



सत्यमेव जयते

National e-Governance Division
Ministry of Electronics & Information Technology
Government of India

DigiLocker

International Implementation Framework

Standard Operating Procedure for National Digital Document Wallet Deployment

Published by	Document Type
National e-Governance Division (NeGD) Ministry of Electronics and Information Technology (MeitY), Government of India	Standard Operating Procedure

Intended Audience
Any country seeking to implement a DigiLocker-equivalent National Digital Document Wallet in collaboration with DigiLocker, National e-Governance Division, Ministry of Electronics and Information Technology, Government of India.

1. About This Document

This Standard Operating Procedure has been developed by the National e-Governance Division, Ministry of Electronics and Information Technology, Government of India, as a universal reference guide for any country or government entity seeking to codevelop and implement a DigiLocker-like National Digital Document Wallet in its country in collaboration with DigiLocker, National e-Governance Division, Ministry of Electronics and Information Technology, Government of India. It draws from real-world implementation experience across multiple countries and is designed to be adapted to any national context.

1.1 Purpose

- Provide a step-by-step implementation guide for deploying a National Digital Document Wallet ecosystem
- Define governance structures, roles, and responsibilities at every phase
- Specify technical and functional requirements for a scalable, secure deployment
- Enable knowledge transfer and capacity building
- Establish quality, compliance, and go-live standards

1.2 Scope

- Any sovereign government seeking to establish a National Digital Document Wallet system in collaboration with the National e-Governance Division (NeGD), Ministry of Electronics and Information Technology (MeitY), Government of India
- Government ministries, agencies, and technology partners involved in implementation
- Technical and policy teams evaluating DigiLocker as a national deployment model

2. Platform Overview and Expected Outcomes

DigiLocker is India's flagship cloud-based platform enabling citizens to store, access, and share official government-issued documents digitally. Launched in 2015 under the Digital India Programme, it now serves over 700 million users and is designed for global adaptability.

2.1 Core Architecture Components

Component	Description
Citizen Portal and Mobile Application	Web and mobile interface for citizens to register, access, manage, and share documents
Issuer Ecosystem	Application Programming Interfaces (APIs) and gateway enabling government departments to issue documents directly into citizen wallets
Requestor and Verifier Ecosystem	Secure OAuth 2.0-based verification channel for organisations to verify documents with citizen consent
Access and Consent Gateway	Manages consent-based document sharing, ensuring citizen privacy and data sovereignty
Admin Portal	System management, issuer and requestor onboarding, analytics, and compliance monitoring

Component	Description
Identity Integration Layer	Connects with the national identity system for citizen authentication and account creation

2.2 Expected Outcomes

#	Expected Outcome	Key Benefit
1	Digital issuance of government documents	Eliminates paper-based production costs and anytime access
2	Citizen-owned digital document repository	Empowers citizens with self-sovereign document access
3	Consent-based document sharing	Protects citizen privacy and data rights
4	Real-time document verification	Reduces fraud and speeds up service delivery
5	Paperless delivery of public services	Reduces bureaucracy and increases efficiency
6	Reduced document fraud	Cryptographic verification prevents forgery
7	Improved ease of doing business	Faster document submission and verification for businesses
8	Inter-agency interoperability	Unified document ecosystem across all government arms

3. Key Stakeholders and Governance Structure

Successful implementation requires active participation from the following stakeholders. Country may identify its own equivalent agencies and constitute the two mandatory governance bodies below.

