CASE STUDY

A Case Study on:

Digi Locker: CITIZEN'S VAULT OF TRUST ON PUBLIC CLOUD OF INDIA

By: Capacity Building Division, NeGD

Introduction

The National e-Governance Division (NeGD), under the Ministry of Electronics & Information Technology (MeitY), is at the forefront of driving the Digital India vision. A critical pillar of this mission is Capacity Building (CB), aimed at equipping government officials and stakeholders with the knowledge and skills required to implement and sustain transformative digital initiatives.

This case study on "DigiLocker—India's Vault of Trust in the Public Cloud" is part of NeGD's ongoing effort to document, analyse, and disseminate pioneering practices in digital governance and citizen-centric service delivery. It presents a comprehensive account of DigiLocker's journey—from its conceptualisation in 2014 to its emergence as a mission-critical layer of India's Digital Public Infrastructure (DPI) by 2025.

Drawing upon extensive field-level insights, stakeholder narratives, and official documentation, the study traces DigiLocker's evolution, its strategic design choices, and its impact across sectors such as education, finance, health, and defence. It also examines the platform's legal foundations, privacy architecture, and operational challenges—including technical heterogeneity, institutional scepticism, and rural underutilisation.

By capturing both the milestones and dilemmas of DigiLocker's implementation, this case study aims to serve as a valuable knowledge asset for policymakers, technologists, administrators, and capacity-building practitioners. It offers practical lessons on building scalable, secure, and inclusive digital platforms, and contributes to the broader goal of fostering sustainable and trusted digital transformation under the Digital India umbrella.

Acknowledgment

The Capacity Building Division, NeGD, extends its deepest gratitude to Professor Charru Malhotra from the Indian Institute of Public Administration (IIPA) for her guidance and support in shaping this case study on DigiLocker—India's Vault of Trust in the Public Cloud.

We are immensely thankful to the visionary leaders and the dedicated team at NeGD who conceptualised and built DigiLocker. Special thanks are due to Dr. R.S. Sharma, former Secretary, DeitY; Mr. Debabrata Nayak, Chief Technology Officer, NeGD; Mr. Amit Jain, former Technical Lead, DigiLocker; and Ms. Srishti, Project Manager, NeGD, for generously sharing their time, experiences, and invaluable insights that form the core of this narrative.

We also acknowledge the contributions of the numerous Ministries, Departments, and Organizations (MDOs) at the Central and State levels—particularly CBSE, MoE, RBI, SEBI, NIC, and the Indian Armed Forces—whose trust and collaboration were pivotal in integrating their services and records with the DigiLocker platform.

Furthermore, we thank the internal teams at NeGD for their diligent coordination, review, and support throughout the development of this case study.

Disclaimer

This case study has been developed by the National e-Governance Division (NeGD) under its Capacity Building mandate for the purpose of knowledge sharing and academic reference. The information presented herein has been compiled from official government sources, project documents, and interviews with relevant stakeholders involved.

While every effort has been made to ensure the accuracy and reliability of the information, this document is intended for educational and illustrative purposes only. It should not be interpreted as an official policy statement or a guideline for implementation. The views and conclusions expressed are those of the author and contributors based on their analysis and do not necessarily reflect the official position of the Ministry of Electronics & Information Technology (MeitY) or the National e-Governance Division (NeGD).

The commercial use of this material is strictly prohibited. This case study is meant to be used as a learning tool for government officials, trainees, and individuals interested in e-Governance and public policy.

Any reproduction or use of this material must include proper attribution to 'National e-Governance Division (NeGD).' All intellectual property rights remain with NeGD unless otherwise specified.

DigiLocker

CITIZEN'S VAULT OF TRUST ON PUBLIC CLOUD OF INDIA

In late 2014, amidst the rustle of files and the hum of the daily office routine of Electronics *Niketan*, a transformative idea emerged - Dr. R.S.Sharma, then Secretary, Department of Electronics and Information Technology (DeitY)[1]Government of India (GoI), posed a simple yet visionary question to his team: *"For decades, our citizens have been struggling with the safe storage and retrieval of physical copies of their vital documents issued by the government. What if every official document a citizen needs could be securely stored and accessed from a government-backed cloud?"* This deceptively simple yet profound question of Dr. Sharma became the catalyst for a digital revolution of paperless governance in India. Backed by the National e-Governance Division (NeGD), the erstwhile DeitY (now MeitY) team set out to build a secure, *Aadhaar*-linked digital repository for citizens' documents in a government-backed vault. The result was 'DigiLocker: *private space in the public cloud*', launched on July 1, 2015, under the Digital India Programme[2]. A new era of paperless, citizen-centric governance descended in India.

