APPLICATION FOR ONBOARDING ON API SETU

Contents

SECTION I – INTRODUCTION

In 2009, the National e-Governance Division was created by the Ministry of Electronics & Information Technology as an Independent Business Division under the Digital India Corporation {erstwhile Media Lab Asia}. Since 2009, NeGD has been playing a pivotal role in supporting MeitY in Programme Management and implementation of the e-Governance Projects; provide technical and advisory support to Ministries/ Departments, both at Central and State levels along with other Government organizations. NeGD's major operational areas include programme management, project development, technology management, capacity building, awareness and communications related activities under the flagship Digital India Programme. NeGD has developed and is managing several National Public Digital Platforms such as DigiLocker, UMANG, Rapid Assessment System, OpenForge, API Setu, Poshan Tracker, Academic Bank of Credits, National Academic Depositories, National AI Portal, My Scheme, India Stack Global, Meri Pehchaan, etc.

NeGD intends to create a robust ecosystem through strategic initiatives and collaborations spanning both public and private domains and hence wishes to empanel multiple API Solution/Service providers, including private API providers, on API Setu with the vision to deliver substantial benefits, both for the Government and citizens.

Further, NeGD invites Request for Onboarding applications from experienced and qualified Firms/Service Providers/service providers for "Onboarding of Application Programming Interface (API) under the API Setu initiative. API Setu serves as a unified platform to enable seamless API integrations, promote interoperability, and facilitate secure, scalable, and robust data exchange between systems.

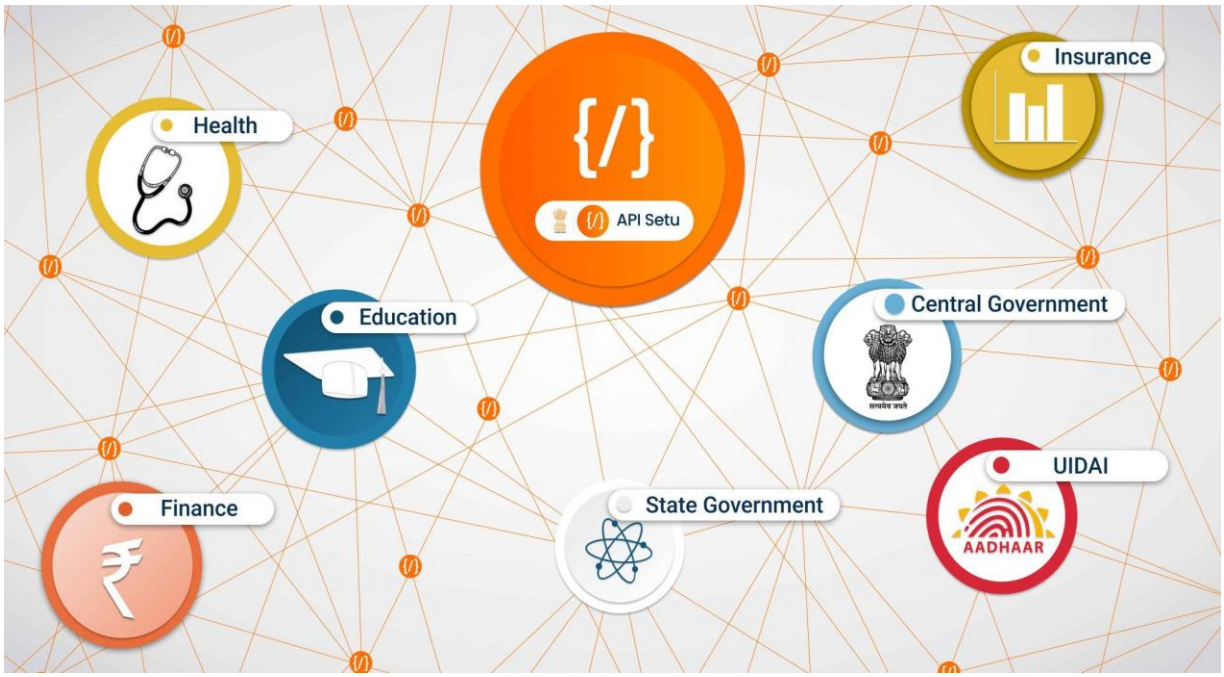
ABOUT API SETU

API Setu is an Open API (Application Programming Interface) Platform from the Ministry of Electronics and IT, Government of India. One of the major objectives of the platform is to build an open and interoperable digital platform to enable seamless service delivery across Government Departments. One of the aims of the platform is to enable and promote safe and reliable sharing of information and data across various e-Governance applications and systems.

API Setu is one such Open API platform from MeitY, that aims to bring digital transformation. It is based on the Government's Open API policy to ensure swift, transparent and secure exchange of information across diverse digital domains.

The platform is developed referring to the Open API policy that was notified by MeitY in the year 2015, that focuses upon:

- Building open and interoperable digital platform to enable seamless service delivery across government silos
- Promoting 'API first' approach ; (Re-usability)
- Enabling and promoting safe and reliable sharing of data across various e-Governance applications and systems.
- Promoting innovation through the availability of data from e-Governance applications and systems to the industry and public.
- Providing guidance to Government organizations in developing, publishing and implementation using these APIs.



