. Therefore, standardization and improvements in addressing processes do not have an isolated impact but reverberates throughout society and manifests in different forms in these sectors and beyond. The layered, federated, and interoperable architecture of DHRUVA will therefore ensure that its benefits are translated smoothly for all stakeholders in a manner which is best suited to their needs. A multitude of use cases can be identified for DHRUVA, subject to legal and regulatory requirements, including applicable verification and KYC procedures. Its legal and governance structure may identify possible areas where seamless integration of the ecosystem with other sectors can be achieved in a legally sustainable manner.

The following outcomes, benefits, and use-cases provide a basic understanding of the transformative value of DHRUVA.

2.2.1. Benefits for Users

DHRUVA can empower citizens by removing long-standing barriers to accessing essential services that rely on accurate address information. When adopted by relevant Ministries and Government agencies, subject to sectoral requirements on KYC and verification, DHRUVA can result in advantages in terms of service delivery and user convenience. For many, especially those in informal settlements or frequently shifting residences, updating an address may lead to challenges in receiving services and benefits or accessing timely deliveries. By allowing individuals to generate a secure, standardized and interoperable Digital Address that they can control, DHRUVA can reduce dependence on physical documents, local knowledge, or other intermediaries who may be necessary for sharing addressing information. Citizens will not need to repeatedly fill out forms or stand in queues to update their address information across different services. Instead, a unified interface can be used to reflect changes. This also means faster access to services, fewer errors in deliveries, and a more efficient interaction with systems that previously caused inconvenience. In doing so, DHRUVA can help bridge systemic gaps in governance and inclusion, ensuring that every person regardless of where they live can participate fully and confidently in the digital and physical economy.

Use Cases of DHRUVA for Citizens

- ***Changing Address after Relocation:*** Workers and employees who move residences frequently can update their addresses in applicable systems via a digital interface. This one-step sharing can work across services preventing long wait times and reducing the scope of errors in address sharing.

- ***Accessing Subsidies in Remote Settlements:*** Beneficiaries living in informal settlements, for instance, in hilly regions or outside urban limits, can become more visible for targeted welfare delivery, such as LPG connection schemes or housing benefits by sharing their Digital Addresses.

- ***Booking a Medical Home Visit:*** Elderly people who wish to avail health services at home can share their geo-tagged Digital Address to enable accurate location through a one-click system where they may struggle to use complex interfaces or type in their address precisely.

- ***Real-Time Consent Withdrawal for Address Use:*** A user who has shared their Digital Address with a logistics service provider for one transaction can easily withdraw consent to retain or reuse that data.

Illustration 1: Improving Emergency Response Routing through Structured Address Data

Emergency response services often rely on caller-provided location descriptions, which are unstructured and prone to misinterpretation. This leads to critical delays, particularly in areas without formal street signage or where address formats vary widely. DHRUVA enables users to generate a standardized, interoperable geo-coded Digital Address that is machine-readable and linked to precise coordinates via a DIGIPIN. Emergency dispatch systems can access this data to retrieve exact latitude-longitude details and route vehicles directly to the location, eliminating the dependency on manual interpretation. In environments where response time is a direct determinant of outcomes, DHRUVA can remove address-based ambiguity and makes location intelligence accurate, and serviceable. This can lead to faster and more consistent emergency response operations across geography types.

Illustration 2: Enhancing Visibility of Decentralized Public Service Centres

In areas where addressing conventions are not well developed or are inconsistent, locating public service centres such as health camps, skill training hubs, or Aadhaar enrolment offices may often be difficult for citizens. Their discovery is typically dependent on SMS alerts, physical banners, or word-of-mouth, which do not scale well and are easily missed. With DHRUVA, these centres can be assigned easily shareable Digital Addresses, anchored to a DIGIPIN for precise discovery using any map-based or search-enabled application. These addresses are short, standardized, interoperable and machine-readable, making them compatible with digital flyers, public dashboards, and chatbot-based helplines used by citizens. Since users can search by either the label or underlying DIGIPIN, it removes the ambiguity often associated with manually typed inputs. Public service portals and mobile apps can embed DHRUVA-based address pickers or drop-downs that display currently active service centres nearby without relying on users to interpret vague descriptions. This allows service sites to be accurately located even in dense, unstructured areas, improving citizen turnout and reducing missed opportunities for enrolment or access.

2.2.2. Benefits for Governance

DHRUVA can equip governance systems with a foundational layer of precision, consistency, and user control, enabling more responsive, efficient, and citizen-centric administration. By replacing fragmented and unreliable address records with a unified, geo-coded standard, it can reduce operational inefficiencies that have long hindered public service delivery from welfare disbursements to emergency response. With standardized and interoperable address data, government bodies can eliminate redundancies, reduce accuracy related burdens, and coordinate more effectively across programs. This not only improves speed of service delivery but also strengthens strategic planning and allocation of resources, whether for infrastructure, urban development, or welfare outreach. Crucially, the granular addressability which DHRUVA enables has the potential to extend the reach of governance to under-served areas, such as informal settlements or remote habitations ensuring that no community is excluded from receiving essential services or benefits due to address-related gaps. By making every location digitally discoverable and accurate, DHRUVA can create an opportunity to expand the effective footprint of welfare and service distribution, making governance equitable and accessible. The consent-based framework ensures that data use remains transparent and legally compliant, enhancing institutional accountability and public trust. Importantly, by making governance systems address-aware, DHRUVA lays the groundwork for simplified citizen onboarding for various government schemes. Its rollout may pave the way for potentially integrating it with existing DPIs, subject to legal and regulatory requirements, thus increasing its utility and multiplying the areas in which it can offer its advantages and services. It provides the groundwork for more scalable and innovative DPIs and technological solutions, ensuring that governance keeps pace with the complexity and scale of India's demographic and territorial diversity.

Use-Cases for Governance through DHRUVA:

- ***Last-Mile Welfare Distribution in Flood-Affected Areas:*** During floods, which can affect the discoverability of landmarks, local authorities can use DHRUVA to locate addresses and dispatch relief packages, ensuring coverage of even newly developed or unknown colonies.