3.1 Key Stakeholders

Stakeholder	Typical Examples	Primary Role
Lead Government Ministry	Ministry of Information and Communications Technology / Digital Transformation / e-Government Authority	Project ownership, policy decisions, funding, inter-agency coordination
National Identity Authority	National Identity Authority, Civil Registration, Population Registry	Citizen authentication, identity verification, single sign-on integration
Issuing Agencies	Transport Department, Education Ministry, Tax Authority, Immigration	Official document issuance into citizen wallets via application programming interfaces (APIs)
Requestor and Verifier Agencies	Banks, Universities, Employers, Government Departments	Consent-based document verification for service delivery
Data Protection Authority	National Data Protection Agency / Privacy Commissioner	Regulatory oversight, compliance approval, data governance, data privacy

Stakeholder	Typical Examples	Primary Role
India National e-Governance Division Team	National e-Governance Division, Ministry of Electronics and Information Technology, Ministry of External Affairs	Technical development, knowledge transfer, go-live support

4. Pre-Implementation: Initiation and Agreements

Before any technical work begins, two pre-implementation activities must be completed. These form the official entry points for any country initiating the DigiLocker implementation journey.

4.1 Formal Agreements

Agreement	Purpose	Parties	Mode of Interaction
Memorandum of Understanding / Implementation Framework Agreement	Establishes official partnership, scope, deliverables, and mutual obligations for platform co-development	Host Country Government and Government of India (Ministry of External Affairs and Ministry of Electronics and Information Technology)	Physical
Non-Disclosure Agreement	Protects proprietary technical architecture, source code, and sensitive platform information	Host Country Technical Team and National e-Governance Division / Ministry of Electronics and Information Technology	Physical or Online
Data Sharing and Processing Agreement	Governs handling of citizen data, test data, and government data shared during integration and testing	Host Country Data Protection Authority and National e-Governance Division	Physical or Online

4.2 Technical and Feasibility Assessment Visit

A feasibility visit by the DigiLocker team to the host country is required during implementation of DigiLocker before GO LIVE. Timing is agreed mutually.

Assessment Domain	Key Evaluation Points
Digital Identity Platform	Existence of national identity system, authentication interface availability and documentation maturity
Cloud and Data Center Infrastructure	Cloud platforms available (public, private, or hybrid), data centre capacity, network bandwidth etc.
Mobile and Internet Penetration	Smartphone penetration, internet coverage (urban versus rural), digital literacy levels

Assessment Domain	Key Evaluation Points
Language and Localization	Official languages, Unicode support, right-to-left or left-to-right requirements, existing portal localization
Regulatory Environment	Data protection legislation, electronic signature law, electronic document legal validity
Existing Government Platforms	e-Citizen portals, payment systems, existing interface ecosystems, interoperability standards
Technical Resource Availability	Local developers, DevOps engineers, security specialists for the project team

Deliverables from Pre-Implementation Phase

- Signed Memorandum of Understanding / Implementation Framework Agreement
- Signed Non-Disclosure Agreement
- Feasibility Assessment Report with infrastructure gap analysis
- Implementation Charter (approved by mutual consensus)
- Project Governance Structure (Technical Working Group constituted)
- High-Level Implementation Roadmap with tentative timelines

5. Implementation Steps

The implementation follows nine sequential steps aligned with real-world deployments. Total estimated duration is 24 to 36 weeks depending on country-specific complexity.

Step	Activity	Mode of Interaction
1	Identification of Authentication Mechanism — interface for DigiLocker account creation and login	Online
2	Identification of 2 to 3 pilot Issuing Departments and documents for the pilot phase	Online / Offline
3	Provide identified APIs to the India DigiLocker team for Minimum Viable Product integration and initial testing	Online
4	Minimum Viable Product presented to host country for initial feedback and testing	Online
5	Development of all modules: partner onboarding, user authentication, document issuance and management, document verification	Online
6	Product submitted for Vulnerability Assessment and Penetration Testing, User Acceptance Testing, and pilot rollout deployment	Online / Offline
7	Limited release to controlled user group, then full national rollout to all citizens	Online
8	India National e-Governance Division team provides critical online hypercare support for first 3 months post go-live	Online

Step	Activity	Mode of Interaction
9	Full Knowledge Transfer: documentation, source code, operations training to ensure host country team is self-sufficient	Online