DigiLocker offers a secure, *Aadhaar*-linked public cloud service available to individuals for storing, accessing, and sharing their government-issued documents, marking the first time in India's governance history that such records, about various domains, including education, transport, finance, and health, can be accessed digitally, anytime and anywhere. The net outcome was: *"No queues. No photocopies. With DigiLocker- Just click, fetch, and go."*

And unlike commercial cloud services[3] DigiLocker also directly integrates with issuing authorities of these documents, while providing e-Sign functionality, and QR-based verification features too. This has gone a long way in simplifying public service delivery and reducing documentation-related fraud. If some government issued documents are not available in real time, the platform also allows citizens to scan and upload their documents[4]. With this dual capability of issuing and self-uploading records, DigiLocker serves as a complete and lifelong credential repository of individuals' documents in the public cloud. DigiLocker operates on a secure, government-managed public cloud infrastructure, aligned with India's digital governance standards and hosted on ISO 27001 certified data centers under the aegis of MeitY. Now, DigiLocker provides three foundational functions: (1) Digital issuance of official

---

[1] The erstwhile name of Ministry of Electronics and Information Technology (MeitY, Government of India)

[2] **Digital India Programme** is a flagship initiative of the Government of India aimed at transforming the country into a digitally empowered society and knowledge economy. It focuses on providing digital infrastructure as a core utility, delivering government services electronically, and promoting digital literacy and inclusion.

[3] **Commercial cloud services**, also known as generic cloud services, refer to cloud storage and computing platforms offered by private companies (e.g., Google Drive, Dropbox, or OneDrive) where users can store, manage, and access files over the internet.

[4] However, DigiLocker clearly states, "*these scanned and uploaded documents are NOT treated as authentic original documents*"

documents by over 2,000 verified government and institutional issuers (2) Secure cloud-based storage of both issued and user-uploaded documents (3) Real-time verification and sharing of documents with authorised verifiers through a trusted API-based ecosystem (Figure 1).

