

# **API Manager APIMBBONE**

## **Manuale per Sottoscrizione API**

| <b>VERSIONE</b> | <b>PARAGRAFO O<br/>PAGINA</b>     | <b>DESCRIZIONE DELLA VARIAZIONE</b>            |
|-----------------|-----------------------------------|--|
| V01             | Tutto il documento                | Versione iniziale del documento                |
| V2.0.0          | Tutto il documento                | Revisione per upgrade a WSO2 API Manager 4.1.0 |
| V2.0.1          | Capitolo 3.1                      | Modificate le indicazioni per apertura ticket  |
| V2.0.2          | Paragrafo 3, 3.2, 3.3, 3.4, 3.4.1 | Aggiunto ambiente di test                      |
| V2.0.3          | Paragrafo 3.3                     | Dettagliato iter di sottoscrizione             |
| V2.0.4          | Paragrafo 3.4.1                   | Indicazione di utilizzo protocollo http/https  |

**1 Sommario**

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>API Management .....</b>                                | <b>3</b> |
| <b>2</b> | <b>Gestione della sicurezza .....</b>                      | <b>4</b> |
| <b>3</b> | <b>Fruizione di API esposte su API Manager .....</b>       | <b>4</b> |
| 3.1      | Accreditamento allo Store .....                            | 5        |
| 3.2      | Creazione dell'applicazione fruitrice delle API .....      | 6        |
| 3.3      | Sottoscrizione dell'API di interesse .....                 | 7        |
| 3.4      | Generazione e utilizzo delle chiavi di accesso .....       | 11       |
| 3.4.1    | Generazione Token .....                                    | 13       |
| 3.4.2    | Esempio di chiamata cURL alla token API:.....              | 14       |
| 3.4.3    | Esempio di codice java per ottenere l'access token .....   | 14       |
| 3.4.4    | Esempio di codice phyton per ottenere l'access token ..... | 16       |
| 3.5      | Invocare un API .....                                      | 16       |

## 1 API Management

Le soluzioni di API Management costituiscono l'elemento abilitante per arricchire e personalizzare l'interazione tra le applicazioni che richiedono l'accesso ad API e i servizi di business che espongono le informazioni utili per la composizione delle applicazioni stesse. L'introduzione di un layer di astrazione tra i servizi che espongono funzionalità (API Providers) e le applicazioni che li consumano (API Consumers) semplificano gli sviluppi e favoriscono il disaccoppiamento tra i due livelli.

L'API Manager è la soluzione che permette di centralizzare il punto di ingresso per le chiamate, applicare politiche di throttling efficienti, monitorare le risorse utilizzate, tracciare le chiamate dei fruitori delle API di business ed ultimo ma non meno importante securizzare i servizi API.

Gli obiettivi principali dell'API Manager possono essere riassunti come segue:

- **Gestione della sicurezza:** garantisce l'accesso soltanto agli utenti/sistemi autorizzati ed evita l'uso improprio delle risorse protette. Sono disponibili diversi framework di sicurezza, lo scenario attuale implementato prevede l'adozione di OAuth2
- **Gestione del traffico:** performance gestite in maniera puntuale e dinamica per ciascuna API con limitazione del traffico in ingresso (rate limiting), applicazione di politiche di accesso diversificate in base sistema chiamante (throttling), routing e cache dei messaggi. Filtraggio del traffico in ottica di identificazione e neutralizzazione di minacce
- **Gestione del ciclo di vita delle API:** fasi di sviluppo, test, produzione e dismissione, nonché versionamento. Questa funzionalità garantisce la coerenza di differenti versioni dell'API consentendo il suo utilizzo da parte di diverse tipologie di utenti, in ambienti diversi e con diversi gradi di maturità
- **Audit del sistema:** tracciamento attività e statistiche di utilizzo.

Le componenti principali dell'API Manager sono le seguenti:

- **API Store**, Store dedicato agli sviluppatori e alle terze parti che intendono integrare le API nelle loro applicazioni, il portale ospita la documentazione di supporto, monitorare l'utilizzo delle API nonché accedere ad altri strumenti di comunicazione e condivisione.
- **Publisher**, applicazione web che permette agli API Providers di creare e pubblicare le API. Nel Publisher si definiscono tutti gli aspetti di configurazione dell'API, compresi endpoint dei servizi di back-end e politiche di throttling e rate limiting.
- **API Gateway**, componente di runtime dell'API Manager che ha come finalità essenziale di esporre i servizi messi a disposizione dall'intero sistema in maniera sicura, facilmente fruibile e controllata. L'API Gateway, dal punto di vista architetturale, è un proxy dei servizi esposti dai sistemi di back-end, in modo tale che tutti i sistemi fruitori debbano effettuare l'accesso a servizi e risorse attraverso questo componente. Dal punto di vista funzionale, il Gateway, riceve le richieste per accedere alle API ed attua le politiche di controllo di accessi, applica le regole di rate limiting e throttling e instrada le richieste verso i sistemi di back-end.
- **Key Manager**, componente che ha il compito di gestire tutte le questioni relative alla sicurezza e alle chiavi. Tutte le richieste di generazione di nuovi access token sono gestite da questo componente che effettua la validazione di tutti i parametri inviati nella richiesta (client\_id, client\_secret, username, password, ecc...).

- **Traffic Manager**, componente che si occupa di regolare il traffico di ciascuna API secondo le politiche che sono state definite in fase di definizione dell'API e in fase di sottoscrizione alla stessa. Il motore di elaborazione del Traffic Manager elabora le politiche di throttling in real time, incluse le politiche di rate limiting delle chiamate alle API.

## 2 Gestione della sicurezza

Open Authorization 2 (OAuth2) è lo standard de facto supportato dall'API Manager per l'autorizzazione a risorse (API) protette da autenticazione senza necessità di dover condividere pubblicamente tali credenziali. Il protocollo OAuth permette di autorizzare una terza parte a gestire sezioni riservate di una risorsa senza vincolare il sistema a mettere in circolazione le credenziali per accedervi. I vantaggi offerti da questa tecnologia derivano direttamente dalla possibilità di avere un accesso in autenticazione mediante generazione di un token di autorizzazione apposito.

Per la generazione degli access token si possono utilizzare diversi grant types OAuth 2.0 in base ai casi d'uso applicativi, di seguito i grant type supportati:

- client credentials
- authorization code
- refresh token
- resource owner password

Per le specifiche dei grant type si rimanda al sito ufficiale della OAuth 2.0 industry-standard protocol for authorization <https://oauth.net/2/grant-types/>.