- ***Utility Expansion Planning in Growing Suburbs:*** Urban local bodies or electricity boards can plan new power grid connections in peri-urban zones that are expanding rapidly but lack formal cadastral mapping.

- ***Audit Trail for Benefit Disbursal:*** The DHRUVA ecosystem provides consent-based details of where and when benefits were delivered, enabling post-facto auditing and accountability in governance. These measures can ensure the effective distribution of resources as well.

Illustration 3: Streamlining Pension-related Services by Eliminating Address Ambiguities

Services related to pensions for retired employees of the Central or state governments or other government organizations, which rely on addresses, are also affected due to the challenges of the prevailing addressing system. Doorstep generation of Digital Life Certificates (*Jeevan Pramaan)* and doorstep banking facilities to avail pensions become difficult as a result, especially in informal settlements or when pensioners relocate. DHRUVA can provide each beneficiary with a user-controlled Digital Address that will be anchored to a geocoded point, standardized in structure, and portable across systems. It may be able to support facilities such as the "Doorstep Service for Submission of Digital Life Certificate through Postman"[25] to reach pensioners for the purposes of generation of their Digital Life Certificates[26]. Similarly, pensioners who are able to avail the facilities of disbursing agencies offering 'Door Step Banking'[27] may also be able to share their Digital Address to receive such services. Subject to applicable legal and regulatory requirements, coupled with confidence scores, it may also support validation at the time of releasing benefits in the future. Moreover, when pensioners relocate seasonally, their address can be updated easily when requested by them, making it easier to avail doorstep services. This can improve efficiency in the workflow for authorities, thereby supporting efforts to mitigate both administrative and operational costs. Resources which previously may have been spent on handling failed deliveries or address disputes may be redirected towards improving service quality and onboarding new beneficiaries. This may reduce delivery failures and improve coverage accuracy with minimal changes to existing workflows.

Illustration 4: Enhancing Postal Operations through Standardized and Interoperable Addressing

Postal workflows at the Department of Posts are heavily dependent on the accuracy and legibility of address data across booking, sorting, and last-mile delivery. Currently, incomplete or non-standard addresses result in frequent manual interventions during data entry, misrouting of articles during automated sorting, and inefficiencies in delivery sequencing. Delivery staff often rely on personal knowledge of localities to make sense of vague or incorrectly written addresses, leading to inconsistent service quality and high dependency on legacy workforce experience. The integration of DHRUVA can introduce a standardized, interoperable and machine-readable Digital Address that will be geo-coded and structured in a uniform format across all operational systems. At the booking stage, DHRUVA can allow customers to input an address identifier (e.g., Digital Address) instead of filling in lengthy address fields, enabling faster and more accurate data capture. During sorting, the use of geocoded addresses can eliminate errors caused by duplicate or conflicting Pincodes and improves the accuracy of automated sorting machines by ensuring uniform surface readability and metadata integrity. At the delivery end, DHRUVA-backed addresses can be directly fed into GNSS-enabled mobile applications used by delivery persons, allowing for route optimization, workload balancing, and precise doorstep navigation. This can significantly reduce manual sorting time, enhance delivery predictability, and lower operational costs by cutting re-attempts and misdeliveries. Importantly, it can future-proof the Department of Posts' logistics chain by reducing reliance on manual address interpretation and making the entire system more scalable, efficient, and digitally aligned.

2.2.3. Benefits for the Private Sector

DHRUVA offers a transformative set of benefits to the private sector by addressing long-standing inefficiencies in location accuracy, service delivery, and customer onboarding. For businesses, especially in logistics, e-commerce, and utilities, the introduction of standardized, interoperable and geo-coded addresses through DIGIPIN and Digital Addresses can drastically reduce delivery errors and operational overhead, enabling more precise route optimization, better infrastructure planning, and ultimately greater profitability. In sectors such as banking, insurance, and telecom, the availability of accurate consent-based address data can simplify compliance-heavy processes like the facilitation of KYC, allowing for faster customer onboarding and reduced costs. By making the system interoperable and machine-readable, DHRUVA can also enhance strategic functions such as market segmentation, service planning, and targeted outreach giving new and smaller businesses the ability to make more informed, geography-driven decisions. Crucially, the architecture of DHRUVA is open and innovation-friendly, enabling the private sector to build value-added services and applications on top of the ecosystem, from geospatial intelligence platforms to dynamic service discovery tools. This spur of entrepreneurial activity will ensure that business growth aligns with user consent and privacy expectations. For local businesses and the tourism sector, it can facilitate easier location discovery and increased footfall by improving visibility and navigation, supporting inclusive economic growth in both urban and remote geographies. In summary, DHRUVA provides the private sector with a high-trust, high-precision infrastructure that enhances operational agility, customer satisfaction, and innovation capacity.

Use-Cases for Private Sector through DHRUVA:

- ***Efficient Last-Mile Delivery for E-Commerce:*** A logistics company servicing a Tier III town can use DHRUVA to eliminate delivery errors stemming from ambiguous or missing house numbers, increasing delivery success rates.

- ***Facilitating Digital KYC for Microfinance Lending***: Subject to applicable laws (including KYC requirements), a microfinance institution intending to verify the authenticity of the borrower's address, can verify the same using DHRUVA, reducing field verification costs and distributing loans to applicants in rural areas.

- ***Geo-Targeted Marketing for Local Retail Chains:*** A retail chain can leverage data from DHRUVA, to map high-footfall localities and target promotions for a new store launch with precision, avoiding wasteful ad spends in non-priority zones.

- ***Tourism App Route Optimization:*** A travel startup can integrate DHRUVA to help tourists discover hidden local attractions and plan optimized walking or driving routes in heritage towns with complex layouts.

- ***Address Verification for Workforce Management:*** An e-commerce platform can use DHRUVA to verify addresses and track their delivery partners based on accurate travel time predictions and reduce delays in service delivery.