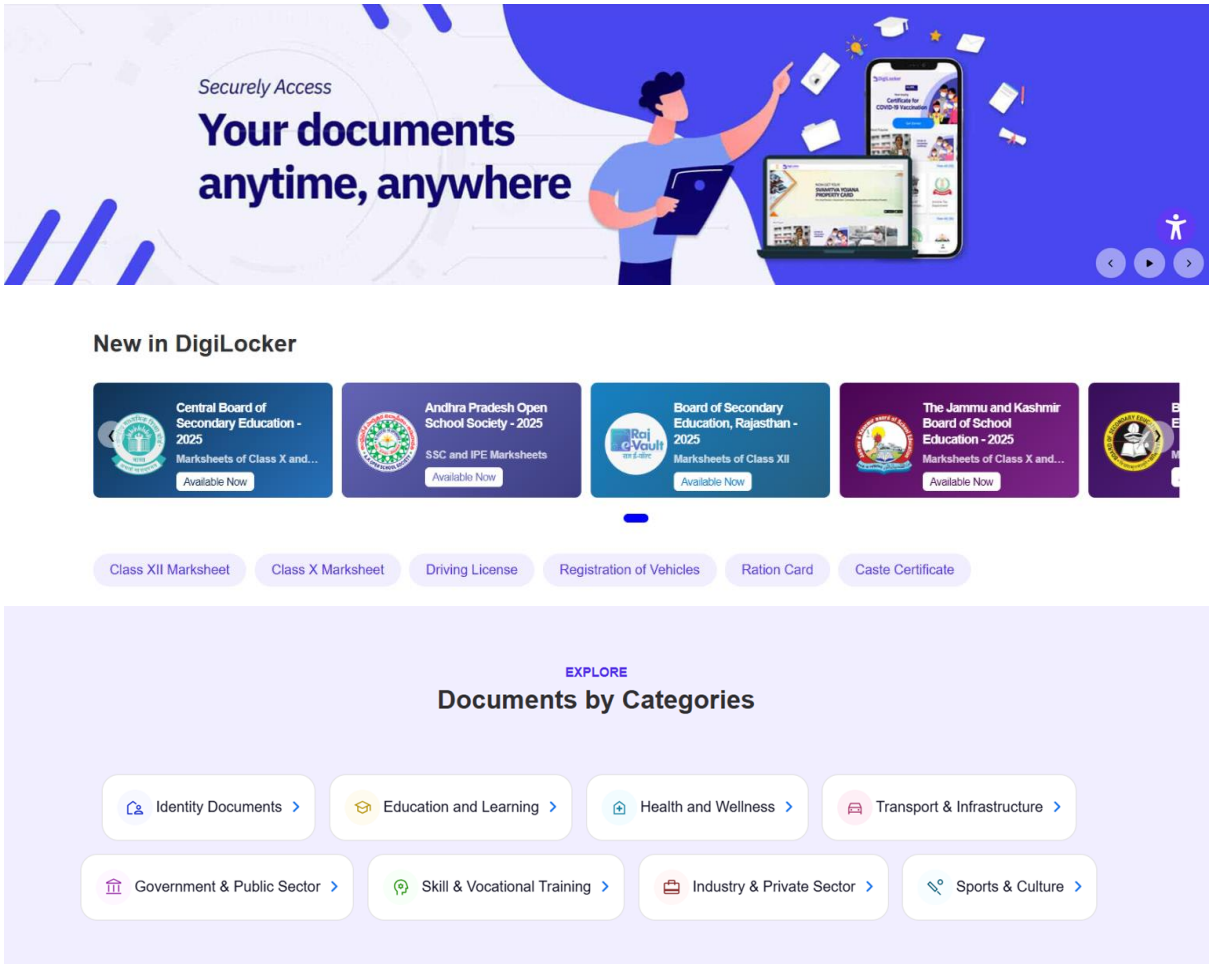

Figure 1 : DigiLocker HomeScreen
(Source: https://www.digilocker.gov.in/; Accessed on July1, 2025)

Recognising its transformative role, Finance Minister Smt. Nirmala Sitharaman had once, during her Union Budget speech in the *Lok Sabha* on February 1, 2023, described DigiLocker as "*a one-stop solution for reconciliation and updating of identity and address of individuals maintained by various government agencies, regulators and regulated entities.*" Beyond improving efficiency and transparency at the national level, DigiLocker advances global Sustainable Development Goals[5] (SDGs). By replacing physical documents with digital credentials, it directly supports SDG 12 (Responsible Consumption and Production) by cutting paper and resource use. Its interoperable architecture and innovation in digital infrastructure align with SDG 9 (Industry, Innovation, and Infrastructure), while its equitable access helps bridge social and regional gaps, contributing to SDG 10 (Reduced Inequalities). DigiLocker,

[5] **Sustainable Development Goals (SDGs)** are a set of 17 global goals adopted by all United Nations member states in 2015 as part of the 2030 Agenda. They aim to address global challenges such as poverty, climate change, peace, and justice, providing a shared blueprint for achieving sustainable and inclusive growth worldwide.

thus, exemplifies how inclusive, citizen-centric digital solutions can simultaneously enhance governance and promote sustainability.

Genesis and Evolution: Conceptualised under the leadership of Dr. R.S. Sharma at erstwhile DeitY (now MeitY) in 2014 and developed in 2015 by the three-member core team of NeGD, the DigiLocker platform (at times being referred to only as 'the platform') represented a bold step towards the vision of a paperless digital ecosystem...an initiative way ahead of its times. The technical design and development of DigiLocker was built on the learnings of a similar type of state initiative of the Government of Maharashtra, called MahaOnline[6]. The first version of DigiLocker was released in 2015 and hosted at the National Informatics Centre (NIC). At that time, it had offered two main features- 'user-upload functionality for scanning and adding personal documents' as well as 'secure digital storage of documents' and was designed to be both 'issuer' as well as 'verifier' of the data through extensive use of APIs[7].

At present, DigiLocker boasts of three main features: *Aadhaar*, e-KYC and e-Sign[8]. *Aadhaar* helps to verify user credentials, while e-KYC enables seamless and secure transmission of these verified details. However, the game changer is 'e-Sign' that aids remote digital authentication. As Mr. Debabrata Nayak[9], then Additional Director, NeGD, recalls, *"When we had implemented e-KYC and e-Sign in DigiLocker, we knew we had struck gold. Within its first year itself, DigiLocker had attracted over 10 lakh[10] users, with 20 lakh documents uploaded or issued".* With the rise of digital KYC (e-KYC) and paperless onboarding, fin-tech companies, banks, telecom providers, and Non-Banking Financial Companies (NBFCs) also began integrating DigiLocker APIs to verify documents submitted by users. The numbers kept spiralling, and as of August 2025, DigiLocker has issued over 990 crore[11] documents and served more than 57 crore registered users across India (*source: DigiLocker Statistics dashboard, August 2025*). Indeed, through its trusted digital architecture, document integrity mechanisms, and legal recognition, DigiLocker has emerged as a mission-critical layer of India's Digital Public Infrastructure[12] , also known as 'India Stack', powering secure, paperless, and verifiable service delivery across sectors (Figure 2).

---

[6] **MahaOnline** is a joint venture between the Government of Maharashtra and Tata Consultancy Services (TCS) aimed at delivering government services electronically to access various state services online, reducing the need for physical visits to government offices and promoting e-governance in the state.

[7] **API (Application Programming Interface)** is a set of protocols that allows different software to communicate with each other. It defines how requests should be made, what data to be sent, and what responses to expect.