## 3 Fruizione di API esposte su API Manager

Le API pubblicate sull'API Manager sono disponibili sullo Store al seguente indirizzo:

- ambiente di produzione: <https://api-piemonte-store.csi.it/>
- ambiente di test: <https://tst-api-piemonte-store.ecosis.csi.it/>

Per poter accedere alle API è necessario che il fruitore completi i seguenti passi operativi:

- Accreditamento allo Store
- Creazione dell'applicazione contenitore delle API
- Sottoscrizione dell'API di interesse
- Utilizzo delle chiavi OAuth2 per accedere all'API

**ATTENZIONE.** Lo Store delle API dell'**ambiente di test** è accessibile solamente da rete interna CSI, pertanto gli utenti esterni che non possiedono una VPN non potranno effettuare le operazioni di accreditamento, creazione dell'applicazione, sottoscrizione dell'API e generazione delle chiavi in autonomia, come descritto nei successivi paragrafi [3.1](#), [3.2](#), [3.3](#) e [3.4](#). Tali attività dovranno essere mediate dal referente interno del CSI che fornirà le chiavi OAuth dell'applicazione agli utenti esterni che le utilizzeranno per generare i token di accesso per poter invocare le API, come descritto nei paragrafi [3.4.1](#) e [3.5](#). Gli endpoint del gateway dell'ambiente di test, per la generazione dei token di accesso e l'invocazione delle API, sono raggiungibili anche da internet per il solo protocollo 'https'.

### 3.1 Accreditamento allo Store

Il primo passo, per chi vuole utilizzare le API, è l'accreditamento allo Store delle API.

Lo Store supporta le seguenti tipologie di utenti:

- Aziende fornitrici di un ente
- Aziende accreditate presso un ente
- CSI-Piemonte e i suoi fornitori
- Funzionari di un ente

Le aziende con sede in Italia è necessario che dispongano di credenziali SPID per l'accesso allo Store API, nel caso l'azienda sia straniera e non possa disporre di credenziali SPID, l'accesso sarà garantito attraverso credenziali locali allo Store generati dall'amministratore della piattaforma.

CSI-Piemonte e i suoi fornitori, se dispongono di un accesso VPN, possono accreditarsi mediante Identity Provider "Unified Communication".

I funzionari degli enti pubblici possono accedere attraverso Identity Provider RUPAR Sistema Piemonte.

Ogni credenziale di accesso allo Store sarà verificata e validata dall'amministratore della piattaforma che contatterà il richiedente per la corretta attribuzione del ruolo all'interno dello Store.

A seconda della tipologia di utente si dovrà fare richiesta di accreditamento in modalità diverse:

- gli utenti di Aziende fornitrici di un ente, di Aziende accreditate presso un ente, di Funzionari di un ente dovranno segnalare al referente delle API che intende sottoscrivere i seguenti dati:
  - Nome e cognome dell'utente che si accrediterà al portale API Store
  - Codice fiscale dell'utente
  - Indirizzo mail
  - Nome Azienda (nel caso di funzionario PA indicare l'ente di appartenenza)
  - Nome del gruppo di lavoro (opzionale): permette la condivisione delle informazioni contenute nell'applicazione che fruirà delle API, quali ad esempio le chiavi di per generare il token di access. Il nome del gruppo di lavoro dovrà, salvo casistiche da gestire puntualmente, essere composto dal nome dell'applicazione concatenando il suffisso **\_team**.

Il referente dell'API provvederà ad inoltrare la richiesta di accreditamento attraverso la piattaforma Self Portal del CSI Piemonte disponibile al seguente link <https://selfportal-itsm.csi.it> o direttamente inoltrando un ticket su [CMDBuild](#), selezionando la tripla

- Gestione utenze applicative
- Abilitazione utenza
- API MANAGER PER ESPOSIZIONE API REST - API Backbone - CFI3132

Ricevuto il riscontro positivo da parte del referente API, sarà possibile accedere all'API Store utilizzando l'Identity Provider di competenza. Al primo accreditamento da parte dell'utente, l'amministratore dell'API Store confermerà alla casella di posta indicata l'autorizzazione all'accesso al portale.

gli utenti CSI-Piemonte e i suoi fornitori dovranno segnalare al referente delle API la richiesta di utilizzo e inoltrare la richiesta di accreditamento attraverso la piattaforma Self Portal del CSI

Piemonte disponibile al seguente link <https://selfportal-itsm.csi.it> o direttamente inoltrando un ticket su [CMDBuild](#), selezionando la tripletta

- Gestione utenze applicative
- Abilitazione utenza
- API MANAGER PER ESPOSIZIONE API REST - API Backbone - CF13132

### 3.2 Creazione dell'applicazione fruitrice delle API

La sottoscrizione di API richiede che l'utente, dopo aver effettuato il login sullo Store, effettui il censimento di una applicazione virtuale che costituisce il contenitore di sottoscrizioni ad una o più API che fanno capo ad un progetto di fruizione.

Gli attributi che sono richiesti in fase di creazione dell'applicazione sono:

- **Nome dell'applicazione:** nome parlante che riconduca il più possibile al nome dell'applicazione client che utilizza le API. Il nome dell'applicazione può avere al massimo 70 caratteri e non deve contenere caratteri speciali né spazi e deve essere in lowercase.  
Nello scenario di applicazioni realizzate dal CSI Piemonte il nome dell'applicazione dovrà essere valorizzato con i dati censiti su Anagrafica Prodotti ovvero dal codice prodotto, codice componente e linea cliente. Il formato sarà quindi:  
{codice prodotto}\_{codice\_componente}\_{linea cliente}  
Nello scenario di applicazioni realizzate fuori del contesto CSI Piemonte, il nome dell'applicazione dovrà avere il suffisso **-ext**.
- **Gruppi:** elenco dei gruppi di lavoro con cui condividere le informazioni dell'applicazione nello store. Il campo è preimpostato con i gruppi di lavoro di appartenenza dell'utente definiti in fase di accreditamento. Gli utenti che fanno parte del gruppo di lavoro possono visualizzare le chiavi di production e sandbox, generare i token e sottoscrivere API.
- **Quota condivisa per token dell'applicazione:** limite massimo di richieste alle API per ciascun token generato. Il valore è preimpostato ad Unlimited e non è modificabile.
- **Descrizione:** descrizione significativa dell'applicazione che ne permetta il riconoscimento e lo scopo. Nella descrizione occorre riportare l'Ente di riferimento dell'applicazione e l'azienda/ente di appartenenza dell'utente che sta creando l'applicazione.

