



API Setu

Standard Operating Procedure (SOP) for consuming API through API Setu

Version 02/2024

API Setu, is an Open API (Application Programming Interface) Platform from Ministry of Electronics and IT, Government of India.

Background

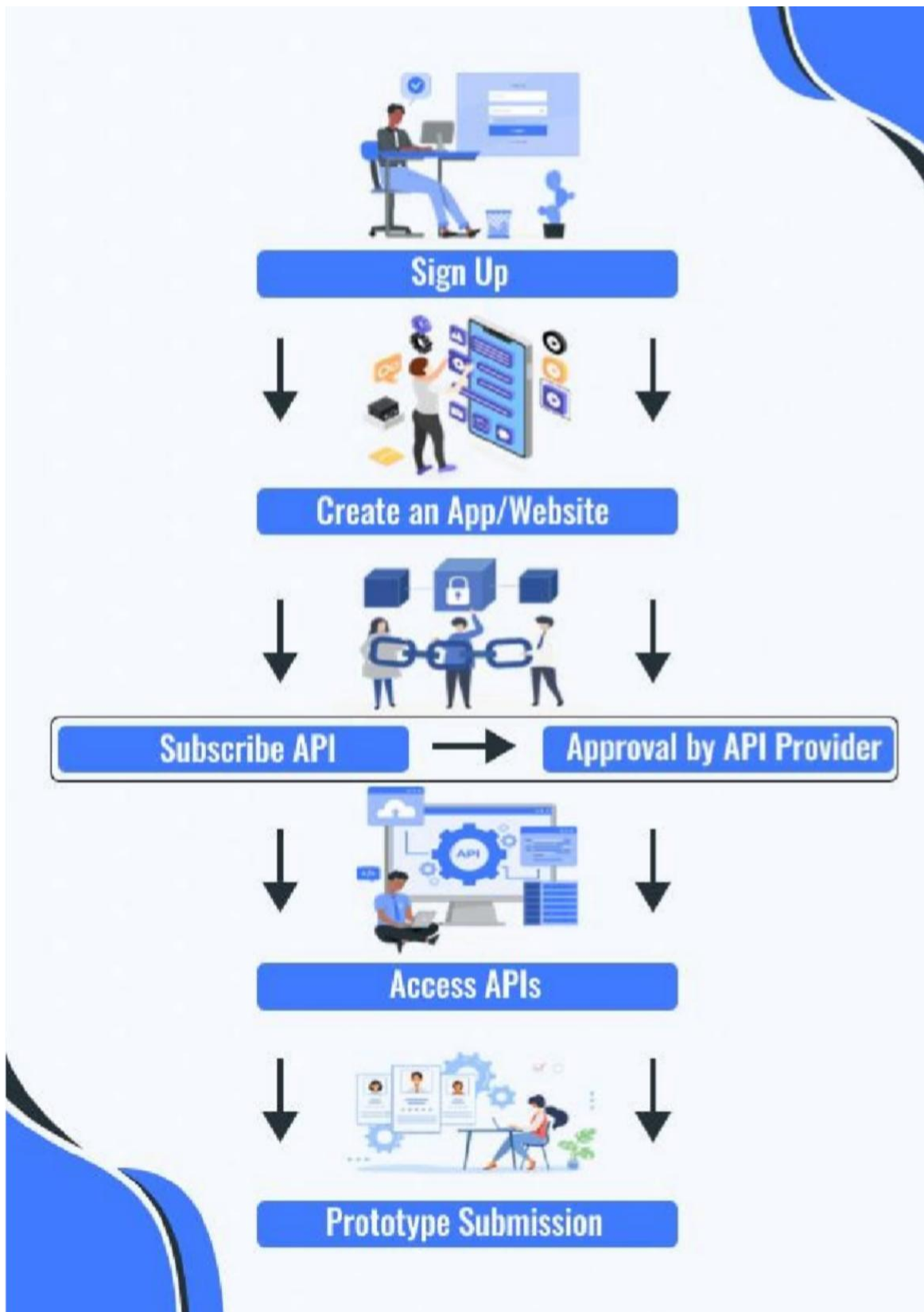
An 'Open API' policy was notified by Ministry of Electronics and IT (MeitY) in July 2015 with an objective to develop an open and interoperable platform to enable seamless service delivery across government, thereby providing access to data S services and promoting citizen participation for the benefit of the community. It was felt that to provide impetus to the policy implementation an API platform to act as an API Marketplace cum Directory Portal is necessary. Hence, MeitY has initiated the project 'API Setu' in March 2020. This platform aims to bring the Open API policy into realization.