API Setu APIs are interconnected

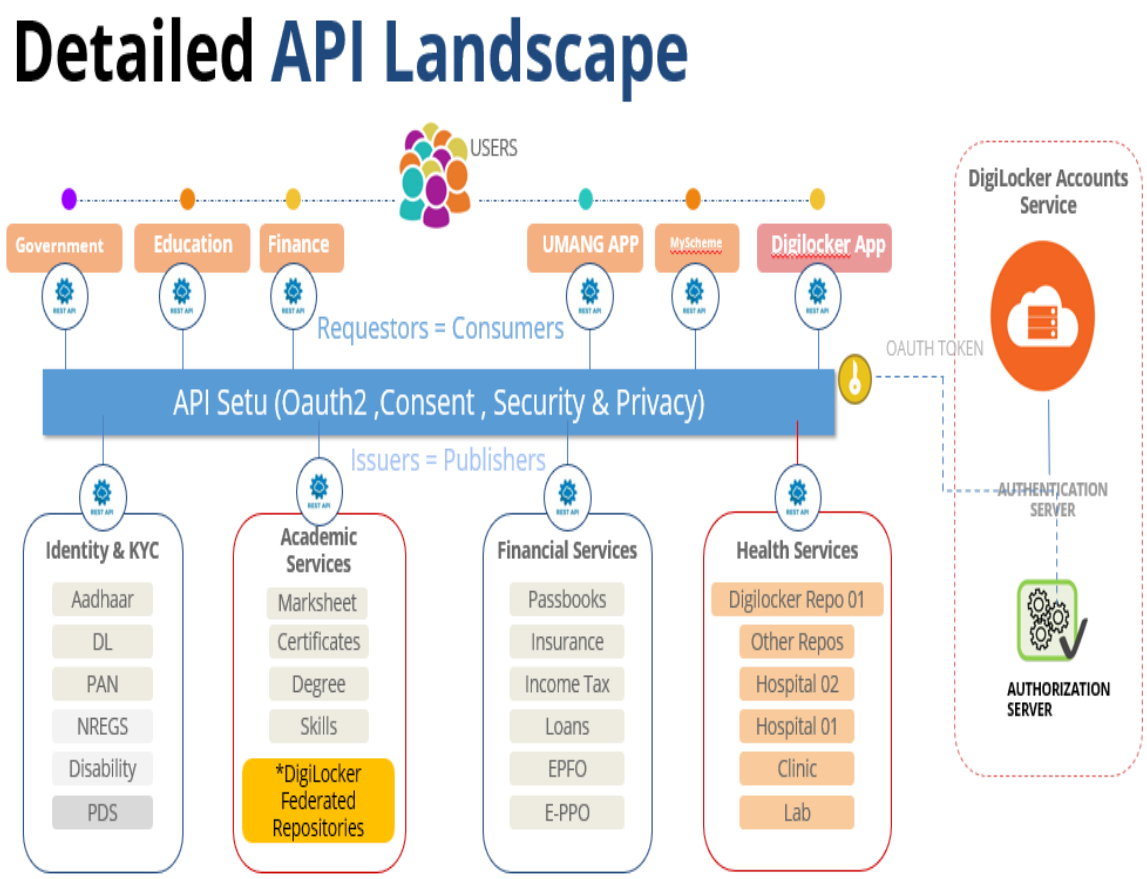
It hosts a vast number of APIs that are published and consumed by various Government and private entities, who in turn can develop user-centric innovative products for various sectors such as health, education, business etc.

For instance, API of the CoWIN platform powered several vaccine scheduling apps, which ensured that India could fight the pandemic effectively. Or API's of DigiLocker are transforming document access, sharing and verification through various partners.

API Setu connects with UMANG, DigiLocker, PAN, CBSE Results etc. together breaking the silos and building a digitally empowered Nation.

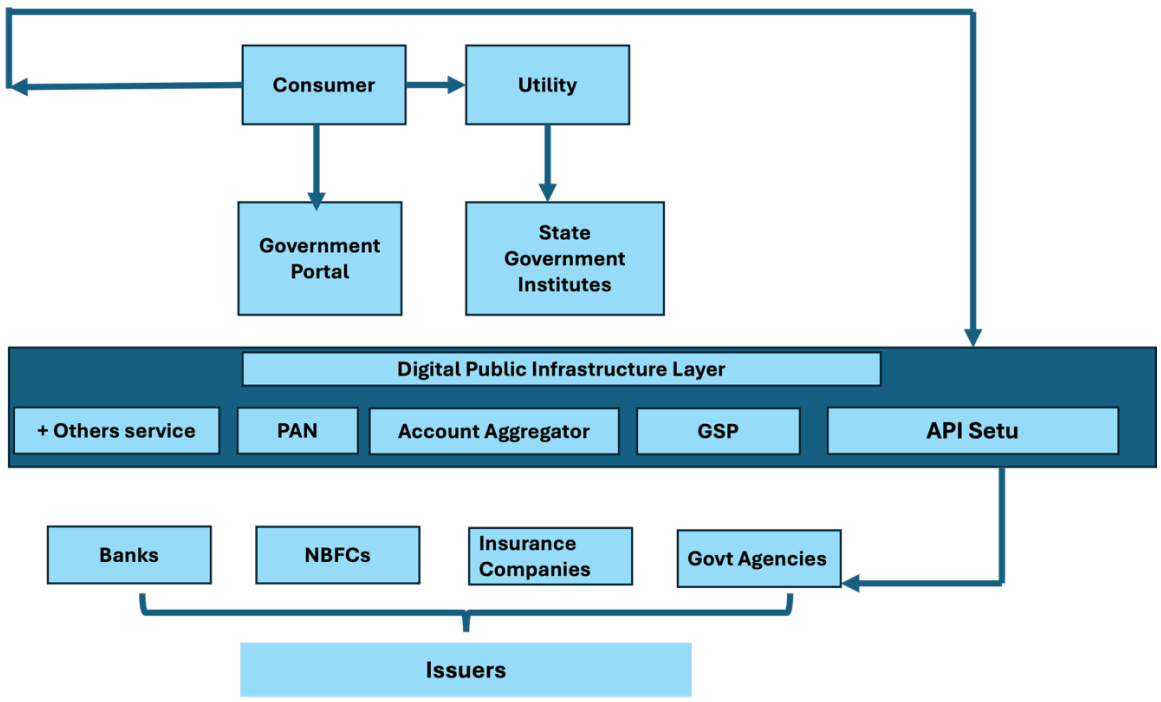
As on date API Setu has more than 2000 partners with more than 6400 published APIs. The platform records approximately 80 million transactions every month.

The platform is fully functional and is available at https://apisetu.gov.in



Alignment with India Stack, ONDC, ULIP, and Sahamati Frameworks

This empanelment initiative is strategically aligned with India's digital public infrastructure vision, particularly the India Stack framework, which promotes interoperable, secure, and scalable APIs for identity, payments, data sharing, and consent-driven services. The onboarding of private API providers under these Guidelines for Onboarding will further enable the seamless exchange of data and services across Government-to-Citizen (G2C), Government-to-Business (G2B), and Government-to-Government (G2G) interfaces. Additionally, the initiative complements national digital platforms such as ONDC (Open Network for Digital Commerce), ULIP (Unified Logistics Interface Platform), and the Sahamati-led Account Aggregator ecosystem, encouraging innovation and efficiency through standardisation and plug-and-play architecture. API Setu will serve as the unified interface layer to ensure discoverability, governance, and trust in API consumption at scale.