Al termine della creazione l'applicazione è in stato INACTIVE, è necessario attendere la validazione da parte dell'amministratore della piattaforma per poter procedere con la fase successiva. Il fruitore riceverà una mail non appena l'applicazione sarà validata.

A titolo di esempio seguono i passi per la creazione dell'applicazione.

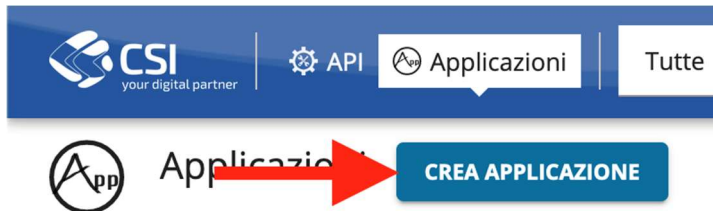
Accedere al portale store, dell'ambiente di test o produzione, ed effettuare il login

Cliccare sul link Applicazioni nella barra in alto.

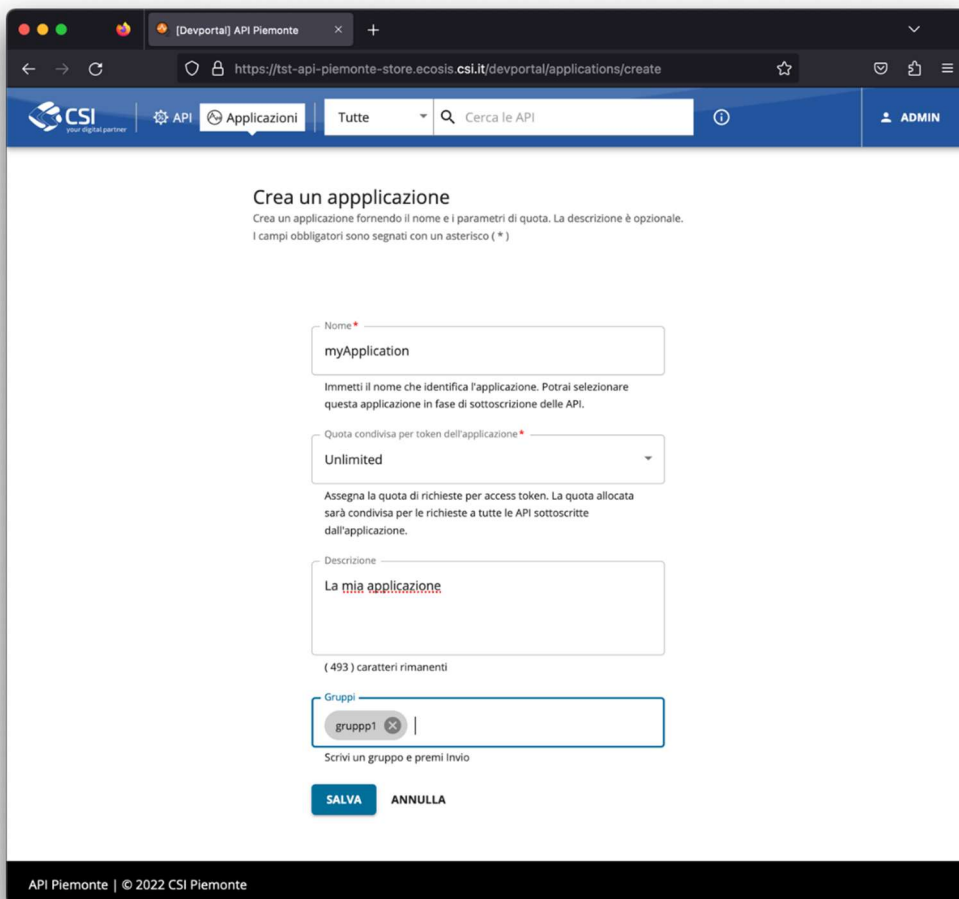


Verrà visualizzata la lista di applicazioni censite.

Cliccare sul link CREA APPLICAZIONE.



Valorizzare i campi presenti nella schermata, come descritto precedentemente.



**Crea un'applicazione**  
Crea un'applicazione fornendo il nome e i parametri di quota. La descrizione è opzionale.  
I campi obbligatori sono segnati con un asterisco (\*)

Nome\*  
myApplication

Immetti il nome che identifica l'applicazione. Potrai selezionare questa applicazione in fase di sottoscrizione delle API.

Quota condivisa per token dell'applicazione\*  
Unlimited

Assegna la quota di richieste per access token. La quota allocata sarà condivisa per le richieste a tutte le API sottoscritte dall'applicazione.

Descrizione  
La mia applicazione

( 493 ) caratteri rimanenti

Gruppi  
gruppo1

Scrivi un gruppo e premi invio

**SALVA** **ANNULLA**

API Piemonte | © 2022 CSI Piemonte

Cliccare sul pulsante Salva.

### 3.3 Sottoscrizione dell'API di interesse

L'utente fruitore dal portale API Store può richiedere la sottoscrizione di una API non appena dispone di un Applicazione il cui stato è ACTIVE. Contestualmente alle operazioni di sottoscrizione effettuate sul portale, occorre inoltrare una richiesta via e-mail all'owner dell'Api mettendo in copia [supporto.apimanager@csi.it](mailto:supporto.apimanager@csi.it)

Concluso l'iter di sottoscrizione da parte dell'utente, seguirà un iter di autorizzazione all'accesso da parte dell'amministratore di piattaforma. L'utente riceverà comunicazione via mail sull'esito dell'operazione.

Gli stati della sottoscrizione di un'API sono:

- ONHOLD: in attesa di approvazione
- UNBLOCKED: approvata
- BLOCKED: bloccata dall'owner dell'API
- REJECTED: rifiutata dal gruppo di amministrazione dell'API Manager