How To Get Started

API Setu offers a collection of APIs that allows organizations/ departments to integrate with APIs and develop various applications.

Follow the steps below to get started

- a) To access the APIs through the API Gateway, developers must first request access by contacting the API Gateway team or the designated API Manager. The sign up may be made using the link <https://partners.apisetu.gov.in/signup> and a valid use case should be provided. During the sign up please provide Proof of Identity , Authority Letter, Organization PAN, GST registration certificate and Certificate of Incorporation. The request should be made through domain registered email id only. And Only one request will be entertained from one organization.
- b) The API Management team will evaluate the request and the use case and approve the sign up request.
- c) API consumer shall subscribe to the APIs that are of interest as per the use case and approve necessary approval from the API provider. API Setu team will facilitate in API subscription. Once the approval is granted from the API provider, the API Setu team will provide the necessary documentation, credentials, and permissions to access the required APIs.
- d) Each developer will receive a unique API key or access token, which should be securely stored and not shared with others.



Standard Operating Procedures for accessing APIs on API Setu

Purpose:

The purpose of this Standard Operating Procedure (SOP) is to establish guidelines and best practices for using APIs (Application Programming Interfaces) through our API Gateway “API Setu”. This document aims to ensure secure, consistent, and efficient interactions with APIs, promoting better integration and data exchange between systems while maintaining high standards of security and performance.

Scope:

This SOP applies to all developers, engineers, and stakeholders who interact with APIs hosted on our API Gateway within your department/organization. It covers the process of registering, obtaining credentials, and making API requests using the API Gateway.

API Usage Guidelines:

- a. **API Endpoint URLs:** Developers should use the API endpoint URLs provided in the documentation. These URLs may vary based on the API version and resource being accessed.
- b. **HTTPS Methods:** Developers must use the appropriate HTTP methods (GET, POST, PUT, DELETE, etc.) as specified in the API documentation. Using the correct method ensures data integrity and prevents unintended changes.
- c. **Request and Response Format:** Developers should adhere to the defined request and response formats as specified in the API documentation. Use standard data formats like JSON or XML for data exchange.
- d. **Error Handling:** Developers should implement robust error handling mechanisms and provide meaningful error messages in responses. Error codes and messages should be documented and consistently used across APIs.
- e. **Rate Limiting:** Respect any rate limits set by the API Gateway to prevent abuse and ensure fair usage. Exceeding the rate limits may result in temporary or permanent suspension of API access.
- f. **Security:** All API requests must be made over HTTPS to ensure data confidentiality. Sensitive information should not be exposed as query parameters, and authentication should be done using the provided API keys or tokens.

Consent Management

It is the prime responsibility of the API Consumer to develop a consent capture mechanism to capture the consent from the citizen. This should be either physical or electronic. All data

must be exchanged between the provider and the consumer in a secure fashion using either data and/or channel encryption.

Purpose of data access: This may include information about the application domain and the application within that domain that is enabled through the data access and a free-form textual description.

Logging of consent and data flows: The consent artifact includes identifiers for entities which collect and store logs. Logging could be done by the consent collector or by other entities e.g., logs could be sent to the users' own email addresses, if the user desires so. Data providers and data consumers could also independently maintain logs for auditing and analytics purposes.

Monitoring and Reporting:

- a) The API Gateway team will monitor API usage, performance, and security to ensure smooth operation and compliance with the defined standards.
- b) Any anomalies or security incidents should be reported to the API Setu team immediately.

Compliance and Violations:

- a) Non-compliance with this SOP may result in the suspension or revocation of API access privileges.
- b) Developers should report any suspected API abuse or security vulnerabilities to the API Setu team or the designated security contact with a subject line as 'API abuse or security vulnerabilities'.

Review and Updates:

This SOP will be periodically reviewed and updated by the API Gateway team to accommodate changes in technology, security best practices, and business requirements.

If you have any questions or need further clarification, please feel free to reach out to the API Setu team.

Contact us

<https://apisetu.gov.in>

email: apisetu.support@digitalindia.gov.in, nirmit.mehrotra@digitalindia.gov.in