SECTION II – SCHEDULE OF EVENTS

S. No	Event	Date
1.	Date of commencement of Request for Onboarding Process	13th May 2025
2.	Last date for receiving comment, if any (Only via email : partners.apisetu@digitalindia.gov.in)	25th May, 2025
3.	Last Date and Time for Request for Onboarding Submission along with all supporting documents for Round 1. Submissions to remain open and evaluated on an ongoing basis.	30th May, 2025
4.	Date of Technical Presentations for Round 1	To be notified

SECTION III – PURPOSE/ OBJECTIVE

NeGD intends to empanel reputed API provider Companies/Firms /Service Providers that can offer:

- Handling the entire API lifecycle, encompassing design, implementation, development, deployment, management and monitoring, along with the dedicated tools to assist in the completion of tasks at each level.
- API integration solutions across diverse systems and platforms.
- Secure, reliable, and scalable API services to enhance interoperability across Government and Non-Government entities.
- Value-added services such as API analytics, monitoring, lifecycle management, and versioning.
- Support for microservices architecture and emerging API frameworks.
- Support various internal and external APIs by incorporating quintessential security features and offer consistent and modern API Management Solution functionality for new/existing back-end services.

Onboarded providers will play a critical role in advancing the API Setu ecosystem by ensuring the availability of robust, standardized, and interoperable APIs for government entities to consume. In turn, private API providers will have rapid access to government projects. The API Providers shall be onboarded only after evaluating the onboarding criterion as laid down in Annexure VII and should cater to legitimate business purposes as desired by B2G, G2G, and G2C services. Detailed API business purposes can be seen in Annexure VIII.

SECTION IV – INDICATIVE STEPS TO PUBLISH APIs ON API SETU

The onboarding process shall entail more than just connecting APIs. It must involve multiple layers of review, testing, and validation to ensure that API Setu can provide secure, scalable, and efficient services to Government Departments. Each API must undergo an iterative process from registration to production release, with checks for data privacy, compliance, and operational performance at every stage.

- Registration of the API Provider
- Submission of API Documentation
- Compliance, Security, and Privacy Review
- Technical Review and Sandbox Testing
- Contract Signing and Legal Agreements
- Approval of API Publication

Roles and Responsibilities in API Onboarding Process:

- API Provider: Submit documentation, test the API, and ensure privacy compliance.
- API Setu Team: Review, test, and validate API. Enforce SLAs and DPAs.
- NeGD Legal Counsel: Draft and review SLA, DPA, and privacy policies.
- NeGD Technical Reviewers: Conduct sandbox testing and performance benchmarking.
- API Setu Security Team: Conduct penetration testing and ensure compliance with privacy laws.

SECTION V – SCOPE OF WORK

The empanelled API service providers will be expected to comply with the technical criterion as laid down in Annexure VI at the time of onboarding to API Setu and, further, maintain the performance as laid down in Annexure VII. We envisage that the APIs shall be tested on technical criteria, and a detailed report shall be made available to any Government entity that intends to utilize the published APIs via API Setu. The API provider shall make provisions for integration with NeGD's reporting dashboards for automated fetching of KPI data for error-free reporting and measurement of performance score on a rolling basis.

API analytics to track:

- Usage trends, success/error rates, and performance metrics.
- Generate periodic reports for stakeholders to measure API effectiveness.

Apart from setting up the DC and DR site, the Service Provider shall also be responsible for creating separate Development, UAT, and Sandbox/Pre-Production environment setups for multiple users, simulating near-production functionalities per the MeitY requirement.

Service providers must ensure a resolution time of 4 hours for any issue in the solution, individual APIs, etc.

(This Space Intentionally Left Blank)

SECTION VI – VALIDITY OF EMPANELMENT AND TERMINATION

The validity of the empanelment will be for 36 months and further extendable for another 24 Months as deemed by NeGD based on mutual consent and subject to fulfilment of the performance criterion laid down in Annexure VII. The validity of empanelment may be extended for a suitable period at the behest of the NeGD. Irrespective of the period, the empanelment will be deemed operative until the completion of the assigned projects and hence the empaneled firm should ensure resource availability until completion of the work at hand.

Termination: The Authority may, by not less than 30 (Thirty) days written notice of termination to the selected Service Provider, such notice to be given after the occurrence of any of the events specified in this clause, terminate this Agreement if:

- The selected Service Provider fails to remedy any breach hereof or any failure in the performance of its obligations hereunder, as specified in a notice of suspension, within 90 days of receipt of such notice of suspension or within such further period as the Authority may have subsequently granted in writing;
- The selected Service Provider becomes insolvent or bankrupt or enters into any agreement with its creditors for relief of debt or takes advantage of any law for the benefit of debtors or goes into liquidation or receivership, whether compulsory or voluntary;
- The selected Service Provider fails to comply with any final decision reached because of arbitration proceedings; The selected Service Provider submits to the Authority a statement which has a material effect on the rights, obligations, or interests of the Authority and which the selected Service Provider knows to be false;
- Any document, information, data, or statement submitted by the selected Service Provider in its Proposals, based on which the selected Service Provider was considered eligible or successful, is found to be false, incorrect, or misleading;
- As a result of Force Majeure, the selected Service Provider cannot perform a material portion of the Services for more than 60 days, or The Authority, in its sole discretion and for any reason whatsoever, decides to terminate this Agreement.

Note: This document is not exhaustive in describing the functions, activities, responsibilities, and services for which the Service Provider will be responsible. The Service Provider, by participation in this Onboarding process, implicitly confirms that if any functions, activities, responsibilities, or services which are either not explicitly described in these Guidelines for Onboarding or specifically described but have to undergo suitable changes/modifications due to regulatory/statutory changes and are termed necessary or appropriate by NeGD for the proper performance of the contract, such functions, activities, responsibilities or services (with applicable changes, if any) will be deemed to be implied by and included within the scope of services under these Guidelines for Onboarding and Service Provider's response to the same

extent and in the same manner as if specifically described in the Service Provider's request for Onboarding.