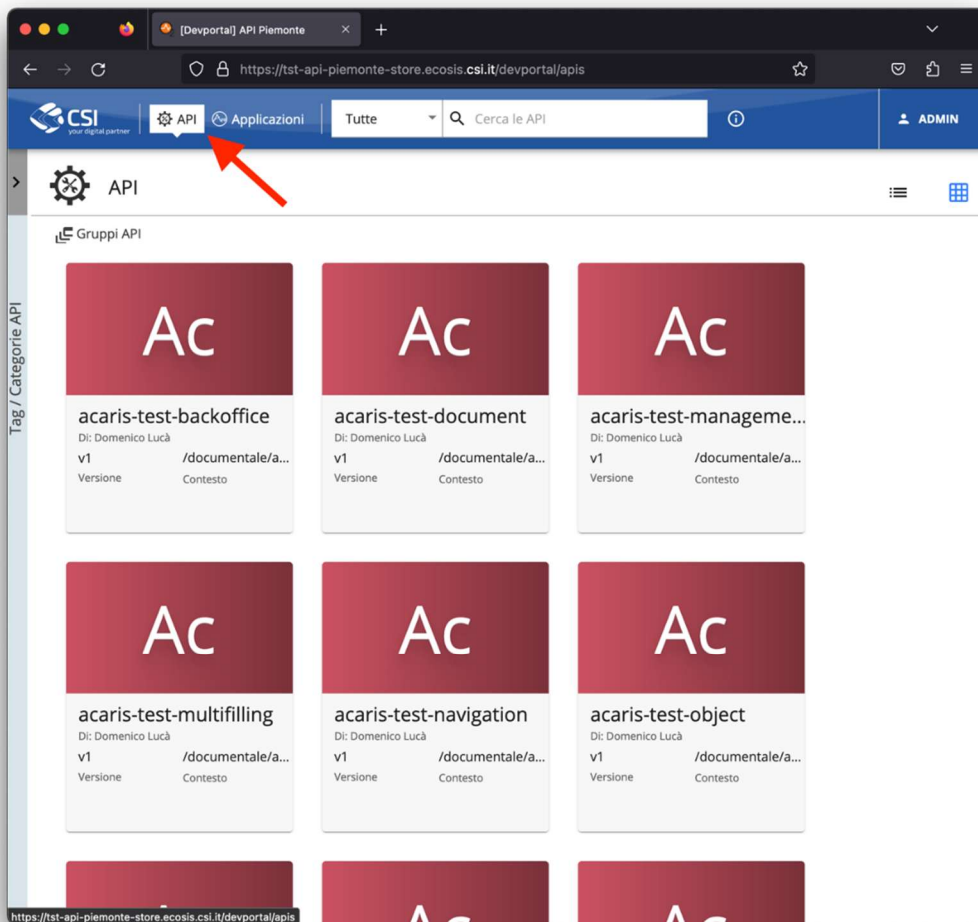
Al termine della procedura la sottoscrizione è in stato ONHOLD, ottenuta l'autorizzazione lo stato muterà in "UNBLOCKED" e sarà possibile per il fruitore effettuare le chiamate all'API sottoscritta.

A titolo di esempio seguono i passi da eseguire per effettuare la sottoscrizione.

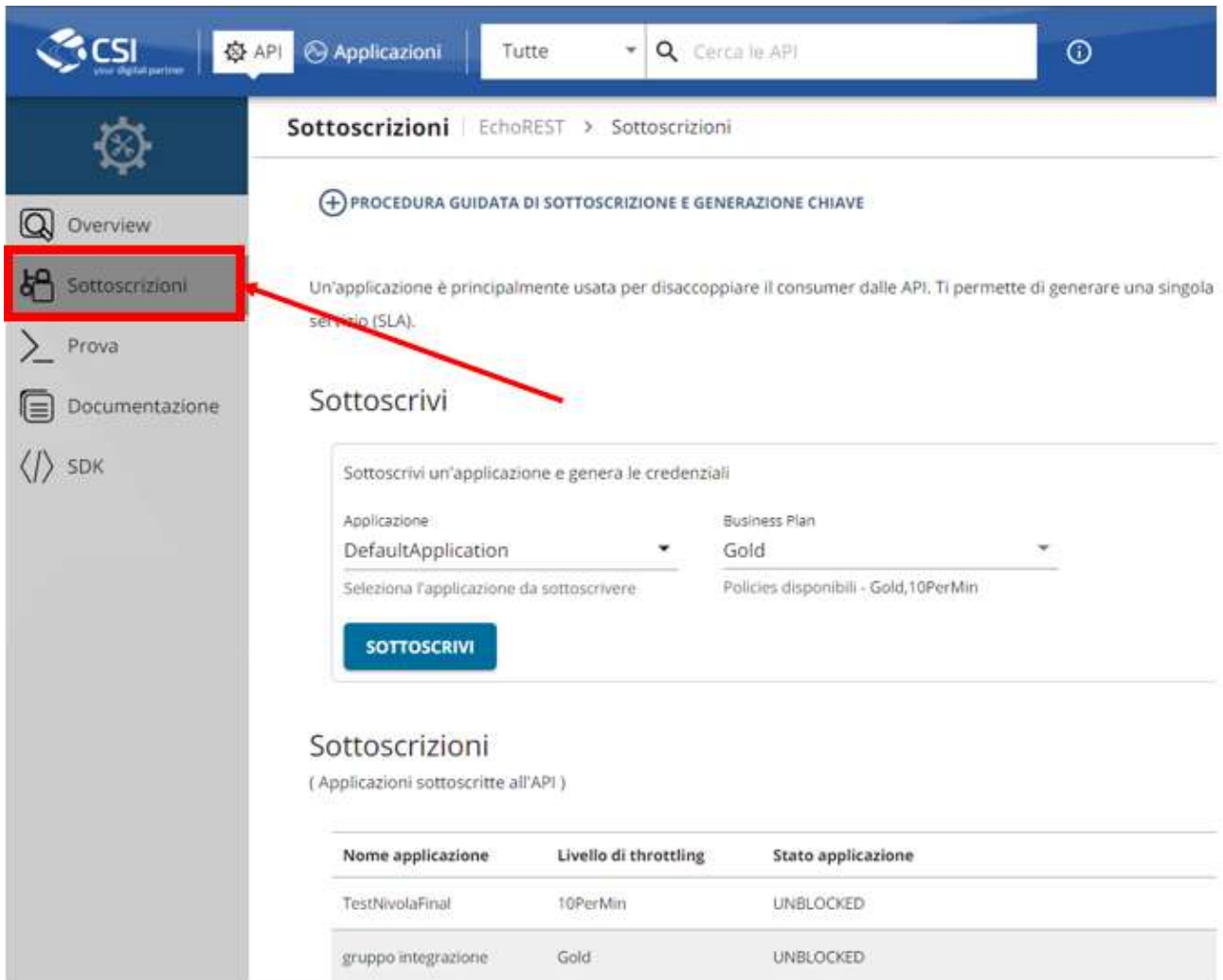
Accedere al portale store, dell'ambiente di test o produzione, ed effettuare il login.

Cliccare sul link API, nella barra in alto.





Cliccare sull'API che si vuole sottoscrivere. Si aprirà una pagina di dettaglio con le informazioni descrittive dell'API. Quindi selezionare la voce Sottoscrizioni nella barra di sinistra.