[8] **e-Sign** was developed by NeGD, and Controller of Certifying Authorities (CCA) and replaced dongle-based digital signatures with *Aadhaar* enabled e-signing thus enabling secure digital transactions accessible to all.

[9] **Mr Nayak**, presently serving as 'Chief Technology Officer' CTO, NeGD, MeitY

[10] 10 Lakhs is 1 million

[11] 1 billion is 100 crore

[12] **Digital Public Infrastructure (DPI)** refers to the core digital systems and services that are built and maintained by the government or public institutions to enable secure, inclusive, and efficient access to digital services for everyone. DPI can be deemed as the digital equivalent of public roads and bridges—but instead of moving cars, it moves data, services, and trust.

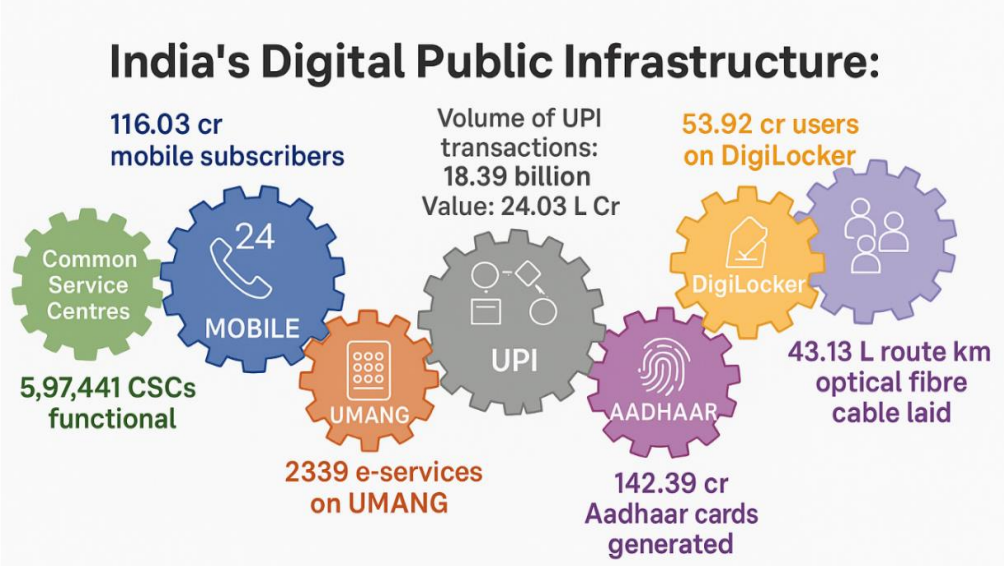

Figure 2: India's Digital Public Infrastructure - 2025
(Source- DPI data 2025, as per reliable government sources https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2123137)

Yet, underpinning this success were numerous challenges, which were systematically and diligently addressed by the DigiLocker team through strategic planning and technical expertise.

One of the earliest challenges during the design and development of the DigiLocker platform was about managing a geographically distributed team of developers who had been working in this manner since 2015. Unlike most government digital projects of that era, which typically relied on co-located teams and dedicated infrastructure, DigiLocker was developed by a geographically dispersed team across the country. This proved to be a daunting task. Coordinating for software design, coding, testing and stakeholder engagement remotely in a pre-pandemic era, when remote collaboration tools were still maturing, was a relatively unique proposition.

Subsequently, the platform also faced slow institutional buy-in and inter-departmental scepticism, where *"several officials often insisted on physical copies; others were hesitant to share data; some found no merit in adopting a centralised platform especially as there were no specific policy mandates to insist on the same."* narrates Mr. Amit Jain, another of the three team members of DigiLocker who had worked shoulder to shoulder with Mr. Nayak. He further added, *"MeitY and NeGD, were the custodians of DigiLocker, but had no formal authority to insist on any agency to integrate with the platform"*. On the technical side, as jointly recounted by Mr. Nayak and Mr. Jain, *"data and format inconsistencies became another significant issue"*. Various government entities were using varying file formats, such as PDFs, XML, text, or even HTML, to create and store their respective documents, which was creating technical difficulties in rendering and displaying documents uniformly across the DigiLocker platform. Each new integration led to a new cycle of customised code development, which in turn led to obvious technical inefficiencies. Last but not the least, with emerging global and national discourses on privacy and consent management, a newer set of challenges emerged.