Illustration 5: Address Validation in Logistics Without Manual Surveying

For logistics providers, particularly in last-mile delivery and field servicing, the lack of standardized and interoperable addresses results in frequent misdeliveries and high field correction costs. Many delivery agents rely on calling the customer or triangulating using local landmarks, which delays service and degrades customer experience. By adopting DHRUVA, logistics platforms can allow customers to register Digital Addresses that are geocoded and linked to a DIGIPIN. These may be embedded into the platform's address book and shared with delivery personnel through routing APIs. Since Digital Addresses follow a uniform structure and are tied to precise map coordinates, delivery planning systems can sort and optimize routes more effectively. This eliminates the need for post-order address verification or mid-route course corrections. As more deliveries are completed successfully at a given address, its confidence score within DHRUVA framework improves, allowing for predictive confidence. The result is lower average delivery time and improved service quality without increasing manpower.

Illustration 6: Improving KYC Address Verification for Financial Institutions

In the financial sector, address verification compliance remains a foundational requirement for onboarding individuals, and among the most persistent and operationally burdensome components of the KYC compliance. Traditional approaches ranging from the submission of physical documents such as utility bills or property documents, to doorstep verification are both resource-intensive and time-consuming. These legacy methods introduce delays, increase onboarding costs, and constrain the ability of financial institutions to scale, particularly to customers in remote or rural areas. DHRUVA can introduce a transformative possibility through which financial institutions can reimagine existing onboarding workflows and digitize it. By sharing a Digital Address linked to a DIGIPIN, financial institutions can receive address information that is highly precise. The methods of verification of the address information will depend on the risk profile of the customer and authorization under applicable laws. DHRUVA's services can be integrated into existing workflows such as the 'Digital KYC' under the Reserve Bank of India's *Master Direction- Know Your Customer (KYC) Direction, 2016*. The Digital KYC requires a live photo along with latitude and longitude of the location where such photo is being taken. Using the Digital Address for this process can simplify the fulfilment of this compliance requirement with great efficiency. In the long term, this digital-first, mechanism reduces the cost of compliance, curbs fraudulent submissions, and expands the reach of financial services by removing geographic and procedural barriers to inclusion.

3. Implementation of DHRUVA

Addressing practices have evolved over time in India in silos without a common institutional foundation, leading to challenges discussed in Section 1. DHRUVA seeks to address these systemic issues by introducing a comprehensive blueprint with a robust governance mechanism, legal foundation, and operational framework that can support the implementation of its technical architecture. This emphasis on implementation is foundational to DPIs. India's experience with DPIs such as Aadhaar, UPI, and ONDC, demonstrates that success at scale requires more than a technical layer - it requires dedicated institutions, enforceable standards, and a legal framework that enables trust, efficiency, and success. These DPIs have shown that when implementation is embedded in the design from the outset, the resulting infrastructure becomes durable, inclusive, responsive and responsible. DHRUVA draws from these lessons, by treating governance as an integral component of its architecture and not as an afterthought.

This section sets out the structural design that enables this outcome. It outlines the institutional framework that allocates responsibility and oversight, the technical architecture for the implementation of DHRUVA, the legal framework that confers authority and ensures compliance with applicable laws, and the standards that govern the use, scaling, and sustainability of the ecosystem.

3.1. Institutional Framework

Across DPIs, institutional frameworks have come to be recognized as one of the key enablers of scale, resilience, and public value. They have helped in the creation of a stable locus for governance, and a neutral mechanism for integrating stakeholders. They are designed not only to uphold technical standards, but to protect user interests and rights, ensure legal compliance, and create mechanisms for accountability.

Designing an institutional framework depends on a range of contextual factors. These include the nature of data being transacted, the degree of legal oversight required, the institutional complexity of the ecosystem, and a balance of public and private participation. The choice of institutional participants, both public-facing, and inward-facing entities of a DPI, must be guided by these considerations, ensuring that the governance structure that is subsequently developed for them reflects the operational and legal needs of the ecosystem it serves.

This section describes the roles and responsibilities of the key actors involved in its implementation. These institutions enable DHRUVA to function not just as a technological tool, but as a live and responsive system, capable of supporting innovation, adapting to changes, ensuring reliability, and protecting end users across sectors. Beyond these institutional actors, end-users are at the centre of the DHRUVA ecosystem, exercising control over how their address data is used and shared.

3.1.1. Address Information Providers ('AIP')

AIPs are entities that are responsible for generating and managing the Digital Address. Subject to the consent of the user, AIPs through Address Information Agents (described below) obtain the descriptive addressing information from the users, provide the interface to generate a DIGIPIN, and allow the users to generate a Digital Address that is linked to the DIGIPIN and to the descriptive address.

Given the significant role of AIPs in the DHRUVA ecosystem, only such entities that have been authorized under law may function as AIPs. To be authorized as an AIP, the entity will be required to satisfy certain governance and technical eligibility criteria set out in the law. In developing such eligibility criteria, due consideration will be given to the entity's proven expertise of securely handling user data, address-related infrastructure or logistics, satisfaction of capital requirements and technological infrastructure to act as an issuer of Digital Addresses. AIPs may include a diverse range of institutions from the public and private sector with whom users have shared their address data. Such entities could include public service providers, India Post, utilities or financial institutions. These entities, which already have vast experience in address information management, may be envisaged as potential AIPs, by tapping into their domain expertise and existing infrastructure. The ecosystem allows users to harness existing address data, enhancing convenience, eliminating duplication of efforts, and leverage existing information and infrastructure. AIPs will be required to adhere to both technical and governance standards to ensure user protection, system integrity and compliance with applicable laws.

3.1.2. Address Information Users ('AIU')

AIUs are authorized entities that can access the address information linked to Digital Address from the AIP through DHRUVA, to deliver services and enable information exchange. AIUs represent the demand side of the Digital Address ecosystem and play a critical role in translating address data into functional outcomes across sectors. Any entity seeking to consume address information through DHRUVA must be authorized to act as an AIU under the applicable law. In determining the eligibility criteria for AIUs, due consideration will be given to the valid and lawful purpose recognized under applicable laws, for utilizing Digital Addresses, capacity to handle data securely, technical capacity to receive and process address information. AIUs may include a wide spectrum of actors, private and public entities that provide services in logistics, e-commerce, banking, insurance, welfare distribution and more. Their operations have to be governed by strict adherence to user consent protocols, data protection standards, and purpose limitation principles as laid out by the Governance Entity (described below). As the ecosystem expands, AIUs will become increasingly central to the value creation enabled by it. Their ability to interact with address information in a lawful, transparent, and user-centric manner will be essential to the successful functioning of DHRUVA.

