



CAITEL

Catasto Impianti TERMICI Liguria

API CAITEL

Istruzioni richiesta abilitazione ditte

Versione 1.0.0

Regione Liguria — Liguria Digitale

11 Settembre 2026

Supporto: caitel-api-assistenza@liguriadigitale.it

Sommario

Sommario	2
1. Introduzione	3
1.1 Scopo del documento	3
2. Introduzione	3
2.1 Mail di richiesta abilitazione all'utilizzo delle API	3
2.2. Mutua autenticazione	4
2.3 Consegna credenziali (Client ID e Client Secret)	4
2.4 Autenticazione	5
2.5 Acquisizione del Bearer Token	6
2.6 Invocazione API CAITEL (per ogni chiamata)	6
2.7 Verifica autorizzazione lato backend (per ogni chiamata)	7

1. Introduzione

1.1 Scopo del documento

Il presente documento descrive il flusso che devono seguire le ditte accreditate su Caitel per poter svolgere le attività legate all'integrazione dell'utilizzo delle API nei loro sistemi gestionali.

Il documento riporta anche il dettaglio relativo alla componente di autenticazione per ogni chiamata API.

2. Introduzione

2.1 Mail di richiesta abilitazione all'utilizzo delle API

Le ditte accreditate per Caitel che necessitano di integrare l'utilizzo delle API nei loro sistemi gestionali devono inviare una richiesta alla casella caitel-api-assistenza@liguriadigitale.it indicando i seguenti dati:

- a) Riferimenti della ditta così come risulta accreditata su Caitel
- Ragione Sociale della ditta
 - Identificativo fiscale della ditta

Se la ditta si avvale del supporto tecnico di una casa software per l'integrazione delle API nei suoi sistemi gestionali e vuole coinvolgere direttamente la casa software nelle comunicazioni tecniche, nella mail di richiesta è necessario indicare anche:

- b) Riferimenti della casa software e del personale tecnico da contattare
- Ragione Sociale della casa software
 - Identificativo fiscale casa software
 - Nome dell'applicativo software utilizzato
 - Riferimenti del personale di contatto (nome, cognome, indirizzo mail, numero di telefono)

Tali riferimenti verranno utilizzati per le comunicazioni che vengono gestite tramite la casella caitel-api-assistenza@liguriadigitale.it

In alternativa, la ditta può essere l'unica a comunicare con la casella caitel-api-assistenza@liguriadigitale.it occupandosi poi in autonomia della condivisione del materiale con la casa software.

Se una ditta non si avvale più dell'assistenza di una casa software, è necessario che lo comunichi tempestivamente alla casella caitel-api-assistenza@liguriadigitale.it in modo che si intervenga sulle abilitazioni per bloccare l'utilizzo delle API da parte della casa software a nome della ditta stessa.

Se una ditta necessita di cambiare la casa software di riferimento, è necessario che lo comunichi tempestivamente alla casella caitel-api-assistenza@liguriadigitale.it indicando i riferimenti della casa software da "disabilitare" e indicando i riferimenti della nuova casa software.

- c) Ambiente per il quale si richiede l'abilitazione all'utilizzo delle API

E' indispensabile che nella richiesta venga esplicitato per quale ambiente si richiede l'abilitazione scegliendone uno tra i seguenti:

- ambiente di sperimentazione

- ambiente di esercizio

A questo proposito, si fa presente che l'utilizzo delle API in ambiente di esercizio determina azioni sui dati "reali" gestiti dal sistema ufficiale "CAITEL LIBRETTO DI IMPIANTO e NUOVO CAITEL PWA" raggiungibile dalla welcome page Caitel <https://servizi.regione.liguria.it/page/welcome/CAITEL> : tali dati sono quindi visibili anche alle autorità competenti e ai responsabili di impianto, ciascuno per la parte di interesse.

In fase iniziale, si suggerisce di richiedere prima l'abilitazione all'ambiente di sperimentazione e di richiedere l'abilitazione all'ambiente di esercizio solo a termine delle prove.

2.2. Mutua autenticazione

A fronte della ricezione della mail di richiesta di abilitazione all'uso delle API, Liguria Digitale provvede alla configurazione del certificato sul gateway e alla creazione dell'Application WSO2 relativa alla ditta specifica.

