National e-Governance Division (NeGD)

Ministry of Electrnics and Information Technology (MeitY)

Partner Organisation Onboarding Standard Operating Procedure (SOP) for DigiLocker

(5th June, 2024)

1. Introduction

DigiLocker aims to provide paperless governance and to reduce administrative overhead by minimizing the use of paper and curtail the verification processes. It allows registered Partner Organisations to integrate with the platform using APIs and acts as a secure document exchange platform between the Partner Organisation and the Citizen. This document outlines the standard operating procedures for onboarding new Partner Organisations and integrating them with the DigiLocker ecosystem.

2. Scope

This Standard Operating Procedure (SOP) outlines the comprehensive process for onboarding Partner Organisations into DigiLocker ecosystem. It specifies the eligibility criteria for organizations seeking to become DigiLocker Partner Organisations. It encompasses Partner OrganisationIdentification, Evaluation, Verification, Agreement or Terms of Service (TOS),Technical Integration, Testing, Launch, and Ongoing Support.

3. Eligibility of Partner Organisations to get registered as Issuing or Requesting authorities on DigiLocker Platform.

i. Partner Organisation should be registered with or under MCA/ MSME/ Start up India/ Society Act/ Companies Act/ Partner Organisationship Act/Trusts etc. in India.

ii. The Partner Organisation shall possess demonstrable experience in providing online services to Indian citizens. Following listed entities can become a Partner Organisation:

a) All central government Organizations
b) All state governments Organizations,
c) All private Organizations
d) All public limited Organizations,
e) All PSUs,
f) All Partner Organisationship firms,
g) All Proprietorship firms,
h) All Societies and Trusts

iii. The Partner Organisation must have a functional website portraying the nature, type and mode of online services being delivered to Indian Citizen.

iv. Partner Organisations must have an authorization from the appropriate governmental regulatory bodies to issue and authenticate documents for citizens of India.

v. Partner Organisations must be able to access digital documents issued by authorized agencies and provide additional value-added services to Indian Citizen.

vi. Partner Organisations must have a requisite digital infrastructure to perform the value added service efficiently within India.

vii. Partner Organisations must have their own digital signatures and DOC Signing for DigiLocker API integration.

viii. Partner Organisations must have official domain email Ids.

4. Partner Organisation Onboarding process

i. **Liaison and Support: The Business Development Team shall undertake liaison duties with both prospective and current** Partner Organisation**s concerning all products/projects of DIC/NeGD. This includes organizing meetings and workshops to facilitate communication. Furthermore, the team is designated as the primary point of contact for entities pursuing** Partner Organisation**ship opportunities with DigiLocker.** The team shall provide **support to these organizations/departments throughout the integration process.** During the **Post-integration** phase the team shall **liai**son **with relevant regulatory bodies to secure official Notifications or Government Orders endorsing the project/product.**

a) **Registration and Vetting of Partner Organisations**: Partner Organisations are required to register on DigiLocker **Partner Organisation's Portal** only through the DigiLocker account of the authorized person at the Partner Organisation.The vetting process for organizations applying to the DigiLocker Partner Organisations Portal involves several critical steps as detailed below:

b) **Telephonic Meeting:** DigiLocker team shall arrange for a telephonic meeting with the applying organizations wherein the authorised personnel shall be required to verify the accuracy of the information provided on the Partner Organisation's Portal and address any discrepancies or inconsistencies in the request made by the Partner Organisation.

c) **Details Verification:** All details submitted by the Partner Organization shall meticulously reviewed by the DigiLocker team.

d) **Authentication of Digital Signatures:** For seamless API integration the DigiLocker team shall ensurethatthe Partner Organisation has an authenticated digital signatures or DOS.

e) Partner Organisation shall mandatorily sign Agreement/Terms of Use mentioned on the DigiLocker portal.

ii. **Approval of Application**: After the organization has been successfully registered on the Partner Organisations Portal and has undergone thorough vetting of its use cases and user journey, the Onboarding team will initiate a formal request for Partner Organisation approval within the portal. This request is forwarded to the Onboarding Partner Organisation Approval Committee, which shall consist of the BD Head, BD Manager, and Legal Compliance Manager. Upon their recommendation, the request shall be documented and shall be put up on the file for final approval to the CEO

iii. **Onboarding Committee:** Onboarding Committee comprising of the Onboarding leads, the Partner Organisationships Head, and a Legal team member shall hold weekly meetings to review and approve the scrutiny of business teams representing organizations applying on the DigiLocker Partner Organisation portal. The Committee's recommendations will be documented and shall be put up on the file for final approval by the CEO.