3.1.3. Address Information Agents (‘AIA’)

AIAs are entities acting as intermediaries between users, and AIPs and AIUs. These intermediaries provide simplified interfaces to users to interact with DHRUVA and enable them to manage their Digital Addresses. AIAs can provide a range of innovative services to users. AIAs will also provide consent management services to allow users to control the flow of their information through the ecosystem. AIA interfaces will have to be compliant with all applicable laws, DHRUVA’s technical and operational standards, and the design principles integral to it.

3.1.4. Governance Entity

In India’s DPI experience, institutions like the Unique Identification Authority of India (‘**UIDAI**’), National Payments Corporation of India (‘**NPCI**’), National Health Authority (‘**NHA**’) and Open Network for Digital Commerce (‘**ONDC**’) have demonstrated the importance of an anchor entity that can steward implementation, issue protocols, and sustain participation across diverse stakeholders. In a similar spirit, DHRUVA also envisages a dedicated governance entity (‘**Governance Entity**’) to ensure it transitions from a conceptual phase into a durable, nationally recognized layer of digital infrastructure. The Governance Entity will be foundational in bringing institutional alignment, preserving functional neutrality, and managing the evolving complexity of address data in both public and private sector contexts.

The operationalization of DHRUVA will require a robust Governance Entity that performs two distinct yet complementary roles: operational and standard setting. While the operational role focuses on active management and execution of ecosystem processes, the standard-setting role establishes the frameworks and protocols that guide these operations., This dual function is essential for maintaining ecosystem integrity, as operational effectiveness depends on clear standards, while standards must be informed by operational aspects of the ecosystem. The Governance Entity must perform these roles to ensure that: (a) it retains its primary characteristic as a DPI, (b) it complies with the laws applicable to it as a nodal agency responsible for the operation of the ecosystem, (c) it generates trust of the end-users and participants, and (d) it actualizes the foundational principles, such as security, interoperability, scalability, and compliance across the ecosystem.

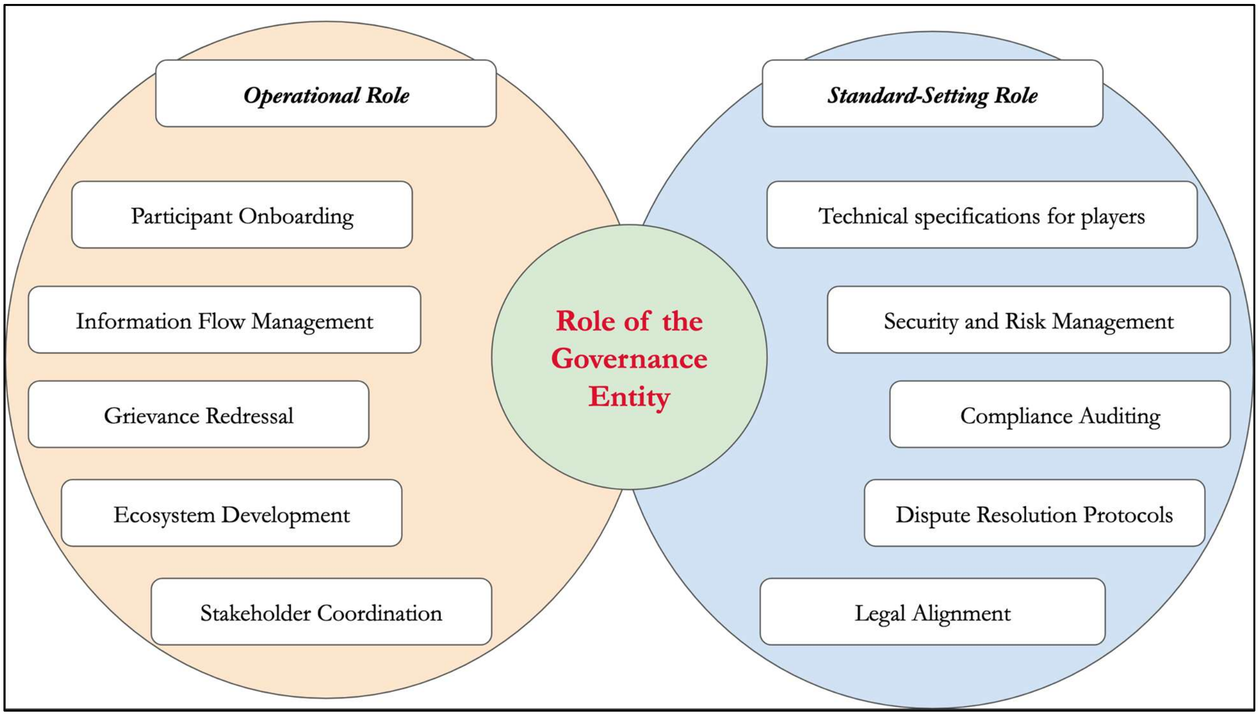

Fig 4: The different types of operational and standard-setting roles which the Governance Entity will play.

Image Description: Venn diagram illustrating the dual role of the Governance Entity. The left circle, labeled 'Operational Role', includes five functions: Participant Onboarding, Information Flow Management, Grievance Redressal, Ecosystem Development, and Stakeholder Coordination. The right circle, labeled 'Standard-Setting Role', includes five functions: Technical Specifications for Players, Security and Risk Management, Compliance Auditing, Dispute Resolution Protocols, and Legal Alignment. Both circles are connected at the center by a circle, which states 'Role of the Governance Entity'.

Any governance entity aimed at effectively regulating DHRUVA must satisfy a number of legal, institutional and administrative parameters. The first of these parameters is legal authority - the entity must be legally empowered to issue binding standards and decisions, so that its role is clear and enforceable across the ecosystem. As discussed subsequently in this document, the Post Office Act, 2023 ('**Post Office Act**') enables the Central Government to issue standards for the DIGIPIN and the Digital Address.