**Sottoscrizioni** | EchoREST > Sottoscrizioni

**PROCEDURA GUIDATA DI SOTTOSCRIZIONE E GENERAZIONE CHIAVE**

Un'applicazione è principalmente usata per disaccoppiare il consumer dalle API. Ti permette di generare una singola servizio (SLA).

**Sottoscrivi**

Sottoscrivi un'applicazione e genera le credenziali

Applicazione: **DefaultApplication** Business Plan: **Gold**

Seleziona l'applicazione da sottoscrivere: Policies disponibili - Gold, 10PerMin

**SOTTOSCRIVI**

**Sottoscrizioni**  
 ( Applicazioni sottoscritte all'API )

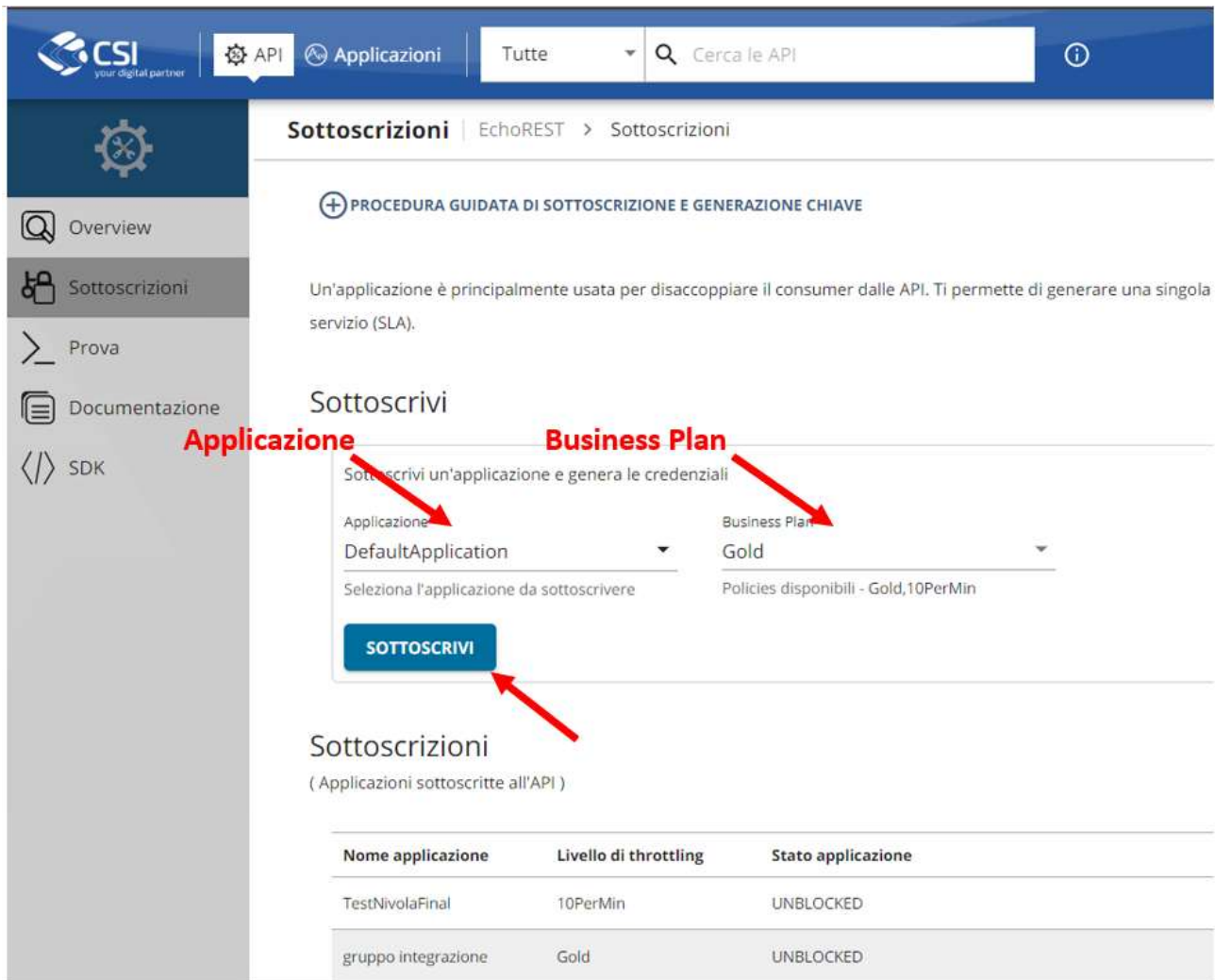
| Nome applicazione   | Livello di throttling | Stato applicazione |
|---------------------|-----------------------|--------------------|
| TestNivolaFinal     | 10PerMin              | UNBLOCKED          |
| gruppo integrazione | Gold                  | UNBLOCKED          |

Nella sezione "Sottoscrivi" selezionare l'applicazione che si vuole utilizzare per sottoscrivere l'API e il Business Plan da utilizzare.

Il Business Plan rappresenta il numero di richieste che è possibile effettuare nell'unità di tempo. I Business Plan disponibili di default sono:

- Unlimited (numero illimitato di richieste)
- Gold (5000 richieste al minuto)
- Silver (2000 richieste al minuto)
- Bronze (1000 richieste al minuto)

I Business Plan selezionabili in fase di sottoscrizione di una API sono quelli resi disponibili dall'owner dell'API.



**Sottoscrizioni** | EchoREST > Sottoscrizioni

**PROCEDURA GUIDATA DI SOTTOSCRIZIONE E GENERAZIONE CHIAVE**

Un'applicazione è principalmente usata per disaccoppiare il consumer dalle API. Ti permette di generare una singola servizio (SLA).

**Sottoscrivi**

Sottoscrivi un'applicazione e genera le credenziali

Applicazione: **DefaultApplication** | Business Plan: **Gold**

Seleziona l'applicazione da sottoscrivere | Policies disponibili - Gold, 10PerMin

**SOTTOSCRIVI**

**Sottoscrizioni**  
( Applicazioni sottoscritte all'API )

| Nome applicazione   | Livello di throttling | Stato applicazione |
|---------------------|-----------------------|--------------------|
| TestNivolaFinal     | 10PerMin              | UNBLOCKED          |
| gruppo integrazione | Gold                  | UNBLOCKED          |

**Nota importante:** tutte le sottoscrizioni che non verranno approvate entro due mesi dalla data dei sottomissione potrebbero venire rigettate d'ufficio nell'ambito delle attività periodiche di pulizia dello storico.