(This Space Intentionally Left Blank)

SECTION VII – SERVICE PROVIDER'S ELIGIBILITY CRITERIA

S. No.	Requirement	Specific Requirement	Documents Required
	Certificate of Incorporation	The Service Provider must be an Indian Company/ LLP /Partnership firm registered under the applicable Act in India and should have existed continuously for at least the last 3 completed fiscal years as of the date of Onboarding request. Registered with the Income Tax Authorities. Registered with the GST Authorities.	A copy of the Certificate of Incorporation and the Memorandum and Articles of Association are required. Copy of PAN Card. A copy of the GST Registration Certificate was issued by GSTN authorities.
	Turnover	The Service Provider must have an average turnover of a minimum of Rs. 10 crores during the last 03 (three) fiscal year(s) i.e., FY 2021-22, FY2022-23 and FY 2023-24. This must be the individual company's average turnover and not that of any group of companies. MSME agencies registered with the Government are exempted from turnover criteria.	Copy of the audited Balance Sheets and CA certified details for the last 3 financial years are to be submitted
	Profitable organization	The Service Provider should be a profitable organization on the basis of profit before tax (PBT) for the last 03 (three) fiscal year(s) i.e., FY 2021-22, FY2022-23 and FY 2023-24.	CA certified details for the last 3 financial years are to be submitted
	Litigations	Past/ present litigations, disputes, if any (Adverse litigations could result in disqualification, at the sole discretion of the NeGD)	Undertaking by the authorized signatory and a copy of court orders as proof.

	Quality Certification	The Service Provider should have any three (3) of the following valid certifications: 1) ISO 9001:2015 or above certifications 2) ISO/IEC 27001:2022 3) ISO / IEC 20000 -1: 2018 4) ISO 22301:2019 5) SOC 2 Type II Attestation	Copy of Valid certificates.
6.	Compliance	The Service Provider (including its OEM, if any) must comply with the requirements contained in OM No.F.7/10/2021-PPD (Order Public Procurement No. 4)	Undertaking by the authorized signatory
7.	Experience	The Service Provider should have experience of minimum 3 years in providing solution / services which includes development, implementation and operation/ maintenance of API technologies, including RESTful APIs, and API management platforms for a period of at least the last three completed financial years as of the last date of submitting a Request for Onboarding.	Detailed technical capability statement highlighting experience work orders, or completion certificates mentioning use of these technologies
8.	Blacklisting	Undertaking by the authorized signatory of the Service Provider that the Service Provider or any of the associated Directors is currently not blacklisted by any Government Organizations, Public Sector Undertakings or Public Limited Companies and is not under a declaration of In-eligibility for corrupt or fraudulent practices as on the date of submission.	Undertaking by the authorized signatory (As per Annexure V)

The process is open to all Service Providers who meet the eligibility criteria outlined below and agree with NeGD according to the terms and conditions of this Guideline for Onboarding document. Service

Providers must provide the necessary documentary evidence supporting the eligibility criteria specified in the onboarding process. Onboarding requests that do not meet the eligibility criteria will be rejected.

SECTION VIII – REQUEST FOR ONBOARDING SUBMISSION PROCESS

1. **Raising of queries/clarifications on Request for Onboarding document:** The Service Providers requiring any clarification on this document should submit their written queries to email ID: partners.apisetu@digitalindia.gov.in. Any suggestions/feedback may also be sent to the above email ID.

2. **Modification in Request for Onboarding document:** At any time, NeGD may modify any part of this document. Such change(s) if any may be in the form of an addendum/corrigendum and will be uploaded on NeGD website https://NeGD.gov.in/. All such changes will automatically become part of this Guideline for API Service Providers and will be binding on all Service Providers. Interested Service Providers are advised to regularly refer to the NeGD website for any updates.

3. Request for extension of date for submission of Request for Onboarding applications, in round 1, will not be entertained. However, to give prospective Service Providers reasonable time to consider the amendment in preparing their Request for Onboarding applications, NeGD may extend the last date for receipt of Request for Onboarding applications. No Request for Onboarding applications may be changed after submission.

4. Service Providers are advised to study the Guideline Document carefully. Submission of the Request for Onboarding will be deemed to have been done after careful study and examination of all instructions, eligibility norms, terms, and requirement specifications in the Guideline document with a full understanding of its implications. Any Requests for Onboarding not complying with all the given clauses in this Guideline Document are liable to be rejected. Failure to furnish all information required in this Guideline Document or submission of a Request for Onboarding not responsive to this Guideline document in all respects will be at the Service Provider's risk and may result in the rejection of the Request for Onboarding.

5. Request for Onboarding as per the format provided in Annexure-II and details as per the format provided in Annexure-III and Annexure-IV should be submitted along with documentary proofs.

6. Suppose the space in the Proforma is insufficient to furnish the full details. In that case, the information shall be supplemented on separate sheets of paper stating therein the part of the statement and serial number. Separate sheets may be used for each part. Any interlineation, erasures, or overwriting shall be valid only if the person(s) signing the Request for Onboarding initial(s) them.

7. **Submission of Request for Onboarding:** The request for onboarding shall remain open until further notice by MeitY, and shall be evaluated on an ongoing basis, as and when they are received. However, we have set a date for publishing Round 1 of Onboarded API Service Providers. Detailed Request for Onboarding must be submitted as per the schedule given on the portal on or before 30th May,2025, at 15:00 Hrs.

8. NeGD may ask Service Providers for clarifications or additional documents/ credentials at its discretion.

(This Space Intentionally Left Blank)

SECTION IX – EVALUATION OF REQUEST FOR ONBOARDING

1. The Request for Onboarding will be examined by NeGD to determine if they meet the Eligibility Criterion, Terms and Conditions mentioned in this document, including its subsequent amendment(s), if any, and whether the Request for Onboarding is complete in all respects.

2. If deemed necessary, NeGD may seek clarifications on any aspect of the Request for Onboarding from the applicant. If a written response is requested, it must be provided within 3 days. Response received beyond 3 days, if any, may not be considered. However, that would not entitle the applicant to change or cause any change in the substances of their Request for Onboarding document already submitted. NeGD will also make inquiries to establish the applicants' past performance regarding similar work. All information submitted in the application or obtained subsequently will be treated as confidential.