iv. **Legal Compliance:** Legal Team shall draft/vet/review all documents pertaining to the Partner Organisationship Agreement/Memorandum of Understanding (MoU)/Contract, and all other documents to be entered into with the Partner Organisation Organizations, to ensure compliance with the applicable laws including but not limited to data privacy regulation.

v. **Technical onboarding:** Technical Onboarding Team shall be responsible for technical integration, rigorous testing, and ensuring complete compliance with DigiLocker Application Programming Interfaces (APIs). The Partner Organisation's technical team shall receive comprehensive technical documentation, detailed APIs, and explicit integration guidelines from the Technical onboarding team. The Partner Organisation's technical team shall seamlessly integrate their systems with DigiLocker, utilizing the provided APIs. Throughout the integration process, DigiLocker's Technical onboarding Team shall extend technical assistance and support to the Partner Organisation.

vi. **Testing and Go Live**: The Partner Organisation's integration with DigiLocker shall be tested to ensure compatibility, functionality, and data security. Test cases to be executed to validate various use cases, such as document upload, retrieval, and sharing.Any issues or bugs identified during testing to be reported, resolved, and retested until satisfactory results are achieved.

vii. **After Go Live**: Upon successful completion of the testing, the Partner Organisation's integration with DigiLocker shall be approved for launch. The Partner Organisation shall be provided with **launch support,** including promotional materials, user guides, and training resources. Ongoing **technical support** and assistance shall be made available to the Partner Organisation to address any issues or concerns. Transaction monitoring shall be done through regular and periodic routine assessment of the

organization process flow with DigiLocker. The Partner Organisation shall submit a quarterly report of usage / operations. Partner Organisations must also specify the business cases for which they utilize DigiLocker APIs.

5. Guidelines for Partner Organisations Registration and Approval on DigiLocker platform.

i. Organization should register with a DigiLocker account of the authorized personnel only.

ii. Organization is required to provide the email id having official domain only. Any email with personal email domains is liable to be rejected.

iii. Telephonic Meeting by DigiLocker will be done to ensure the authenticity and verify the request.

iv. Organization is required to provide all the relevant details that areto be entered inthe registration form. Any incorrect/incomplete request will be rejected.

v. Use case details provided should be thoroughly submitted and no deviation shall be allowed.

vi. No requests of temporary access for any testing purpose etc. will be entertained.

vii. Organization needs to have a digital signature available since that maybe required for DigiLocker API integration.

viii. Organization should share the demo flow and testing data of its integration before going live.

ix. Organization should strictly follow DigiLocker's Terms of Service, failing which the API Account is liable to be blocked without any notice. Link for the same is - https://apisetu.gov.in/digilocker

x. Multiple registrations of the same organization are not allowed. Duplicate requests will be rejected.

xi. Unverified accounts will be automatically deleted by the system after 3 months of approval.

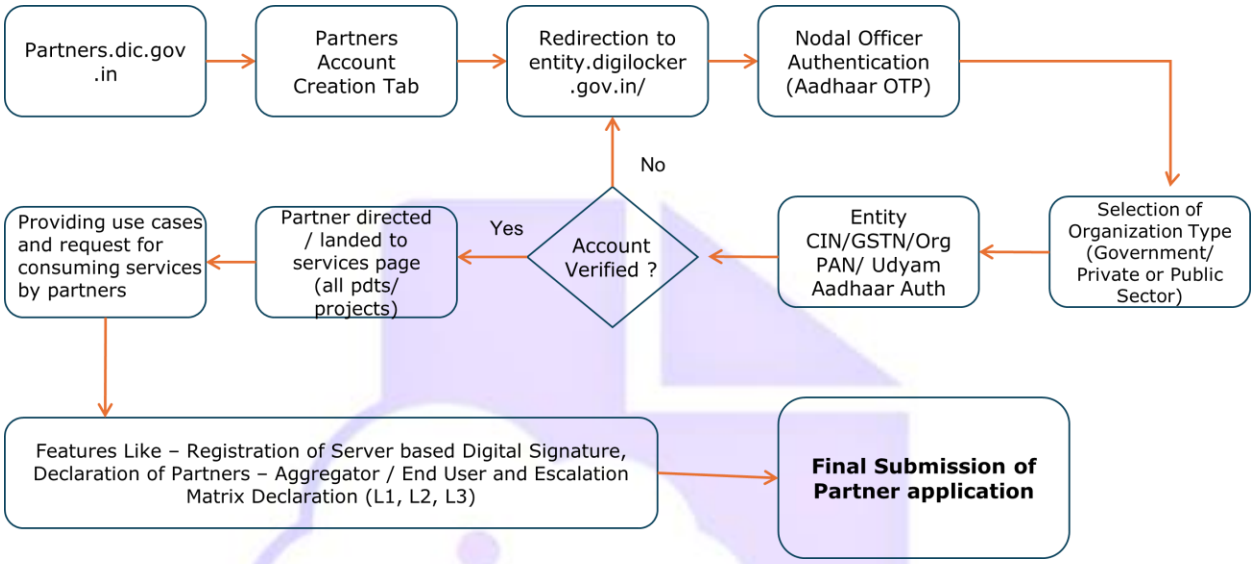
xii. Verified but inactive accounts will be automatically disabled by the system after 3 months of inactivity.