### 3.4 Generazione e utilizzo delle chiavi di accesso

Attraverso lo Store per ciascuna applicazione è possibile generare le chiavi (consumer key e consumer secret) per la generazione dei token.

Le applicazioni hanno due tipi di chiavi:

- chiavi di produzione
- chiavi di sandbox

Le chiavi di produzione permettono di generare access token per chiamare gli endpoint di produzione delle API. Le chiavi di sandbox permettono di generare access token con cui accedere, se disponibili, agli endpoint dell'ambiente sandbox delle API, utili per la fase preliminare di integrazione. Nell'ambiente di test, indipendentemente dalle chiavi in uso (produzione o sandbox), l'endpoint API è lo stesso, l'API Manager in funzione delle chiavi è in grado di indirizzare al back-end di riferimento (produzione o sandbox). In ambiente

di produzione gli endpoint di produzione e sandbox sono diversi e bisogna utilizzare il token opportuno in base all'endpoint chiamato.

**Info.** Nell'**ambiente di test** l'endpoint definito come *produzione* punta ai servizi di backend esposti in ambiente test, mentre l'endpoint di *sandbox*, quando utilizzato, fa riferimento ai servizi di backend esposti in apposito ambiente sandbox o in ambiente di sviluppo.

Per ciascuna coppia di chiavi (sia di produzione che di sandbox) è possibile decidere quali grant types utilizzare per la generazione degli access token. I grant type standard che la piattaforma è in grado di supportare sono i seguenti:

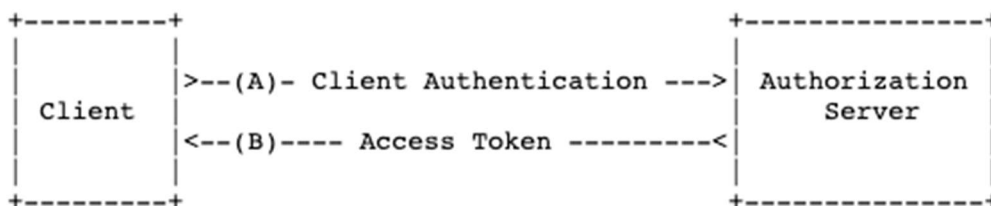
- Refresh Token
- Client Credentials
- Password
- Code

Più quelli custom:

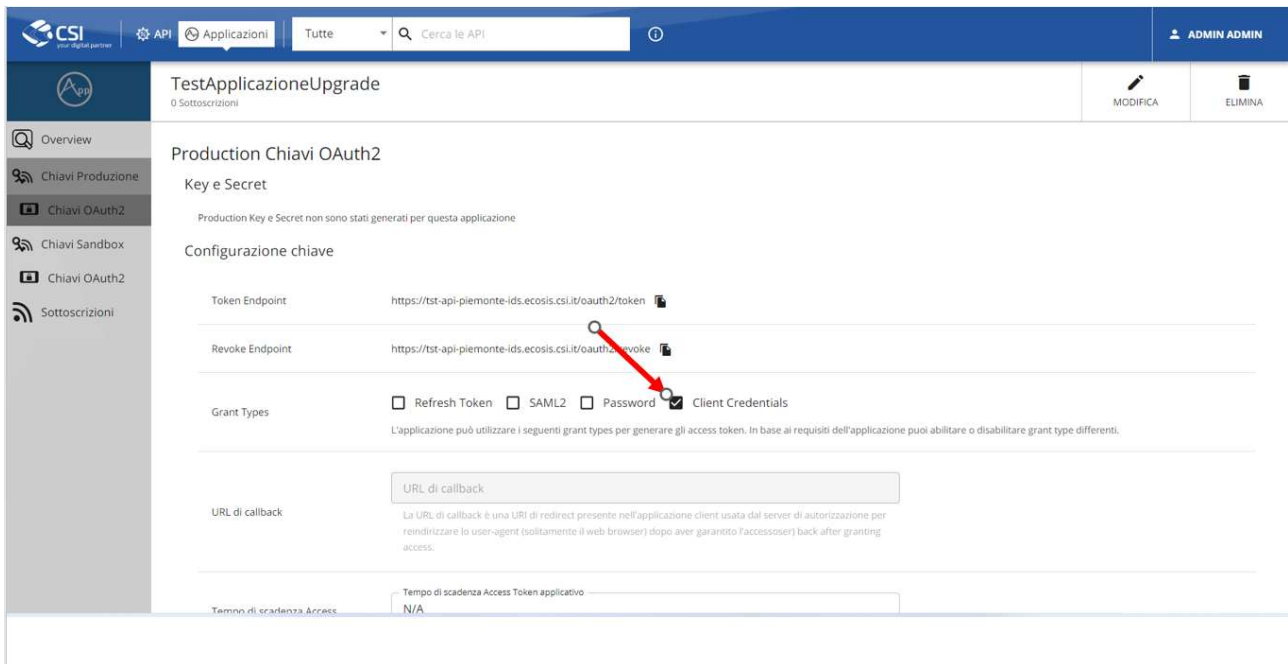
- SAML2
- IWA-NTLM
- JWT
- urn:ietf:params:oauth:grant-type:token-exchange

Per una corretta configurazione dell'applicazione bisogna abilitare **solamente** i grant type strettamente necessari in base al tipo di applicazione che si sta sviluppando.

Ad oggi è abilitato esclusivamente il grant type **client credentials grant type**. Di seguito il flow descritto dalla Internet Engineering Task Force (IETF) nella RFC che descrive il framework Oauth (<https://tools.ietf.org/html/rfc6749#page-40>).



Per procedere alla generazione delle chiavi selezionare il grant type "Client Credentials" e cliccare sul pulsante "Genera chiavi" in fondo alla pagina.



TestApplicazioneUpgrade  
0 Sottoscrizioni

Overview  
Chiavi Produzione  
Chiavi OAuth2  
Chiavi Sandbox  
Chiavi OAuth2  
Sottoscrizioni

Production Chiavi OAuth2  
Key e Secret  
Production Key e Secret non sono stati generati per questa applicazione

Configurazione chiave

|                 |  |
|-----------------|--|
| Token Endpoint  | <a href="https://tst-api-piemonte-ids.ecosis.csi.it/oauth2/token">https://tst-api-piemonte-ids.ecosis.csi.it/oauth2/token</a>                                  |
| Revoke Endpoint | <a href="https://tst-api-piemonte-ids.ecosis.csi.it/oauth2/revoke">https://tst-api-piemonte-ids.ecosis.csi.it/oauth2/revoke</a>                                |
| Grant Types     | <input type="checkbox"/> Refresh Token <input type="checkbox"/> SAML2 <input type="checkbox"/> Password <input checked="" type="checkbox"/> Client Credentials |

L'applicazione può utilizzare i seguenti grant types per generare gli access token. In base ai requisiti dell'applicazione puoi abilitare o disabilitare grant type differenti.