Equally important is operational autonomy - the ability to function independently without interference, allowing it to act decisively and impartially. Subject to the oversight of the Nodal Ministry, the structure of the Governance Entity must also account for how best to ensure that interests of different stakeholders are factored into decision-making, given the fact that DHRUVA involves multiple stakeholders. Adaptability and agility in decision-making are also key in an evolving legal and technological environment, enabling the entity to respond to emerging needs, and then scale in a timely manner, without being held up by protracted institutional processes.

The need for a Governance Entity for DHRUVA is unequivocal and settled. Without it, DHRUVA cannot deliver the legal certainty, operational coherence, or institutional continuity that any DPI requires. This entity will serve as the system's fulcrum anchoring participation, issuing standards, and resolving frictions as the ecosystem evolves. It is not simply a requirement of design, but a condition for its long-term resilience, public legitimacy, and capacity to scale.

3.1.5. Authorized Address Validation Agency ('AAVA')

Certain sectors such as banking, insurance, welfare, and real estate have specific legal and policy requirements regarding the accuracy of the address information which has been provided by the user. The DHRUVA framework recognizes these needs and is accordingly exploring the provision of a legally sustainable validation feature. This will be a user consent-based feature and is intended to be an additional manner for validating address information. DHRUVA does not seek to replace or override sector-specific verification requirements, which are shaped by distinct legal, risk-based, or service delivery considerations. Instead, it offers an optional mechanism that regulators and service providers may choose to rely on, either independently or in conjunction with other validation methods, depending on their context and needs. Subject to the consent of the end user and applicable laws, this functionality would allow authorized entities, called AAVA, to carry out limited, physical confirmation of whether the information associated with a Digital Address corresponds to an actual locatable place. This process will be undertaken without assessing the identity of the addressee or legal status of an address or location.

AAVAs form a critical part of the ecosystem by providing independent, certified address validation services. Their inclusion in DHRUVA enables scalability without compromising on privacy, extending the reach and reliability of validated Digital Addresses, while preserving user autonomy and system transparency. Only authorized government entities with experience in securely handling user data with robust technical and data governance protocols in place authorized under applicable laws can operate as AAVAs. Their onboarding process will involve a thorough assessment of their capacity and compliance with protocols established. To maintain ecosystem integrity, AAVAs will be subject to certain standards, periodic audits, quality assurance checks, and disciplinary protocols in case of non-compliance. A Code of Conduct is also envisioned for AAVAs to govern their functions, and to ensure that they do not collect any personal information at the time of carrying out their functions.

3.2. Process Flow

Central to the vision of the DHRUVA ecosystem is a robust technical architecture that will underpin the entire ecosystem, ensuring that address data can be shared and managed with accuracy and in a standardized format.. This section introduces DHRUVA's multi-layered technological ecosystem. It provides technical insights into the DIGIPIN and Digital Address Layer and provides a high-level understanding of how users and other key players in the ecosystem interact with each other to deliver its services.

3.2.1. The DIGIPIN Layer

The DIGIPIN's structure allows for the encoding of the latitude and longitude coordinates of a location into a sequence of an alphanumeric string using sixteen symbols (2, 3, 4, 5, 6, 7, 8, 9, C, J, K, L, M, P, F, T). A bounding box, which covers the territory of the entire country is split into 16 (4x4) regions. Each region is labelled by one of the symbols mentioned above, forming level 1 of the partition. Each region within level 1 is further subdivided into 16 subregions and allocated symbols, forming layer 2. This exercise is continued until each area of approximately 4m x 4m has been assigned the ten-digit alphanumeric string, that is, DIGIPIN. The symbols are assigned in an anticlockwise fashion, spiralling outwards.

The format of the DIGIPIN is intuitive, with a sense of directionality infused in its format. It is independent of land-use patterns and the structure built on top of the land. Therefore, it does not change with changes in the names of the state, city, or locality, or with changes in the road network in an area. The length of the DIGIPIN is designed to be as small as possible to provide an efficient digital representation of addresses. The Department of Posts has released the DIGIPIN logic in public domain, and its source code is available under an open license.[28]

3.2.2. The Digital Address Layer

As mentioned in Section 2.1, Digital Addresses are human-friendly labels that encapsulate address information. A Digital Address resembles an email or UPI address (e.g., name@suffix) and typically includes two key components: a DIGIPIN, which encodes geospatial data, and a descriptive address for added context. Each Digital Address may also include verification details, providing insight into the relevance and accuracy of the encoded address information. There can be different methods for address validation to ensure flexibility. Such mechanisms may include fetching address attributes from verified public address databases, for automatic validation. The users may also be allowed to provide self-declared addresses, which may be tagged with their confidence scores. For cases that may require higher assurance, physical verification will be conducted by empaneled agencies, ensuring on-ground validation and compliance with regulatory or sector-specific requirements.

3.2.3. DHRUVA’s Federated Architecture

DHRUVA’s technological architecture proposes to establish a federated DPI, defined in terms of building blocks. A federated architecture is an architectural approach that allows interoperability and information sharing between autonomous de-centrally organized entities, information technology systems and applications. A federated approach for DHRUVA is needed for enhancing the security and privacy of the information of users, while ensuring interoperability, an open-source approach, and technological agnosticism. This will also enable the streamlining of information flows across stakeholders in the ecosystem while keeping users, their privacy, and their confidentiality at the core of the ecosystem.

The features of the federated architecture adopted manifests in the following ways:

- Decentralized Data Storage: All user address data shall be maintained by AIPs in a decentralized manner.

- Citizen-centric Data Control: Citizens shall have full control over the processing of their address data, including how and by whom it is accessed or used.

- 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.

3.2.4. Key Players and Components of DHRUVA

AIPs: AIPs maintain the digital address registry, which includes core address data and any associated validation details. They also track which AIA supports each Digital Address. By keeping the registry current and secure, AIPs guarantee that only authorized parties can access accurate and up-to-date address information.

AIUs: AIUs directly interact with users, offering services - such as deliveries, location-based support, or logistics that rely on Digital Addresses. AIUs access address details through the Central Mapper and AIPs, always ensuring they obtain and honour appropriate user consent.