5.1 Phase Grouping and Timeline

Phase	Description	Duration
Phase 1: Planning and Preparation	Strategic alignment, roadmap, technical knowledge transfer (Steps 1 to 3)	2 to 4 Weeks
Phase 2: Architecture and Development	Platform foundation, authentication integration, issuer interfaces, citizen portal, mobile applications (Steps 3 to 5)	14 to 20 Weeks
Phase 3: Testing and Compliance	Vulnerability Assessment and Penetration Testing, User Acceptance Testing, load testing, regulatory sign-off (Step 6)	4 to 6 Weeks
Phase 4: Pilot and National Rollout	Controlled release, full rollout, hypercare support (Steps 7 to 9)	4 to 8 Weeks and Ongoing

6. Knowledge Transfer and Capacity Building

Knowledge transfer is woven throughout the implementation lifecycle — not a single end-of-project activity. The objective is to ensure the host country's technical team can independently operate, maintain, and scale the platform after the National e-Governance Division's engagement concludes.

Phase	Knowledge Transfer Activity	Format
Phase 1	Technical stack orientation, infrastructure sizing, best practices walkthrough	Workshop (Physical or Virtual)
Phase 2	Architecture review, environment setup, Development Security Operations training	Hands-on Sessions
Phase 3	Module-by-module code walkthroughs, interface documentation handover, mid-development review	Pair Programming, Documentation, and Visit
Phase 4 — Testing	Security testing methodology, compliance framework, testing tools training	Training Sessions
Phase 4 — Pilot	Production operations training, monitoring tools, incident management	On-the-Job Training
Post Go-Live	3-month support, issue resolution, performance tuning	Online Support and Documentation

7. Go-Live Checklist and Post-Launch Support

7.1 Pre-Go-Live Checklist

All items below must be confirmed complete before production go-live is approved by the National Steering Committee.

#	Checklist Item
1	Security audit (Vulnerability Assessment and Penetration Testing) completed; all critical and high findings remediated
2	User Acceptance Testing formally approved and sign-off obtained from Lead Ministry
3	Production infrastructure provisioned and hardened
4	Disaster Recovery site operational and tested
5	Monitoring, alerting, and dashboards fully configured
6	Backup and restore procedures tested and documented
7	Data protection compliance sign-off obtained
8	All pilot issuer agencies integrated and validated
9	Operations and support team trained and rostered
10	Full documentation package handed over and acknowledged
11	Citizen awareness and communication campaign prepared
12	Rollback procedure tested and ready
13	Production deployment finalized
14	Formal go-live

8. Conclusion

The DigiLocker International Implementation Framework is a blueprint for transforming how governments serve their citizens in the digital age. Grounded in India's decade-long experience building one of the world's largest digital document ecosystems, this Standard Operating Procedure distils proven governance models, engineering practices, and change management strategies into a framework that any sovereign government can adopt and adapt.

Successful implementation requires sustained commitment at every level: leadership, technical rigor from implementing teams, regulatory clarity from oversight bodies, and genuine engagement with the citizens the platform ultimately serve. It is expected that a secure, scalable, citizen-centric digital document wallet is achievable within a structured 24 to 36 week timeline.

The National e-Governance Division, Ministry of Electronics and Information Technology, remains a committed partner throughout this journey — from the signing of the Memorandum of Understanding and the initial feasibility visit, through every phase of development, testing, and go-live. Post-deployment support and structured knowledge transfer ensure that host country teams are not merely recipients of a system, but fully capable stewards of a national digital infrastructure.

As digital governance standards continue to evolve globally, the DigiLocker platform is designed to evolve with them — supporting emerging interoperability frameworks, strengthening data sovereignty mechanisms, and expanding the ecosystem of issuers and verifiers. Governments that invest in this foundation today are building the digital trust infrastructure that will underpin public service delivery for generations.

For Implementation, Enquiries and Partnerships

- 1. May please contact Mission offices (Indian Embassies) of your country.**
- 2. May write to**
 - **director.anc@digitalindia.gov.in**
 - **dlmanagement4@digitalindia.gov.in**
 - **partners@digitallocker.gov.in**