URL di callback

URL di callback

La URL di callback è una URI di redirect presente nell'applicazione client usata dal server di autorizzazione per reindirizzare lo user-agent (solitamente il web browser) dopo aver garantito l'accesso back after granting access.

Tempo di scadenza Access Token applicativo

Tempo di scadenza Access

N/A

### 3.4.1 Generazione Token

Gli endpoint per la generazione degli access token sono:

- ambiente di produzione: <https://api-piemonte.csi.it/token>, <http://api-piemonte.csi.it/token>
- ambiente di test: <https://tst-api-piemonte.ecosis.csi.it/token>, <http://tst-api-piemonte.ecosis.csi.it/token>

L'endpoint è disponibile sia in http che in https ma in generale vale quanto definito nelle linee guida di progettazione sicura di SOC al par. 3.2.4.3 di cui si riporta un estratto:

*La cooperazione applicativa su rete interna (cioè rete di backend, non accessibile dalle postazioni dell'utente finale) possono avvenire anche in chiaro; le esposizioni su rete esterna (es. rupar o internet) devono invece essere cifrate con https.*

*Si suppone che il rischio del transito di informazioni anche sensibili (dati privati, credenziali) su rete interna/di backend sia basso: per questo motivo, considerando anche l'overhead di performance dovuto alla cifratura del canale e l'overhead organizzativo della gestione dei certificati, la scelta standard per le interazioni a servizi su rete di backend è quella del canale in chiaro.*

Questo paragrafo illustra come generare il token utilizzando il grant type client credentials. Un access token generato con questo grant type identifica solamente l'applicazione chiamante.

Effettuare una chiamata alla Token API con i seguenti parametri:

```
host: api-piemonte.csi.it
path: /token
method: POST
headers:
Content-Type: application/x-www-form-urlencoded
Authorization: Basic base64encode(consumer_key:consumer_secret)
body: grant_type=client_credentials
```

La risposta ritornata in caso di esito positivo è nel seguente formato:

```
http status code: 200
headers
Content-Type: application/json
body:
{
  "scope": "<space separated list of scopes>",
  "token_type": "Bearer",
  "expires_in": <seconds>,
  "access_token": "<access token>"
}
```

Il messaggio restituito contiene un nuovo access token.

In caso di esito negativo verrà restituito un http status code diverso da 200 e nel body un oggetto json che descriverà l'errore, nel formato:

```
{
  "error_description": "Client Authentication failed.",
  "error": "invalid_client"
}
```

### 3.4.2 Esempio di chiamata cURL alla token API:

```
curl -k -d "grant_type=client_credentials" \
-H "Authorization: Basic
SVpzSWk2SERiQjVlOFZLZFPBblVpX2ZaM2Y4YTpHbTBiSjZvVlY4ZkM1TlFMTGxDNmpzbEFDVzh" \
-H "Content-Type: application/x-www-form-urlencoded" \
https://api-piemonte.csi.it/token
```

### 3.4.3 Esempio di codice java per ottenere l'access token

Esempio di codice java per ottenere l'access token

```
import javax.net.ssl.HttpURLConnection;
import java.io.*;
import java.net.URL;
import java.util.Base64;

private static final String clientId = "...";//clientId
private static final String clientSecret = "...";//client secret
private static final String tokenUrl = "https://api-piemonte.csi.it/token";
private static final String auth = clientId + ":" + clientSecret;
private static final String authentication =
Base64.getEncoder().encodeToString(auth.getBytes());

public String getToken() {
```

```
String content = "grant_type=client_credentials";
BufferedReader reader = null;
HttpsURLConnection connection = null;
String returnValue = "";
try {
    URL url = new URL(tokenUrl);
    connection = (HttpsURLConnection) url.openConnection();
    connection.setRequestMethod("POST");
    connection.setDoOutput(true);
    connection.setRequestProperty("Authorization", "Basic " + authentication);
    connection.setRequestProperty("Content-Type", "application/x-www-form-urlencoded");
    connection.setRequestProperty("Accept", "application/json");
    PrintStream os = new PrintStream(connection.getOutputStream());
    os.print(content);
    os.close();
    reader=new BufferedReader(new InputStreamReader(connection.getInputStream()));
    String line = null;
    StringWriter out = new StringWriter(connection.getContentLength() > 0 ?
connection.getContentLength() : 2048);
    while ((line = reader.readLine()) != null) {
        out.append(line);
    }
    returnValue = out.toString();
} catch (Exception e) {
    System.out.println("Error : " + e.getMessage());
} finally {
    if (reader != null) {
        try {
            reader.close();
        } catch (IOException e) {
        }
    }
    connection.disconnect();
}
```