AIAs: AIAs oversee user consent processes and offer a clear, intuitive interface that allows citizens 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.

Central Mapper ('**CM**'): The CM operated by the Governance Entity is responsible for managing suffixes used by AIPs, maintaining a comprehensive registry of all DHRUVA stakeholders (excluding the end users), 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.

3.2.5. Issuance and Use of Digital Address

A simplified process flow for issuance and use of the Digital Address is enumerated below:

1. **AIP Suffix Assignment:** The Central Mapper allocates namespace suffixes to each AIP, creating an authoritative map of who is responsible for every Digital Address domain.

2. **Digital-Address Management by the User**: The user signs in to the AIA to create, update, or deactivate their Digital Addresses, remaining in full control of every operation on their own identifiers.

3. **Digital-Address Registration:** Acting on the user's request, the AIA registers the chosen Digital Address with the appropriate AIP, reserving the name@suffix pair inside that provider's registry.

4. **Address-Information Assignment:** The AIA submits the geospatial DIGIPIN (and any descriptive address) to the same AIP, binding real-world location data to the newly registered Digital Address.

5. **User Request for an AIU Service:** The user presents a Digital Address to an AIU, for example, an e-commerce or postal service - when initiating a transaction that requires physical fulfilment.

6. **AIU Initiates Digital-Address Resolution**: Before accessing the address details, the AIU contacts the AIA to obtain proof of the user's permission to resolve the given Digital Address.

7. **Consent Management**: The AIA authenticates the user, captures (or validates) consent for the specific AIU and purpose, and issues a time-bound token that represents that approval.

8. **AIP resolves the Digital-Address for the AIU**: Armed with the consent token, the AIU queries the relevant AIP. The AIP validates the token, retrieves the stored address information, and returns it, enabling the AIU to complete its service for the user.

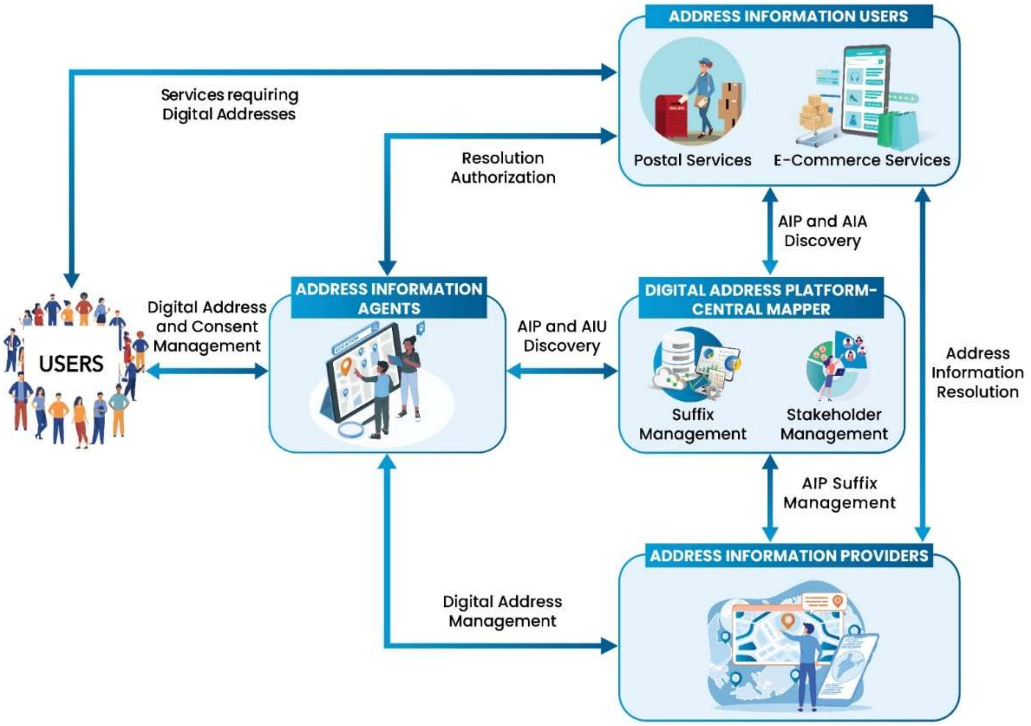
ADDRESS INFORMATION USERS
Postal Services
E-Commerce Services
Services requiring Digital Addresses
Resolution Authorization
AIP and AIA Discovery
USERS
Digital Address and Consent Management
ADDRESS INFORMATION AGENTS
AIP and AIU Discovery
DIGITAL ADDRESS PLATFORM-CENTRAL MAPPER
Suffix Management
Stakeholder Management
Address Information Resolution
AIP Suffix Management
ADDRESS INFORMATION PROVIDERS
Digital Address Management

Fig 5: Core Interactions of Key Players in the DHRUVA Ecosystem

Image Description: A diagram illustrating how different ecosystem players identified in Section 3.2.4 interact with each other.

3.3. Legal Framework

The implementation of DHRUVA requires a legal foundation that is both enabling and protective of the user. This framework not only empowers its institutional design but also ensures that the rights of users and the responsibilities of ecosystem actors are clearly defined and enforceable. Perhaps most importantly, it delivers legitimacy to DHRUVA and its operations, which can develop trust among users and provide certainty to the market participants. To this end, DHRUVA is being designed as an ecosystem that functions in alignment with the Post Office Act, the DPDPA and other applicable laws.

3.3.1. Legal Recognition of DIGIPIN and Digital Address

The Post Office Act is the primary legislation governing all matters connected with the Post Office (defined as the Department of Posts) and all related matters. Section 5 of the Post Office Act already empowers the Central Government to prescribe standards for 'addressing on the items, address identifiers and usage of postcodes'. While the Post Office Act does not expressly define the terms, the DIGIPIN and Digital Address are intended to serve as a form of postcode and address identifier respectively.