L'utilizzo delle API Caitel prevede la mutua autenticazione per effettuare l'autenticazione e garantire la protezione dei dati. Prima di poter utilizzare le API, le ditte devono quindi completare il processo di registrazione con Liguria Digitale, che opera da Certification Authority (CA).

I passi da effettuare da parte delle ditte sono i seguenti:

- 1. Generazione chiave privata: la ditta genera una propria chiave privata RSA e il corrispondente Certificate Signing Request (CSR)

Se la ditta NON si avvale di una casa software, nella CSR vanno riportati i seguenti riferimenti:

- a) **CN**: identificativo fiscale della ditta
- b) **O**: ragione sociale della ditta
così come risulta dall'accreditamento Caitel

Se la ditta si avvale di una casa software, nella CSR vanno riportati i seguenti dettagli:

- c) **CN**: identificativo fiscale della casa software
- d) **O**: ragione sociale della casa software

- 2. Invio CSR a Liguria Digitale: la ditta invia la CSR alla casella caitel_api_assistenza@liguriadigitale.it
La CSR può già essere inviata allegandola alla mail di richiesta di utilizzo delle API
- 3. Ricezione certificato firmato: Liguria Digitale firma il certificato e invia all'azienda un file PEM contenente la catena completa di fiducia (Root CA Liguria Digitale + SubCA Regione Liguria + certificato della ditta)
I certificati sono validi 5 anni.
Se la ditta Caitel avrà bisogno di continuare ad utilizzare le API anche dopo i primi 5 anni, con un po' di anticipo rispetto alla scadenza del certificato, invierà di nuovo la CSR a Liguria Digitale (è anche possibile rimandare la stessa inviata 5 anni prima e Liguria Digitale la firma di nuovo)

Per il punto 1 e, in caso di necessità, la ditta può chiedere supporto a Liguria Digitale scrivendo alla casella caitel-api-assistenza@liguriadigitale.it

2.3 Consegna credenziali (Client ID e Client Secret)

L'accesso alle API CAITEL avviene tramite il gateway WSO2 di Liguria Digitale, pubblicato su URL pubblico.

A fronte della ricezione della mail di richiesta di abilitazione all'uso delle API, Liguria Digitale provvede alla creazione dell'Application WSO2 relativa alla ditta specifica e alla configurazione del certificato sul gateway.

A seguito del completamento del processo di accreditamento, Liguria Digitale invia alla ditta una mail che consente di scaricare le credenziali specifiche della ditta: **Client ID** e **Client Secret**.

Tali credenziali sono specifiche per ogni ditta accreditata su Caitel, identificano univocamente la ditta sul gateway WSO2 e sono strettamente riservate: non devono essere condivise e vanno conservate in modo sicuro. In caso di compromissione è necessario contattare immediatamente caitel-api-assistenza@liguriadigitale.it.

Nella mail di conferma dell'avvenuto processo di accreditamento, verrà anche riportato l'url relativo all'endpoint da indicare nella POST per ottenere il token, differenziando i riferimenti a seconda che sia stato richiesta l'abilitazione per l'utilizzo dell'ambiente di sperimentazione o dell'ambiente di esercizio.

Solo nel caso la ditta abbia effettuato la richiesta per l'utilizzo dell'ambiente per la sperimentazione, nella comunicazione di avvenuto accreditamento verranno riportati anche i riferimenti di solo 2 soggetti (il rappresentante legale e un operatore) abilitati il cui codice fiscale del soggetto dovrà essere riportato nell'header della chiamata.

2.4 Autenticazione

Tutte le chiamate richiedono l'header HTTP obbligatorio:

Header	Tipo	Pattern	Descrizione
codice-fiscale-operatore	string	^[A-Z]{6}[0-9]{2}[A-Z][0-9]{2}[A-Z][0-9]{3}[A-Z]\$	Codice Fiscale dell'operatore abilitato (16 caratteri, formato CF persona fisica italiano), fornito dal gateway WSO2. In assenza o formato errato risponde HTTP 403.

L'accesso avviene tramite il gateway WSO2 che inietta il codice fiscale operatore nell'header.