### 3.4.4 Esempio di codice python per ottenere l'access token

Esempio di codice python per ottenere l'access token (utilizza la libreria Requests-OAuthlib - <https://requests-oauthlib.readthedocs.io/>):

```
client_id = 'your_client_id'
client_secret = 'your_client_secret'

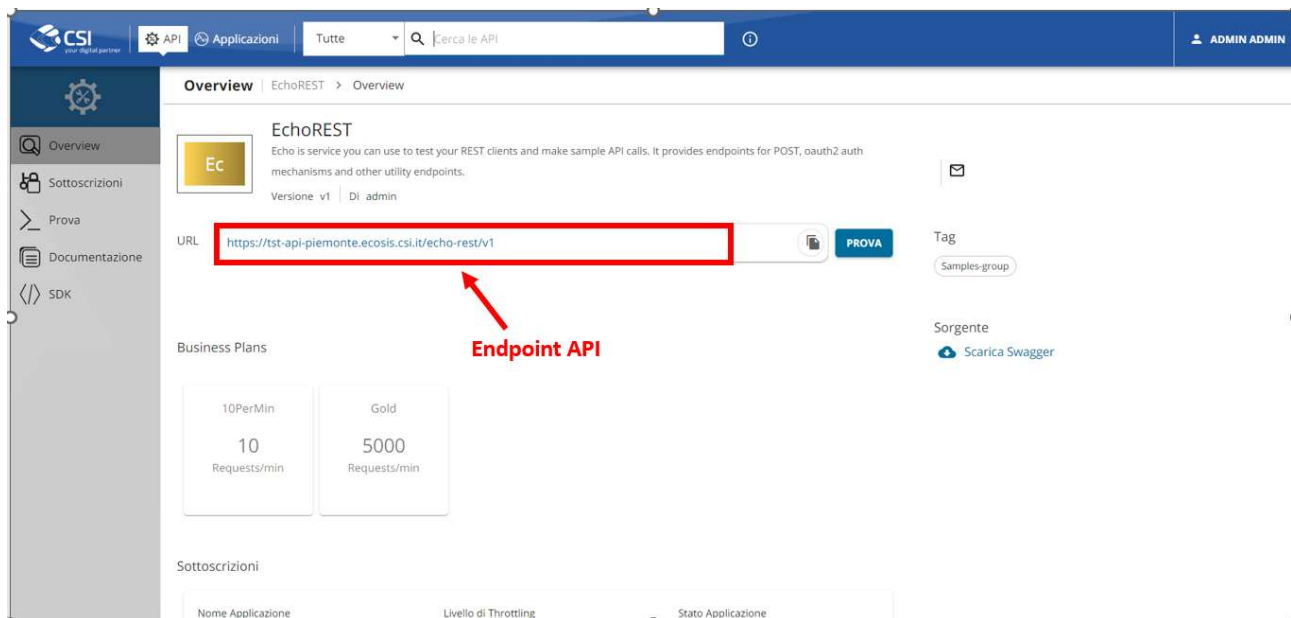
from oauthlib.oauth2 import BackendApplicationClient
from requests.auth import HTTPBasicAuth

auth = HTTPBasicAuth(client_id, client_secret)
client = BackendApplicationClient(client_id=client_id)
oauth = OAuth2Session(client=client)

token = oauth.fetch_token(token_url='https://api-piemonte.csi.it/token', auth=auth)
```

## 3.5 Invocare un API

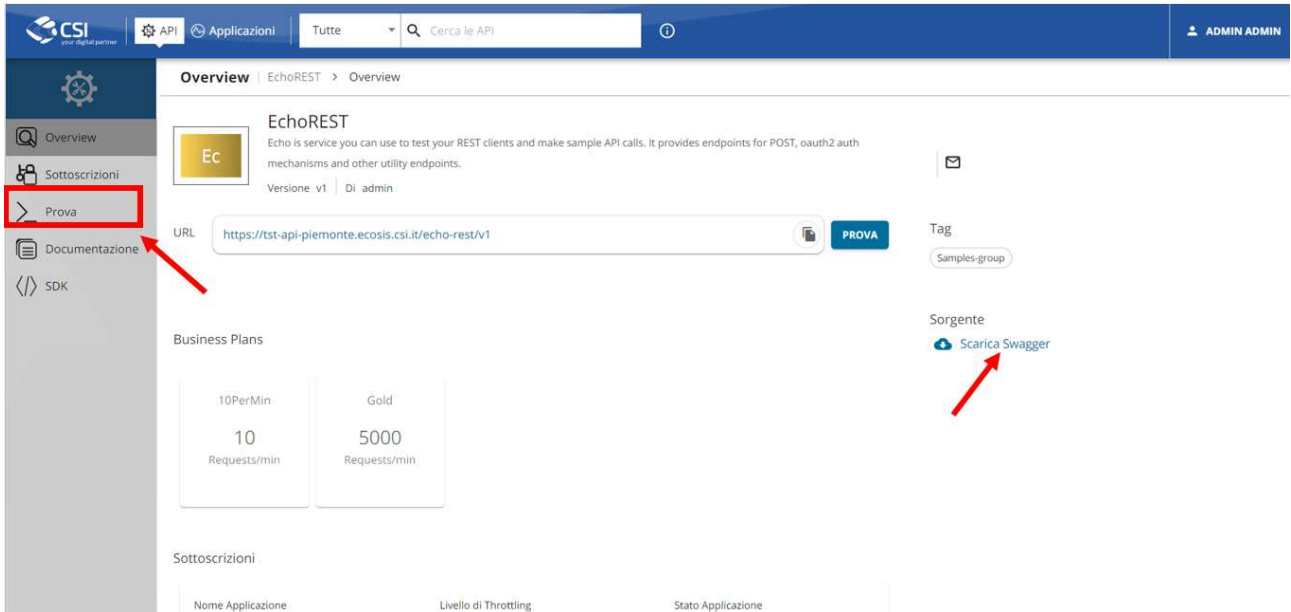
Recuperato l'access token è possibile invocare le API sottoscritte. Gli endpoint delle API e la relativa documentazione sono visibili nella pagina di dettaglio di ciascuna API.



The screenshot displays the API Store interface for the 'EchoREST' API. The URL 'https://tst-api-piemonte.ecosis.csi.it/echo-rest/v1' is highlighted with a red box and labeled 'Endpoint API' with a red arrow. The interface includes a sidebar with navigation options like 'Overview', 'Sottoscrizioni', 'Prova', 'Documentazione', and 'SDK'. The main content area shows the API name, description, version, and business plans.

L'owner dell'API può decidere con quale protocollo di trasporto pubblicare l'API, se http e/o http con SSL (https). In tutti i casi, il trasporto http senza SSL può essere usato solamente dalle applicazioni che risiedono sulla rete interna del CSI. Nella tab "Prova" di una API oppure scaricandosi la definizione Swagger dalla tab "Overview" è possibile vedere, nel caso di un API REST, tutte le risorse esposte con le relative interfacce di input e output.





The screenshot shows the API Manager interface for the EchoREST API. The left sidebar contains navigation links: Overview, Sottoscrizioni, Prova (highlighted with a red box), Documentazione, and SDK. The main content area displays the API details for EchoREST, including its description, version (v1), and a list of Business Plans (10PerMin and Gold). The URL field is populated with `https://tst-api-piemonte.ecosis.csi.it/echo-rest/v1`. The 'Sorgente' section includes a link to 'Scarica Swagger'.

Per invocare l'API quindi bisogna aggiungere l'header Authorization mettendo il bearer token generato.

Di seguito il formato di una chiamata cURL ad una risorsa GET di una API esposta sull'API Manager:

```
curl -H "Authorization: Bearer <access_token>" <api_endpoint>
```

Ad esempio:

```
curl -H "Authorization: Bearer d7252944-14c4-48d5-858b-6b80d8bf08b4" https://api-  
piemonte.csi.it/demografia/v1/anagrafe/cittadini/XXXXXX45B23L219F/famiglia
```