The DIGIPIN layer allows for the conversion of latitude and longitude coordinates into a combination of letters and numbers, or digital code. Section 5 of the Post Office Act empowers the Central Government to prescribe standards for addressing on items, address identifiers, and usage of postcodes. For the purpose of this section, "post code" has been defined in the Post Office Act as "*a series of digits, letters or digital code or a combination of digits, letters or digital code used to identify a geographic area or location*". Therefore, a postcode can be an alphanumeric code used to identify a geographic area or location, which aligns with the nature and purpose of the DIGIPIN. While the term "address identifiers" is undefined, Digital Address - a user-defined label representing the DIGIPIN or descriptive address – can reasonably be argued to serve as an address identifier. In order to fully articulate this intention, and to fulfil the legitimacy requirements for the successful implementation of this DPI, the definition of an "address identifier" in the Post Office Act must clearly include a 'Digital Address'. This would unambiguously enable the Central Government to prescribe standards for the DIGIPIN and Digital Address.

DHRUVA derives its key functionality by enabling the use of address identifiers and postcodes. Through the DPI ecosystem, it deploys key players- a Governance Entity, AIPs, AIUs, AIAs, AAVAs, and a complex but accessible technical architecture, to create an ecosystem though which users can engage and avail their services. Anchoring this ecosystem in legal legitimacy is essential not only to inspire trust among users and institutions, but also to ensure that its foundational features - user-centricity, consent-based data flows, interoperability, and accountability are implemented through stable instruments, which are sustainable and enforceable. Legal grounding enables DPIs to move beyond merely providing a technical solution to provide an institutional framework which can help continued realization of its foundational principles and objectives.

Interventions for legal grounding of DHRUVA would include provisions for recognizing and establishing a Governance Entity that is authorized to issue and enforce standards for proper functioning of the DHRUVA ecosystem. Clear provisions may be incorporated to delineate the structure, roles and responsibilities of the Governance Entity, including managing grievances, and overseeing ecosystem operations. The recognition of AIPs, AIUs, AIAs and AAVAs also needs to be provided, with clear eligibility criteria on what entities can assume such roles. The provisions must also specify the broad principles that need to be ensured and upheld in the ecosystem by its players, including prevention of unauthorized use of personal data, informed consent-based data flow, and ensuring that government services are not denied on the grounds of non-creation or non-use of Digital Address by end users, and compliance with applicable laws. In addition, the legal provisions may also have to account for consequences in case of unauthorized access, submission of false information and use and misuse of Digital Address or personal data by participants in the ecosystem.

3.3.2. Compliance with the Digital Personal Data Protection Act, 2023

While DHRUVA is fundamentally an address infrastructure, in certain instances, the sharing or processing of address information may involve personal data. In such cases, the obligations under the DPDPA become fully applicable. Accordingly, it is being designed as a consent-driven ecosystem, where all data flows, whether initiated by AIPs, requested by AIUs, or mediated through user interfaces are premised on meaningful, informed, and revocable user consent. The ecosystem's operational standards will embed DPDPA aligned principles such as purpose limitation, data minimization, and storage limitation into the operational protocols for all ecosystem participants, who will have to be DPDPA compliant in the relevant instances. This ensures that every actor interacting with personal data within the ecosystem does so with a clear, lawful basis and with full respect for the autonomy and rights of the individual.

Additional safeguards including audit trails for all data access events, certification of ecosystem participants, and compliance monitoring will also be developed by the Governance Entity. The ecosystem will be developed to support the rights granted to users under the DPDPA such as the right to access, correct, and erase their data and enforces purpose limitation at a systemic level. Further, the audit trails shall be maintained by both AIPs and AIUs.

By embedding these principles into both its legal and technical design, the ecosystem ensures that it complies not only with the letter of the DPDPA, but also with its spirit, thereby, creating a system that is user-centric, privacy-preserving, and legally sound.

3.3.3. Operational Aspects

Beyond the technical, institutional and legal framework governing DHRUVA, it is also important to consider the operational and functional aspects through a more micro perspective. Legally backed standards will guide the day-to-day functioning of DHRUVA and responses of different institutions in specific scenarios, in keeping with the institutional and legal framework of the DPI. Their purpose is to embed reliability, accountability, and user-centricity into every layer of the ecosystem's functioning.

This section provides an indicative list of standards, compliances, and protocols which will have to be developed for the DHRUVA ecosystem.

Technical and Operational Standards

The technical standards are aimed at creating the architectural rules and shared protocols that ensure the ecosystem functions with reliability, security, and interoperability. These standards define how participants of the ecosystem interact, and how data flows securely, thereby translating legal and policy commitments into executable code. These technical norms are essential to enabling innovation without compromising on integrity. By laying down a common foundation for all participants, the technical standards embed trust, legal compliance, and scalability into the day-to-day operation of DHRUVA.

Type I: Technical Standards & Specifications

- **DIGIPIN Standards**: Guidelines for generation, decoding, and geospatial mapping
- **Digital Address Standards**: Naming conventions, user-defined labels
- **Interoperability Framework**: APIs, data exchange protocols, encryption requirements
- **Device and Interface Certification Standards**: Guidelines to ensure that the ecosystem's access points are safe, accessible, inclusive and user-friendly

Type II: Standards for Information Flow, Privacy & Consent

- **Information Flow**: Secure, auditable data exchange with permissible use specifications
- **Consent Management**: Guidelines for collection, revocation, renewal, and modification of consent
- **Privacy Protection**: Data minimization, purpose limitation, transparency standards

Type III: Standards for Security & Risk Management

- **Cybersecurity**: Encryption standards, credential management, authentication mechanisms
- **Fraud Detection**: Monitoring, reporting, analytics, and breach notification procedures
- **Disaster Recovery**: Infrastructure requirements, redundancy, backup systems

Type IV: Standards for Participant Onboarding & Compliance

- **Eligibility Criteria**: Technical standards for AIPs, AIUs, and other participants, including guidelines on user information to be collected at the time of registration
- **Compliance Auditing**: Assessment timelines, reporting frameworks, corrective actions

Type V: Standards for Dispute Resolution

- **Resolution Guidelines**: Issue identification, resolution timelines, clear escalation mechanisms
- **Grievance Redressal** : Complaint handling, tracking, time-bound resolutions

Type VI: Standards for Scalability & Innovation

- **Scalability Standards**: Infrastructure, performance, transaction handling capacity
- **Innovation Standards**: Conditions for new services, pilot testing, sandbox environments

Type VII: Protocols for Transparency & Communication

- **Accountability Frameworks**: Reporting standards, disclosure norms, ecosystem metrics
- **Communication Protocols**: Updates, operational alerts, system changes

Type VIII: Inclusivity Standards

- **Equitable Access**: Low-connectivity solutions, multilingual support, accessibility features

---

Endnotes

[1] International Organization for Standardization, 'ISO 19160-1:2015: Addressing- Part 1: Conceptual Model, (ISO 2015) https://www.iso.org/obp/ui/#iso:std:iso:19160:-1:ed-1:v1:en accessed 9 April 2025.