3. Submission of an application does not guarantee publishing; only relevant APIs will be published.

4. API to be onboarded should conform to open web specifications 3.0 standards. API should be provided in YAML format.

TERMS & CONDITIONS

1. Submission of Request for Onboarding is evidence of a Service Provider's consent to comply with the terms and conditions of the Request for Onboarding process and subsequent process. If a Service Provider fails to comply with the terms, its request may be summarily rejected.
2. The willful misrepresentation of any fact in the Request for Onboarding will lead to the disqualification of the Service Provider without prejudice to other actions that NeGD may take. The Request for Onboarding and the enclosed documents will become the property of NeGD.
3. NeGD reserves the right to accept or reject any or all applications received in line with the Guideline document without assigning any reason whatsoever and NeGD's decision in this regard will be final.
4. NeGD may inspect the facilities of the Service Provider at any time during the evaluation stage to verify the genuineness and to ensure conformity with the proposal submitted.
5. The Service Provider must submit its complete profile, giving details about the organization, experience, technical personnel in the organization, competence, and adequate evidence of its financial standing. etc., in the enclosed form, which will be kept confidential.
6. No contractual obligation whatsoever shall arise from the Onboarding process under this Guideline document.
7. Any effort on the part of the Service Provider to influence the evaluation process may result in the rejection of the Request for Onboarding.
8. The selected firms/service providers shall be required to sign a Non-Disclosure Agreement cum Undertaking with NeGD that they shall not disclose any information related to Development/Audit/testing/Security breach with any third person. Confidentiality shall prevail even after the end of the empanelment.
9. NeGD reserves the right to contact the reference clients to ascertain the submission made by the Service Providers during the evaluation process.
10. NeGD reserves the right to verify the validity of the information provided in the Request for Onboarding and to reject any request whose contents appear to be incorrect, inaccurate, or inappropriate at any time during the process of the Request for Onboarding.
11. During the onboarding process, the Service Provider shall indemnify NeGD against direct losses arising from:
    a) Misrepresentations or false information in the onboarding application;
    b) Unauthorized use of third-party intellectual property in demonstrations or testing;
    c) Data breaches or security incidents caused by the Provider's negligence during sandbox testing or API submission.
    Such indemnity shall be governed by applicable laws, including the Digital Personal Data Protection Act, 2023, and the Information Technology Act, 2000. Upon successful onboarding, the SLA/DPA will include comprehensive indemnity obligations.

12. Service Providers shall be deemed to have:
    a. Examined the Guidelines for Onboarding document and its subsequent changes, if any, to respond to it.
    b. Examined all circumstances and contingencies affecting their Request for Onboarding application, which is obtainable by making reasonable enquiries.
    c. Satisfied themselves as to the correctness and sufficiency of their Request for Onboarding applications. If any discrepancy, error, or omission is noticed in the Request for Onboarding, the Service Provider shall notify NeGD in writing as soon as such discrepancy, error or omission is discovered.
13. The Service Provider shall bear all costs associated with submitting the Request for Onboarding and demonstration/ POC desired by NeGD. NeGD will not be responsible or liable for any cost thereof, regardless of the conduct or outcome of the process.
14. Service Providers must advise NeGD immediately in writing of any material change to the information contained in the Request for Onboarding application, including any substantial change in their ownership or financial or technical capacity. Copies of relevant documents must be submitted with their advice.
15. Shortlisted Service Providers must not advertise/ publicise in any form (without prior written permission from NeGD) about their unit having been shortlisted by NeGD.
16. The Service Provider should be agreeable to provide:
    - Competent Manpower
    - Pass through the technical testing to be conducted as part of the onboarding process; against criterion mentioned in Annexure VII.
17. The Intellectual Property Rights on the developed software code (if any) and related documentation shall vest with NeGD. Providers shall not use such IP for competing platforms without NeGD's written consent
18. The application development/ customisation work carried out by the empanelled Service Provider(s) will be subject to unit testing, stress/performance testing, system integration testing & user acceptance testing, etc. and security audit as applicable. However, no additional fees/charges would be payable by NeGD for the rectification of errors detected during such testing/audit process.
19. The Service Provider should agree to provide NeGD with all necessary functional and technical documentation as required by NeGD from time to time.
20. The Service Provider is in agreement with NeGD to execute the contract, Non-Disclosure Agreement (NDA) and Integrity Pact as per the format of NeGD. The contract format along with NDA and integrity pact will be shared with eligible Service Providers.
21. NeGD may re-visit any of the conditions of this Guideline for Onboarding.

22. **Conflict of Interest**: An *Applicant* shall furnish an affirmative statement as to the existence of, absence of, or potential for conflict of interest on the part of the Applicant due to prior, current, or proposed contracts, engagements, or affiliations with this Ministry. Additionally, such disclosure shall address any and all potential elements (time frame for service delivery, resource, financial, or other) that would adversely impact the ability of the Applicant to complete the requirements for the concerned work.

23. The Applicant should not be involved in any way on those work assignments where there is any scope of conflict of business interest.

24. Wherever there is any scope of conflict of business interest, the Applicant has to choose only one role that is either to take the assignment as a part of empanelment or to opt for other business opportunities

25. NeGD shall have the right to change the Terms & Conditions/ cancel the Request for Onboarding process at any time, without thereby incurring any liabilities to the affected Service Providers. Reasons for changing the terms & conditions/cancellation, as determined by NeGD in its sole discretion, include but are not limited to the following:

a. Services contemplated are no longer required

b. Scope of work not adequately or clearly defined due to unforeseen circumstances and/or factors and/or new developments.

c. The project is not in the best interest of NeGD

d. Any other reason

26. "Any dispute arising out of or in connection with this agreement shall be resolved by arbitration in accordance with the Arbitration and Conciliation Act, 1996. The seat of arbitration shall be New Delhi. The language of proceedings shall be English. The dispute shall be resolved by a Sole Arbitrator, which shall be jointly appointed by the parties. In the event of failure of the parties on coming to a consensus to appoint an Arbitrator, the Tribunal shall be constituted in terms of the provisions of the Arbitration and Conciliation Act, 1996 (as amended from time to time).

Annexure I –Eligibility Criteria

"**Request for Onboarding of Application Programming Interface (API) service providers for API Setu"** NeGD will scrutinize the requests received to determine whether they are complete and comply with the request for onboarding requirements. The requests that meet the criteria will proceed to the next stage of evaluation, namely, technical evaluation. If the documents align with the specified format, the service provider will qualify for technical evaluation. All supporting documents and documentary evidence must be attached according to the specifications.