Il codice fiscale del soggetto riportato nell'header deve risultare abilitato ad operare per la ditta stessa sul sistema "CAITEL LIBRETTO DI IMPIANTO e NUOVO CAITEL PWA" (funziona di riferimento: Gestione Operatori) raggiungibile dalla welcome page Caitel <https://servizi.regione.liguria.it/page/welcome/CAITEL>.

Nel caso la ditta abbia effettuato la richiesta per l'utilizzo dell'ambiente per la sperimentazione, potranno essere utilizzati nell'header della chiamata solo i 2 codici fiscali indicati da Liguria Digitale nella mail di avvenuto accreditamento.

2.5 Acquisizione del Bearer Token

Prima di invocare le API CAITEL, la ditta deve ottenere un Bearer Token dal server di autorizzazione di Regione Liguria. Il token ha durata di 1 ora e deve essere rinnovato alla scadenza.

Richiesta HTTP (POST):

```
POST https://[redacted]/oauth2/token
Authorization: Basic <base64(ClientID:ClientSecret)>
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials
```

Il valore dell'header Authorization si ottiene concatenando Client ID e Client Secret con il carattere : (due punti) e codificando il risultato in Base64. Esempio: se ClientID = "myapp" e ClientSecret = "s3cr3t", la stringa da codificare è "myapp:s3cr3t".

Risposta attesa (HTTP 200):

```
{
  "access_token": "674b4195-54e2-3e10-bda8-8845b7f3bd43",
  "token_type": "Bearer",
  "expires_in": 3600
}
```

Campo risposta	Tipo	Descrizione
access_token	string	Token da usare come Bearer nelle chiamate API CAITEL. Valido per expires_in secondi.
token_type	string	Sempre "Bearer".
expires_in	integer	Durata in secondi del token (tipicamente 3600 = 1 ora). Alla scadenza occorre richiedere un nuovo token.

Nota: L'URL da indicare nella POST verrà comunicato da Liguria Digitale in fase di accreditamento

2.6 Invocazione API CAITEL (per ogni chiamata)

Ogni chiamata alle API CAITEL richiede che siano soddisfatte contemporaneamente le seguenti tre condizioni:

Requisito	Come configurarlo	Dettaglio
Bearer Token	Header: Authorization: Bearer <access_token>	access_token ottenuto dal passo §2.5. Rinnovare alla scadenza (expires_in secondi).
CF Operatore	Header: codice-fiscale-operatore: <CF>	Codice Fiscale (16 caratteri, CF persona fisica) del soggetto abilitato per la ditta su CAITEL. I CF abilitati sono comunicati da Liguria Digitale in fase di accreditamento. Assenza o formato non valido → HTTP 403.
Certificato mTLS	Configurazione TLS del client HTTP	Il client HTTP deve presentare il certificato firmato ricevuto da Liguria Digitale (file PEM — vedere §2.2) durante il handshake TLS con il gateway WSO2. In assenza del certificato la connessione viene rifiutata prima di raggiungere il backend.

Esempio di chiamata completa:

```
POST https://services-caitel-test.regione.liguria.it/api/accatamento/nuovo-
impianto/inserisci
Authorization: Bearer 674b4195-54e2-3e10-bda8-8845b7f3bd43
codice-fiscale-operatore: RSSMRA80A01F205X
Content-Type: application/json
[+ certificato mTLS configurato sul client TLS]

{ <AccatamentoRichiesta> }
```

Nota: in immagine è riportato l'URL di test (*services-caitel-test.regione.liguria.it*)

2.7 Verifica autorizzazione lato backend (per ogni chiamata)

Il backend CAITEL effettua i seguenti controlli su ogni richiesta ricevuta:

Passo	Descrizione	Esito in caso di errore
1 — Validazione CF operatore	Estrae l'header codice-fiscale-operatore e lo valida con la regexp: <code>^[A-Z]{6}[0-9]{2}[A-Z][0-9]{2}[A-Z][0-9]{3}[A-Z]\$</code>	HTTP 403
2 — Decodifica token e estrazione PIVA	Estrae la PIVA dell'azienda chiamante (PIVA come claim dell'Application WSO2 creata in fase di accreditamento).	HTTP 403
3 — Verifica abilitazione CN/CF/PIVA	Verifica che il CN della casa software sia abilitato per la PIVA estratta e che il CF operatore risulti abilitato per la PIVA estratta sulla base dati CAITEL.	HTTP 403