[2] Universal Postal Union, *Addressing the World- An Address for Everyone (1st ed. UPU 2012),* Universal Postal Union, https://www.upu.int/UPU/media/upu/publications/whitePaperAddressingTheWorldEn.pdf accessed 9 April 2025, 7–11, 25, 27, 71.

[3] Government of India, 'National Geospatial Policy' (2022) https://dst.gov.in/sites/default/files/National%20Geospatial%20Policy.pdf accessed 10 April 2025.

[4] https://www.hindustantimes.com/ht-school/it-s-how-india-s-pin-codes-work/story-1yTxGBZFZ64QqlSwZ0ZORL.html

[5] K Rustogi et al, 'What is the Right Addressing System for India' https://arxiv.org/pdf/1801.06540 accessed 27 March 2025.

[6] White House Initiative, 'National Address Database' https://www.transportation.gov/sites/dot.gov/files/docs/NAD%20presentation%20(general%20overview)_1.pdf accessed 24 April 2025.

[7] 'Geoscape Geocoded National Address File (G-NAF)' https://data.gov.au/data/dataset/geocoded-national-address-file-g-naf#:~:text=Geoscape%20G%2DNAF%20is%20the,15.4%20million%20G%2DNAF%20addresses accessed 24 April 2025.

[8] 'GhanaPost GPS' https://ghanapostgps.com/ accessed 2 December 2024.

[9] 'The power of the UPRN' https://www.geoplace.co.uk/addresses-streets/location-data/the-uprn accessed 24 April 2025.

[10] 'Address Data' https://geoportaal.maaamet.ee/eng/spatial-data/address-data-p313.html accessed 24 April 2025.

[11] 'Getting to Know the NAD' https://storymaps.arcgis.com/stories/9490f773f65d4c6aa8b79facc528a661 accessed 24 April 2025.

[12] Department for Business Innovation and Skills, 'An Open National Address Gazetteer' https://assets.publishing.service.gov.uk/media/5a7cb22140f0b6629523b3c7/bis-14-513-open-national-address-gazetteer.pdf accessed 24 April 2025.

[13] 'Benefits of GhanaPost GPS' https://www.ghanapostgps.com/benefits/ accessed 24 April 2025.

[14] 'Geoplace: FAQs' https://www.geoplace.co.uk/addresses-streets/data-in-use/faqs accessed 24 April 2025.

[15] S Coetzee, 'Establishing a Virtual National Address Database' https://www.up.ac.za/media/shared/Legacy/sitefiles/file/44/2163/8121/innovate2/inn2bl22.pdf accessed 24 April 2025.

[16] White House Initiative, 'National Address Database' https://www.transportation.gov/mission/open/gis/national-address-database/national-address-database-nad-disclaimer accessed 24 April 2025.

[17] 'The power of the UPRN' https://www.geoplace.co.uk/addresses-streets/location-data/the-uprn accessed 24 April 2025.

[18] 'G-NAF: End User License Agreement' https://data.gov.au/data/dataset/19432f89-dc3a-4ef3-b943-5326ef1dbecc/resource/09f74802-08b1-4214-a6ea-3591b2753d30/download/20160226-eula-open-g-naf.pdf accessed 24 April 2025.

[19] Department of Economic Affairs, Government of India, 'Report of India's G20 Task Force on Digital Public Infrastructure' (July 2024) https://dea.gov.in/sites/default/files/Report%20of%20Indias%20G20%20Task%20Force%20On%20Digital%20Public%20Infrastructure.pdf accessed 7 March 2025.

[20] 'Digital Public Infrastructure should be a bridge, not a barrier: PM Modi at Summit of Future', (DD News, 23 September 2024) https://ddnews.gov.in/en/digital-public-infrastructure-should-be-a-bridge-not-a-barrier-pm-modi-at-summit-of-future/ accessed 10 April 2025. 'English Translation of the Prime Minister's Opening Remarks at the Inaugural Leaders' Session on the 3rd Voice of Global South Summit' (PIB, 17 August 2024) https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2046224 accessed 11 April, 2025.

[21] Department of Economic Affairs, Government of India, 'Report of India's G20 Taskforce on Digital Public Infrastructure' (July 2024), 8. https://dea.gov.in/sites/default/files/Report%20of%20Indias%20G20%20Task%20Force%20On%20Digital%20Public%20Infrastructure.pdf accessed 20 March 2025.

[22] Department of Economic Affairs, Government of India, 'Report of India's G20 Task Force on Digital Public Infrastructure' (July 2024) https://dea.gov.in/sites/default/files/Report%20of%20Indias%20G20%20Task%20Force%20On%20Digital%20Public%20Infrastructure.pdf accessed 7 March 2025.

[23] United Nations Development Programme, 'The SDGs in Action' https://www.undp.org/sustainable-development-goals accessed 7 May 2025

[24] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1; *K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1

[25] 'Doorstep Service for submission of Digital Life Certificate through Postman launched' (PIB Delhi, 12 November, 2020) https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1672278 accessed May 14 2025

[26] 'Welcome to Jeevan Pramaan. Digital Life Certificate for Pensioners' https://jeevanpramaan.gov.in/ accessed May 14, 2025

[27] India Post Payments Bank, 'Digital Life Certificate for Pensioner' https://www.ippbonline.com/web/ippb/digital-life-certificate1 accessed May 14, 2025

[28] https://github.com/CEPT-VZG/digipin