On one hand, a large segment of citizens remained unaware of DigiLocker's existence and its wide-ranging benefits, limiting its adoption. On the other hand, a growing group of digitally literate users, increasingly conscious of their privacy rights, expressed scepticism about how their data was being accessed and used. *"What is very interesting to note is that DigiLocker had already proactively implemented a 'privacy-first architecture' that emphasised on 'mandatory users' consent', 'selective document disclosure' and 'time-bound access",* asserted Dr. Sharma. This design was later very well aligned with the 2017 K S PuttaSwamy judgement of the Supreme Court of India, when 'privacy' was declared as a 'fundamental right' of Indian citizens, and subsequently also with the Digital Personal Data Protection (DPDP) Act 2023 of India. Unfortunately, in those earlier times, some verifiers were not fully implementing these privacy features, like 'granular consent' and maintenance of 'audit logs'. Also, what remained to be seen was *"how much were citizens aware of these robust technology provisions already available in DigiLocker's implementation?*" remembered Mr. Nayak. Furthermore, while the DPDP Act 2023 provides a broad framework for personal data protection, it has notable gaps in areas relevant to DigiLocker's trust ecosystem. For instance, the Act imposes no strict data localization requirements (it merely allows the government to notify conditions for cross-border data transfers), relies on data fiduciaries' internal grievance redress mechanisms with an appeal to the Data Protection Board (instead of an independent regulatory authority), and mandates independent data audits only for designated "Significant Data Fiduciaries". These gaps mean that certain accountability aspects, ensuring all verifiers maintain proper consent records and audit logs, or swiftly addressing user grievances, still depend on robust implementation beyond what the law explicitly prescribes. Additionally, early users of DigiLocker reported practical issues such as OTP verification failures during *Aadhaar*-based sign-ups, and privacy advocates raised concerns about storing sensitive documents on a central platform. The DigiLocker team had to continually address such feedback through technical improvements and clear communication, reinforcing user trust even in the absence of explicit legal mandates.

To address these early challenges, the DigiLocker team employed a balanced strategy—ensuring legal provisions, espousing appropriate technological solutions, undertaking capacity building endeavours among key stakeholders and adopting some other 'out-of-box' solutions too. For instance, in the early years of 2014-15, when managing a distributed team was a significant challenge, DigiLocker leadership turned it into an opportunity by wholeheartedly adopting digital collaboration platforms such as *BharatVC* (a government video conferencing tool). This enabled real-time coordination despite geographical dispersion. This remote-first approach not only improved communication but also cut costs, allowing the team to work flexibly across locations and served as a saviour during the pandemic period. Similarly, to address institutional scepticism, it was established that DigiLocker would not store documents independently but would only fetch them directly from the issuing departments ('issuers'), thereby positioning these issuers as 'the single source of truth' (Figure 3)

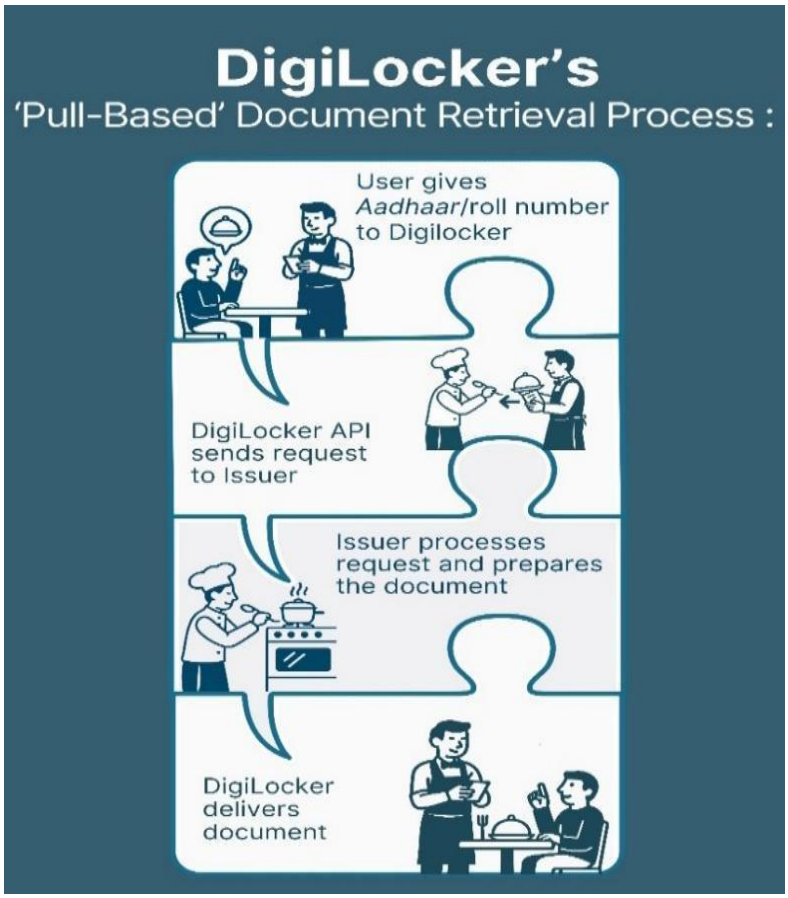

Figure 3: 'Pull-Based' Document Retrieval Process
(Source : IIPA)

As a result, some of the 'issuers' began to show 'interest' in DigiLocker. One of the initial success stories of a massive onboarding was that of the Central Board of Secondary Education (CBSE) in the year 2016, which led to a spate of other success stories too (Box-1).