xiii. In case of any change in authorized personnel or contact details, organization should get in touch with DigiLocker team to get the information updated.

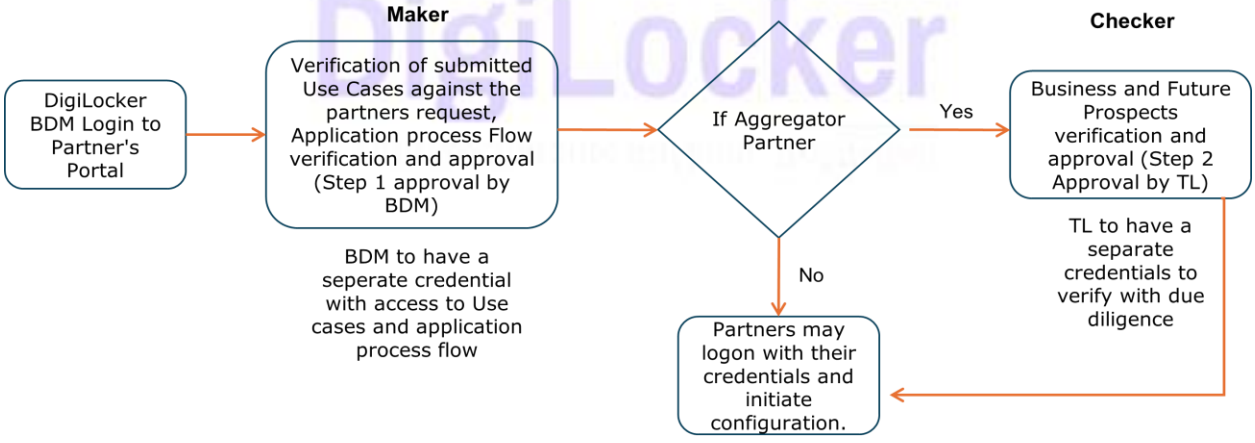
xiv. Organization should never divulge the details such as client id, client secret, username etc. on the public domain. If found so, such account will be blocked immediately without any intimation.

6. Proposed Partner Organisation OnboardingFlow

i. Proposed Partner Organisation Application Process through Partner Organisation's Portal-DigiLocker



ii. Proposed Partner Organisation Apporval Process through Partner Organisations Portal-DigiLocker



iii. **<u>Entity Verification</u>**

a) The Partner Organisation organization is redirected from Partner Organisation's portal to entity Locker verification page for nodal officer authentication using Aadhaar OTP.

b) Critical details like CIN, GSTIN, PAN, and Udyam Aadhaar numbers are verified via this process before proceeding.

c) The Partner Organisation must have a valid digital signature for authentication during API calls.

iv. UseCase Submission

Post entity verification, the Partner Organisation is directed to the services page on the Partner Organisation's portal to review available APIs and submit relevant use cases they want to implement.

v. ApplicationSubmission

The Partner Organisation then submits the final onboarding application form online and receives an automated email confirmation.

vi. 2-StepApproval

a) The Business Development Manager (BDM) thoroughly reviews the Partner Organisation's registration details before approval.

b) The BDM reviews the submitted use cases and proposed integration flow.

c) BDM then submits the application to committee for their decision.

vii. Integration

a) Once approved by the committee, the Partner Organisation gains access to the Partner Organisation Portal where they can initialize API integration.

b) Usage Terms and policies must be strictly adhered to.

c) Inactive accounts may be blocked or deleted after a period of inactivity.

viii. Post Integration Monitoring

a) The Partner Organisation organization provides periodic reports declaring the number and types of documents being accessed through the APIs and STQC audit report of their application.

b) DigiLocker officials also monitor and check API call volumes and usage statistics regularly.