(This Space Intentionally Left Blank)

S. No.	Eligibility Criteria	Compliance (Yes/No)	Service Provider's Response	Attachment Tag / Page No.
	The Service Provider must be an Indian Company/ LLP /Partnership Firm registered under the applicable Act in India and should have been in existence continuously for at least the last 3 completed fiscal years as of the last date of submission of the response to the Request for Onboarding. Registered with the Income Tax Authorities. Registered with the GST Authorities.			
	The Service Provider must have an average turnover of a minimum of Rs. 10 crores during the last 03 (three) fiscal year(s), i.e., FY 2021-22, FY2022-23 and FY 2023-24. This must be the individual company's average turnover and not that of any group of companies. MSME agencies registered with the Government are exempted from turnover criteria.			
	The Service Provider should be a profitable organization based on profit before tax (PBT) for last 03 (three) fiscal years mentioned			
	Past/ present litigations, disputes, if any (Adverse litigations could result in disqualification, at the sole discretion of the NeGD)			
	The Service Provider (including its OEM, if any) must comply with the requirements contained in OM No.F.7/10/2021-PPD (Order Public Procurement No. 4)			

	The Service Provider should have experience of minimum 3 years in providing solution / services which includes installation, development, implementation, and operation/ maintenance of API technologies, including RESTful APIs and API management platforms, for a period of at least the last three completed financial years as of the last date of submitting a response to the Request for Onboarding.			
	Undertaking by the authorized signatory of the Service Provider that the Service Provider or any of the associated Directors is currently not blacklisted by any Government Organizations, Public Sector Undertakings, or Public Limited Companies and is not under a declaration of In-eligibility for corrupt or fraudulent practices as on the date of submission of requests.			

Annexure-II – Request for Onboarding

Request Submission Form

(To be submitted on the letterhead of the Agency(s))

Date:

To,…….,

NeGD

Electronics Niketan Annex,

6 CGO Complex,

New Delhi-110003

Dear Sir,

Subject: Submission of the Request for Onboarding for "**Request for Onboarding of Application Programming Interface (API) service providers for API Setu"**

We, the undersigned, offer to provide services in accordance with your Guidelines for Onboarding for "**Application Programming Interface (API) service providers for API Setu"** dated_____. We are hereby submitting our Request for an Onboarding application.

We hereby declare that all the information and statements made in this Request for Onboarding are true and accept that any misinterpretation contained in it may lead to our disqualification.

We agree to abide by all the terms and conditions of the Request for Onboarding application document. We understand NeGD is not bound to accept any proposal you receive.

Yours sincerely,

Signature [In full and initials]:

Name and Title of Signatory:

Name of Service Provider:

Address:

Location:

Annexure III – Service Provider's Information Details:

Sr. No.	Items	Service Provider's Response
1	**Basic Information**	
	a)Name of the organization Name of the contact person	
	b) Registered office Address	
	c) Phone no. of the contact person	
	d) Email address of the contact person	
	e) Web site if any, of the organization	
	f) Year of commencement of business	
	g) PAN no.	
	h) Service tax registration No. / GST No.	
2	Location of competency center and number of professionals	
3	No. of certified professionals with mandatory skills.	
4	Average relevant experience of Project Managers handled similar projects	
5	Average relevant experience of software engineers implemented similar projects	
6	Net profits during past three fiscal years	
	Net Profit (In Rupee Crores):	
	For 2023-24	
	For 2022-23	
	For 2021-22	
10	Annual turnover of the Service Provider (in Rupee Crores) in each of the last three fiscal years	
	For 2023-24	
	For 2022-23	
	For 2021-22	

Authorized Signatory:

Name of the authorized signatory: OBJ

Date:

Place: Seal:

Annexure-IV- Format for submission of previous projects undertaken

Details of the project undertaken in India or internationally (Attach Copy of Purchase orders/ any documentary evidence) (One sheet for each Project should be submitted)

Project no. 1 ….

Sr. No	Items	Mandatory (Y/N)	Service Provider's Response
1	Client name	Y	
2	Location of the client along with contact person, contact no and email id	Y	
3	Date of Purchase Order received for the project Date of Commencement of contract: Date of Implementation of the project: Status of the Project (whether Implementation /Maintenance etc.):	Y	
4	Nature of project for the Clients (Please list the activities handled by the Service Provider)	Y	
5	Scope of Work	Y	
6	Team Size	Y	
7	Name of the Project Head	Y	
8	Name of the Technical Architect/Designer/Developer	Y	
9	Software Tools & Technology used	Y	
10	Total Efforts in Man months	Y	
11	Contract Amount (in Rupees crores)	Y	
12	Any other relevant information, including the reason for the delay, if any	N	

Note: The Service Provider should only provide the above information in this format.

Authorized Signatory:

Name of the Authorized Signatory: Date:

Place: Seal

(Service Providers are required to furnish details for each project they have undertaken as per the eligibility criteria)

Annexure V- Undertaking: Non-Blacklisting

To

Date

NeGD

Ministry of Electronics & Information Technology,

Electronics Niketan Annex.,

6 CGO Complex, Lodhi Road

New Delhi – 110003

Subject:Request for Onboarding of Application Programming Interface (API) Service Providers for API Setu

Dear Sir/Madam,

In response to the Request for Onboarding document subjected above, I/ We hereby declare that presently, our Company/ firm _____ has an unblemished record and is not declared ineligible for corrupt & fraudulent practices either indefinitely or for a particular period of time by any State/ Central Government/ PSU/Autonomous Body.

We further declare that presently our Company/ firm _____ is not blacklisted/debarred and not declared ineligible for reasons other than corrupt & fraudulent practices by any State/ Central Government/ PSU/ Autonomous Body on the date of Application Submission. If this declaration is found to be incorrect, then without prejudice to any other action that may be taken, my/our security may be forfeited in full, and the tender, if any, to the extent accepted, may be canceled.