Box -1
The Success of the Central Board of Secondary Education (CBSE) Spurred Several

"*For years, students carried the burden of lost certificates, delayed results, and endless queues. With DigiLocker, we gave them dignity, speed, and certainty. That's not just digital governance, it's justice*," reflected Dr. Sharma, the then Secretary, capturing the essence of a quiet revolution. The journey of storing academic records in DigiLocker has a precursor in the genesis of the National Academic Depository (NAD). The Ministry of Education (MoE) had conceptualised NAD in 2014 to securely store higher education academic records of the students for life. For this, they had partnered with National Securities Depository Limited (NSDL) and Central Depository Services Limited (CDSL). The DigiLocker team had also approached MoE, but they were not considered. Instead of being disheartened, they decided to focus on delivering school-level certificates through DigiLocker, and they relentlessly followed up with CBSE, India's largest school board. In the year 2016, CBSE became the first national-level school board to integrate its results with DigiLocker. This integration empowered CBSE students to access their digital mark sheets directly; in a week DigiLocker users spiked from 10

lakhs[13] to 35 lakhs. CBSE authorities and students were equally thrilled. They publicly endorsed DigiLocker's digital delivery approach that was API-driven, real-time and on-demand. The traditional scan-and-upload models would soon become obsolete. More and more academic institutes were attracted to these advantages. Very soon after that, DigiLocker also became an organic source of students' mark-sheet data from Indian Institutes of Technology (IITs) and National Institutes of Technology (NITs) for their Joint Entrance Examination (JEE)[14] admissions process. In the year 2019, DigiLocker was able to successfully issue more than 5 crore academic documents for multiple educational boards and institutions, that rose to more than 9 crore during 2020-21, and reached about 15.2 crore by 2025. Armed with these success stories, DigiLocker decided to approach MoE again, to be considered by them as the third partner for NAD, alongside CDSL and NSDL. To their utter surprise, in March 2020, MoE officially de-notified NSDL and CDSL and named 'DigiLocker the sole academic depository'. Emphasising this turn of events, Srishti, NeGD project manager recalled "*CBSE/MoE gave us the entire responsibility of NAD; our three years of sustained efforts had ripened well. DigiLocker now hosts over 72 crore* (*720 million*) *educational records issued by several education boards and universities of India*", she further shared.

However, as more issuers adopted DigiLocker, the challenge of technical heterogeneity among them became increasingly pronounced. This was resolved by adopting a format-agnostic architecture[15] in DigiLocker. Another feather in the cap was the integration of DigiLocker into the prevailing UMANG[16] app of the Government of India (GoI), which surely enhanced the platform's credibility and gave it the advantage of promotion and broader outreach too. DigiLocker pioneers also realised that it was equally imperative to garner legal acceptance of digital documents hosted in DigiLocker. After persistent efforts, in 2016, MeitY was able to propose Rule 9A of IT Act of India (Exhibit-1), which legally equated digital documents hosted in DigiLocker with their physical counterparts. *"This landmark amendment was because of our senior officers like Dr. Ajay Kumar (erstwhile Additional Secretary, MeitY) who were being supported by several senior legal experts, including Mr. Vakul Sharma- a senior cyber advocate"* shared Mr. Jain. Following the relevant legal backing for DigiLocker, several organisations, such as the Ministry of Road Transport and Highways (MoRTH), also issued their department notifications in September 2016, recognising digital driving licenses and registration certificates (RCs) hosted on DigiLocker as legally valid and instantly verifiable documents. However, these were still stray success stories. Despite all the visible advantages coupled with 'legal acceptance', DigiLocker still did not witness widespread adoption during its initial years, *viz.* 2016–17.

[13] 1 lakh is 0.1 million

[14] **JEE** is a crucial entrance test for engineering aspirants in India, conducted by the National Testing Agency (NTA) for admission to various undergraduate engineering programs.

[15] **Format-agnostic architecture** refers to a system design that can process data in various formats without requiring a specific structure or standard. For instance, standardised XML-based APIs and a sandbox environment were introduced to simplify integrations and testing, reducing technical hurdles for departments.

[16] **UMANG** is a single unified app to access major e-government services anytime, anywhere on your mobile phone.

This was mainly because some citizens, despite possessing valid DigiLocker documents, continued to face rejections from frontline personnel, such as traffic inspectors, across various states of the country. This disconnect stemmed from limited awareness among frontline personnel about the updated policy directives, coupled with inadequate familiarity with digital verification systems. Once this problem was noticed, NeGD immediately launched a spate of sensitisation workshops across various organisations, and initiated more than 40 training workshops for training 'on-ground staff' across the country. These training workshops aimed to educate traffic police, RTO officers, and other frontline staff on Quick Response (QR) code validation and digital authentication protocols. Subsequently, in 2023-2024, more than 20 sensitisation workshops were also initiated in several popular universities. Now it has become a recurring event.

The recent issuance of legal endorsements has significantly bolstered the institutional legitimacy and regulatory credibility of DigiLocker, reinforcing its role as a trusted digital public infrastructure!

Following amendments to the Prevention of Money Laundering Rules in 2019, the Reserve Bank of India (RBI) formally recognised DigiLocker-issued documents for Know Your Customer (KYC) compliance in early 2020. Subsequently, in April 2020, the Securities and Exchange Board of India (SEBI) also permitted the use of DigiLocker for submitting Officially Valid Documents (OVDs) during the onboarding of fund managers, stockbrokers, and other intermediaries—further cementing DigiLocker's role in digital identity verification across India's financial ecosystem. With all these combined efforts and legal backings, a positive shift from 'passive enablement of issuers' to 'active ground-level enforcement' became noticeable.

National Impact and Journey Onwards

The COVID-19 pandemic (2020) was a defining moment for DigiLocker. As public offices shut down and mobility was restricted across the globe, DigiLocker quietly empowered Indian citizens with remote access to their critical documents such as academic records, identity proofs, and especially vaccination certificates. Its role during the CoWIN vaccination drive was transformative. "*People didn't carry papers. They carried DigiLocker. That's when we truly arrived*!" beamed Dr. Sharma.

Beyond the pandemic, DigiLocker's impact has been comprehensive and sector-wide. "*For instance, in the education sector, over 421 million (as of 2025) digital records have simplified verifications and reduced fraud",* remarked Mr. Nayak. Similarly, in finance, real-time e-KYC under RBI guidelines has cut onboarding time from days to minutes. The transformation of DigiLocker into an essential digital utility has been both comprehensive and institutional. By mid-2021, user numbers surged from three crore to over nine crore, underscoring the platform's reliability and public trust. The adoption of DigiLocker documents by the Indian Army especially during the rollout of the *Agnipath* scheme in 2022, encouraged other uniformed forces to also adopt DigiLocker (Box-2).

Box – 2
DigiLocker to the Rescue of Indian Army's *Agnipath* Scheme

It was September 2022, *Agnipath** recruitment scheme was rolled out by the Indian Army (IA). The response of Indian youth to the scheme was overwhelming. The Army received nearly 50 lakh applications for mere 46,000 vacancies. However, this unprecedented scale posed serious challenges to them in verifying applicant identities, preventing duplication, and ensuring fairness in the selection process. To address this, they partnered with the DigiLocker team (2022-23) to implement a secure, *Aadhaar*-linked document verification system. The goal was to ensure that each candidate could apply only once, regardless of location or recruitment centre. Over several months, DigiLocker collaborated closely with the Army, working on-site to integrate with systems managed by NIC and also with the State Bank of India for collecting application fees. Once implemented, the system was able to authenticate over 30 lakh unique applicants, effectively eliminating duplicates and streamlining the scrutiny process. This not only reduced administrative burden but also enhanced the transparency, speed, and credibility of the *Agnipath* Scheme. This success story further catalysed the platform's expansion into other uniformed forces, *i.e.* the Indian Navy, Indian Air Force, and State Police Departments like Uttar Pradesh Police, who also began adopting DigiLocker for their respective processes. This marked a turning point in DigiLocker's journey and transformed it from a simple digital document store into a trusted backbone for identity verification in high-stakes public services.

***Agnipath* Scheme:** This is a new human resources management scheme for the Indian Armed Forces, approved by the Union Cabinet on June 14, 2022. The scheme aims to create a younger and more technologically adept armed forces profile. Individuals recruited under the *Agnipath* scheme are called *Agniveers*. They will serve in the Armed Forces for four years.

By 2023, even states such as Jammu & Kashmir and West Bengal[17] had embedded DigiLocker into their governance workflows, for storing, providing and verifying land records and Mahatama Gandhi National Rural Employment Guarantee Act (MNREGA) beneficiary details and so on.As of July 2025, DigiLocker has become an essential part of India's digital journey, making it easier for citizens to access vital services and documents online. Today, it supports a wide range of services, from storing school and college certificates, NAD records, and driving licenses, to vaccination certificates (CoWIN), birth certificates, DBT[18] eligibility checks, and more (Exhibit-2). Without loud marketing or fanfare, in a span of barely 5 to 6 years, DigiLocker has proven itself to be a secure, scalable, and citizen-centric pillar of India's DPI revolution.