Thanking you,

Yours faithfully,

Name

Signature

Seal of the organization

Date_____ Place _____

Annexure VI - API Onboarding Criterion

1. Security & Compliance Criterion

a. Authentication & Authorization

i. Requirement: The API must support OAuth2, JWT, or equivalent token-based authentication.

ii. Threshold:

1. Must have role-based access control (RBAC) and consent-based data access, as applicable.
2. Tokens must have a maximum lifespan of **60 minutes** and support refresh tokens.
3. Multi-factor authentication (MFA) is mandatory for administrative access.
4. The API Provider should facilitate a Consent Artefact Management Process as and when applicable.

b. Data Encryption & Protection

i. Requirement: Should support secure data transfer and protection of sensitive information.

ii. Threshold:

1. TLS 1.3 must be used for all API communication i.e., data in transit.
2. End-to-end encryption for sensitive data at rest using AES-256.
3. Sensitive data (like passwords, PII) must be encrypted before transmission.
4. Ensure **data masking** for PAN, Aadhaar, and other PII.

c. Security Testing & Vulnerability Assessment

i. Requirement: The API provider should Proactively identify and mitigate security risks.

ii. Threshold:

1. Must pass **Vulnerability Assessment & Penetration Testing (VAPT)** with no “high” or “critical” vulnerabilities.
2. No open vulnerabilities from the **OWASP API Security Top 10**.
3. Secure against business logic abuse, injection flaws, and excessive data exposure.

d. **Incident Response & Data Breach Protocol**

i. **Requirement: The API Provider should** have a robust incident response plan.

ii. Threshold:

1. A documented **Incident Response Plan (IRP)** is required.
2. Providers must notify affected parties, applicable regulators and Cert-In of a data breach within **6 hours.**

e. **Compliance with Legal and Regulatory Standards**

i. **Requirement: Should a**dhere to local and global compliance standards.

ii. Threshold:

1. Comply with the Digital Personal **Data Protection Act 2023 (India)** and IT Act 2000 and its amendments.
2. Must provide evidence of adherence to data protection, privacy, and localization laws.

2. Performance and Reliability Criteria

a. Uptime

i. Requirement: Provide continuous API availability and implement /Heartbeat monitoring.

ii. Threshold:

1. **Minimum 99.9% uptime** (measured over a 30-day rolling window).
2. Scheduled downtime must be pre-notified at least **48 hours** in advance.
3. No single unplanned outage lasting more than **1 hour.**
4. GET /Heartbeat should return 200 OK.

b. **Response Time / Latency**

i. Requirement**:** Provide fast response times to API calls.

ii. Threshold:

1. Average response time (P95) must be **under 200ms**.
2. The maximum response time (P99) must not exceed **500ms**.
3. For critical APIs (e.g., payments), P95 must be **under 100ms**.

c. Error Rate

i. Requirement: Reduce API failures and errors.

ii. Threshold:

1. 4xx and 5xx errors should not exceed **1%** of total requests.
2. Daily spike in error rate should not exceed **5%**.
3. Consistent error rates above **1% for 3 consecutive days** will result in listing failure.

d. Rate Limiting, Quotas and Throttling

i. Requirement: Prevent API overuse and ensure fair access.

ii. Threshold:

1. Must support **rate limiting** to prevent abuse (configurable at user and IP level).
2. Quotas must be configurable for specific customers or user groups.
3. Must support **graceful rejection** (e.g., HTTP 429: Too Many Requests) instead of API breakdown.

e. Scalability & Peak Lead Handling

i. Requirement: Handle traffic spikes efficiently.

ii. Threshold:

1. Must support **horizontal scaling** to handle peak loads.
2. Must handle at least **2000 requests per second (RPS) steady load and 5000 RPS burst traffic,** as defined in the SLA.
3. Must undergo load testing with **50% higher RPS than SLA** to ensure scalability.

3. Technical Quality and Functional Criteria

a. Functional Completeness

i. Requirement: Ensure that all declared API functionality is working as described.

ii. Threshold:

1. 100% of documented API endpoints must be functional at launch.
2. All endpoints must return expected **HTTP response codes**.
3. Endpoints must fail gracefully and return proper error messages (e.g., 400 Bad Request).

b. Backward Compatibility

i. Requirement: Avoid breaking changes.

ii. Threshold:

1. API updates must not introduce **breaking changes**.
2. If breaking changes are unavoidable, providers must issue a **deprecation notice at least 90 days in advance**.
3. Always maintain at least two active versions (latest and previous).

c. Input Validation and Error Handling

i. Requirement: Validate user input and handle errors gracefully.

ii. Threshold:

1. Input validation must prevent SQL Injection, XSS, and parameter tampering.
2. Descriptive error messages (without exposing internal logic) must be returned for all error states.
3. Error codes should conform to HTTP status codes (e.g., 200, 400, 401, 403, 500).

d. Code Quality

i. Requirement: API Provider should maintain high-quality code.

ii. Threshold:

1. Code must be peer-reviewed, and **static analysis tools** must be used.
2. Follow industry-standard secure coding guidelines (e.g., OWASP).

e. Audit Trail

i. Requirement: Maintain 180-day log retention of API calls

ii. Threshold:

1. Log all activities related to API calls that are considered critical for the Business Purpose.
2. 180-day log retention

4. Documentation, Usage, and Support Criteria

a. API Documentation

i. Requirement: The API Provider should publish clear, versioned, and accessible API documentation.

ii. Threshold:

1. Must use **OpenAPI 3.0 specification** for API definitions.
2. API documentation must be clear, concise, and include request/response samples.
3. An **API changelog** must be included for every version update.
4. **Semantic Versioning (X.Y.Z)** in API URLs and response bodies.

b. Developer Support and Onboarding

i. Requirement: Provide timely support and onboarding for developers.

ii. Threshold:

1. Provide **developer support channels** (chat, email, or forums) with a response time of **24 hours or less**.
2. Publish a **sandbox environment** for testing API calls.
3. Must provide SDKs for popular programming languages (Python, Java, Node.js).

c. Pricing and Usage Transparency

i. Requirement: Ensure clear pricing and usage tracking.

ii. Threshold:

1. API providers must clearly specify **free-tier limits, basis of billing** (e.g., fixed fees, per-call fees, and tiered usage fees)and **pricing (in INR) for paid plans**.
2. Providers must enable real-time usage tracking for API consumers.
3. Must provide **usage analytics and billing breakdown**.

The Service Provider should consider the variation of the number of API's and processes to an extent of 20 to 30 % due to the dynamic addition of new requirements in API platform.

Demo / Presentation	
<u>Technical Presentation /Demo</u> The Service Provider should make a demo / technical presentation on the proposed solution in line with the scope of work.	Demo and/or Technical Presentation on as per Scope of work Presentation may be evaluated on the following factors: Scope coverage as per features described in RFP. Proposed workflow design for end user registration and infrastructure allocation Ease-of-use Any other essential parameters <u>Documentary proof -</u> The presentation needs to be submitted to NeGD.