In 2022, the Union Budget announced a 'DigiLocker-like' platform for institutions too. This led to the launch of 'EntityLocker' in August 2024 by NeGD, which has been particularly designed for businesses, educational institutions, non-profits, and government bodies. EntityLocker boasts features that institutions often require for smooth functioning, including

[17] It is pertinent to mention here that West Bengal state had simultaneously also launched a localised version called "iCloud DigiLocker," tailored to its own state's administrative needs.

[18] **DBT (Direct Benefit Transfer)** is a government initiative in India that directly transfers subsidies and benefits into the bank accounts of beneficiaries, reducing delays, leakages, and intermediaries.

'multi-role access', 'delegated permissions', 'bulk uploads', 'ERP[19] integration', and 'compliance/ audit trails'. These features are specifically tailored to optimise the workflows of onboarded organisations. Far from being a replica, it marked a strategic evolution of DigiLocker's architecture. Simultaneously, DigiLocker itself has inculcated several AI-driven features and enhanced dashboards, setting higher standards in citizen-centric digital governance.

Unlike many global platforms, such as Australia's myGov and Canada's MSCA[20] that focus on services or identity, DigiLocker offers a unique, citizen-controlled document vault. And it is built entirely on the public cloud, a feat that remains one of the most binary and globally distinctive initiatives and digital governance. As its next step of growth, India is trying to align itself with global leaders like Estonia's X-Road and Singapore's MyInfo to enable secure, cross-border interoperability.

Dilemma: A Digital Bridge Yet to Reach All

In India, DigiLocker is no longer just a convenience; it has become a trusted, scalable, and secure digital bridge between the citizens and the state. The goal is clear: to establish DigiLocker as a global trust standard for the entire Global South. However, one unresolved challenge looms extensive—its limited penetration and sustained usage in rural India. As an example, DigiLocker's utility for rural students is often limited to downloading board exam results. Once this immediate need is fulfilled, the app is seldom revisited by them. This is just one stray instance. Such underutilisation, particularly by citizens on the wrong side of the Digital Divide, prevents DigiLocker from realising its full potential as a 'Lifelong Credential Hub for All'. This gap underscores the need for sustained infrastructure investments and a structured public awareness strategy. Without active engagement, the platform risks widening digital divides instead of bridging them. To effectively address this, policymakers and researchers also require more granular usage analytics. For instance, distinguishing active versus dormant DigiLocker users, tracking the average number of documents per user, and examining adoption rates across states, regions (urban vs. rural), and demographics (gender, persons with disabilities, etc.) would help identify where the platform is underutilized. Likewise, key governance metrics — such as the average time for new issuers to integrate via API, the document rejection rates by verifiers, or the cost per transaction — could provide insight into operational efficiency and trustworthiness. Making these datasets available (and benchmarking DigiLocker's performance against international digital government indices and adoption curves) would greatly inform future improvements. There can be several innovative models to plug this gap. DigiLocker can now adopt a multi-lingual, multi-channel outreach model, leveraging community-driven engagements to drive adoption among rural users. Ultimately, the DigiLocker story need not end as a technological triumph but must start with

[19] **ERP- Enterprise Resource Planning:** An ERP system provides a centralised platform where data flows seamlessly across departments, improving efficiency, reducing duplication, and enabling better decision-making.

[20] **MSCA (My Service Canada Account)** is an online platform by the Government of Canada that allows citizens to securely access and manage services like employment insurance, pensions, and tax-related information

an unrelenting policy question- *"How can we ensure that the digital dividends of national platforms like DigiLocker reach those who need them the most?"*

***

Exhibit-1

Rule 9A of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016 is a landmark provision that legally equates digital documents stored in DigiLocker with their physical counterparts.

Key Highlights of Rule 9A:

1. **Legal Equivalence**: As per Rule 9A, any certificate or document issued or shared through DigiLocker is considered at par with physical documents under Indian law.

2. **Issuers and Requesters**: Issuers (like CBSE, UIDAI, RTOs, etc.) can push digitally signed documents directly into a citizen's DigiLocker.

3. **Requesters** (such as government departments, universities, or employers) are legally bound to accept these digital documents as valid and original.

4. **Single Source of Truth**: If a document is accessed via a URL (link) that leads to the issuer's repository, it is deemed to be authentic and verified, eliminating the need for physical verification.

5. **Notification and Enforcement**: Rule 9A was officially notified via G.S.R. 111(E) on 8th February 2017, with effect from 21st July 2016

Exhibit-2 :**Key Agencies on DigiLocker (As on July 2025)**