Annexure VII- API Performance

API Performance Evaluation Criterion for Continuance of Onboarding

This framework defines the Key Performance Indicators (KPIs) and evaluation criteria that API providers must adhere to maintain their listing on the API marketplace. The evaluation will be conducted on a **rolling basis (90-day windows)**, ensuring continuous compliance, security, performance, and functional quality. Providers will be assigned a **Performance Score** out of 100. Failure to maintain a **minimum score of 85** will result in **probation**, and consistent non-compliance may lead to **delisting**.

A rolling KPI evaluation mechanism ensures consistent, data-driven performance tracking. API Providers who consistently maintain their scores are rewarded with enhanced visibility, while those who fail face delisting.

This framework ensures only the most reliable and secure APIs remain empaneled.

Each KPI has an assigned weight. API Providers are scored on each KPI according to this formula:

(Actual Performance / Minimum Threshold) * Weight = KPI Score

The total score for the API is calculated as:

- **Total Score = Sum of (All KPI Scores) / 100**
- **Minimum Score**: 85/100.
- **Thresholds for Escalation**:
- **80-85**: Probation for 30 days.
- **Below 80**: Immediate delisting.

Key Performance Indicators:

1. Security & Compliance (Weight: 30/100)

KPI	Description	Weight	Minimum Threshold
Authentication & Access	RBAC, Consent-Driven Access	10	No unauthorized access
Data Encryption	TLS 1.3 for transit, AES-256 for data at rest	5	100% compliance
Security Testing	Monthly VAPT, No OWASP API Top 10 vulnerabilities	5	No "High" or "Critical" vulnerabilities
Breach Management	Timely incident reporting to CERT-In, RBI	5	Report within 6 hours
Compliance Adherence	IT Act, 2000, Data Protection (DPDP, GDPR), Adherence to ReBIT (as applicable).	5	Full legal compliance

2. Performance & Availability (Weight 25/100)

KPI	Description	Weight	Minimum Threshold
Uptime (Availability)	30-day uptime percentage	10	99.9%
Response Time (Latency)	P95 < 200ms, P99 < 500ms for /FI/fetch, /Consent	5	P95 < 200ms, P99 < 500ms
Error Rate	4xx & 5xx errors per total requests	5	<1%
Load Handling	Handles 2000 RPS steady, 5000 RPS burst	5	Full load compliance

3. Functional & Technical Quality (Weight 20/100)

KPI	Description	Weight	Minimum Threshold
API Completeness	All declared endpoints functional	10	100% completeness
Backward Compatibility	No breaking changes, versioning compliance	5	Support 2 versions
Input Validation	SQL Injection, XSS, Parameter Tampering checks	5	No injection flaws

4. Usage, Support & Transparency (15/100)

KPI	Description	Weight	Minimum Threshold
API Documentation	OpenAPI 3.0 definitions, API changelog	5	Clear documentation
Developer Support	24-hour response time for support tickets	5	24-hour response time
Billing & Usage Transparency	Accurate usage tracking, clear pricing	5	Full transparency

5. Audit & Logging (Weight 10/100)

KPI	Description	Weight	Minimum Threshold
Audit Trail Completeness	Audit trail for /Consent, /FI/request, /FI/fetch	5	90-day log retention
Tamper-Proof Logging	Verify tamper-proof nature of logs	5	No log tampering

Annexure- VIII-Business Purposes for API as a Service

The following is a comprehensive superset of business purposes and application areas for which empanelled API service providers may offer their services. These purposes are aligned with the national objectives of building a secure, interoperable, and inclusive digital public infrastructure. The categories reflect various use cases across G2C, G2B, and G2G ecosystems.

This set of purposes provides the foundation for the strategic onboarding and evaluation of API service providers and will evolve in line with emerging national digital infrastructure programs.

A. Identity & Verification

- PAN verification for financial compliance and tax-related services
- Voter ID, Driving License, Passport verification for unified digital identity

B. Financial & Taxation Services

- GST verification and filing
- Income tax return validation and PAN-TAN reconciliation
- TDS record verification for compliance automation
- MCA21-based company and director verification
- Integration with PFMS for public fund tracking and subsidy disbursement
- Government e-Marketplace (GeM) APIs for procurement, seller verification, and bidding

C. Payments & Banking

- UPI-based transaction authentication and payment gateway integration
- Bharat Bill Payment System (BBPS) for utilities and municipal collections
- FASTag payments and tracking for mobility solutions
- e-RUPI-based voucher disbursement for targeted schemes
- Jan Dhan account status verification for inclusion programs

D. Logistics & Trade

- ULIP-based multimodal logistics data for supply chain visibility
- e-Way Bill data for goods movement and taxation
- ICEGATE APIs for customs clearance and trade compliance
- Port Community System integration for maritime operations
- eNAM APIs for digital Agri-marketplace and farmer-to-mandi trade

E. Insurance & Financial Data Sharing

- Account Aggregator APIs for consent-based financial data sharing
- Vehicle insurance verification for traffic police, RTO, and insurers

- National Insurance Repository APIs for policy status and claims data

F. Cybersecurity & Compliance

- CERT-In threat advisories and incident feeds
- eSign APIs for Aadhaar-based or DSC-based digital signature
- API telemetry for access logs, usage alerts, and fraud detection
- Threat Intel

G. Law & Governance

- e-Courts APIs for judicial record validation
- Land records verification for property title validation
- NVSP APIs for electoral roll validation

H. Health & Social Welfare

- CoWIN vaccination record verification and scheduling
- Ayushman Bharat health record integration and hospital empanelment
- e-Hospital APIs for government healthcare systems
- Ration Card and NFSA integration for subsidy management

I. Education & Skill Development

- DigiLocker for education certificate verification
- SWAYAM and NSP scholarship APIs for access to skilling and education programs
- AICTE/UGC data for accreditation checks and institution validation

J. Open Data & Emerging Technology

- Access to OGD datasets via API for analytics and research
- ONDC APIs for enabling digital commerce interoperability
- Geospatial APIs for land mapping, planning, and public works
- Weather data APIs for disaster management and agriculture
- EV Charging APIs for mobility, planning, and smart infrastructure