Linee guida Generali API TS Digital

Header

Ad ogni chiamata è obbligatorio inserire i parametri riportati e popolarli nel seguente modo:

Authorization: Bearer Token. Come si genera il token? Vedi nella sezione info

X-App-Name: codice identificativo rilasciato da Teamsystem al momento del censimento. Non utilizzare valori diversi dall'AppName assegnato in quanto vi sono dei controlli che bloccano tutte le chiamate con AppName non censiti.

User-Agent: nome dell'applicativo/software utilizzato.

X-App-Version: versione dell'applicativo/software utilizzato.

X-Request-ID: Identificativo univoco della singola richiesta nel formato cuid. Esempio: se per ottenere la lista documenti devo chiamare Auth, Anagrafica e B2BRead ogni singola chiamata deve avere un valore diverso di X-Request-ID. NON utilizzare lo stesso valore per chiamate diverse.

X-Correlation-ID: Identificativo univoco del flusso in formato uuid-v4. Esempio: se per ottenere la lista documenti devo chiamare Auth, Anagrafica e B2BRead tutte le chiamate dovrebbero avere lo stesso X-Correlation-ID. In questo modo nei log è possibile tracciare e correlare tutte le richieste. NON utilizzare lo stesso valore per flussi diversi.

X-Item-ID: identificativo di chi effettua la richiesta (UUID). Come si recupera l'UUID? Vedi nella sezione info

X-User-ID: identificativo dell'utenza che sta effettuando la richiesta. (ID della Chiave Tecnica).

X-Manager-ID: parametro opzionale. Da popolare con UUID dello studio che opera per aziende gestite.

> **Chiavi Tecniche**
> Le credenziali (id e secret) da utilizzare nell'autenticazione possono essere generate dalla sezione applicativi del portale.

Per saperne di più, clicca qui.

Token
Per generare il token invece, i passaggi sono i seguenti:
1. Generare il nonce, inserendo nel body della chiamata l'ID della chiave tecnica.
2. Generare il token, inserendo nel body della chiamata l'ID della chiave tecnica.

Calcolare il digest tramite la seguente formula: sha256(sha256(ID + secret) + nonce)

Chiamata per generare il nonce:

```
curl --location --request POST 'https://b2b-auth-service-test.agyo.io/api/v3/nonces' \
--header 'accept: application/json' \
--header 'User-Agent: Postman' \
--header 'X-App-Name: TSxyz' \
--header 'X-App-Version: 1.0' \
--header 'X-Request-ID: 1' \
--header 'X-Correlation-ID: 1' \
--header 'Content-Type: application/json' \
--data-raw '{
    "id":"ID Chiave Tecnica"
}'
```

Chiamata per generare il token:

```
curl --location --request POST 'https://b2b-auth-service-test.agyo.io/api/v3/tokens' \
--header 'accept: application/json' \
--header 'User-Agent: Postman' \
--header 'X-App-Name: TSxyz' \
--header 'X-App-Version: 1.0' \
--header 'X-Request-ID: 1' \
--header 'X-Correlation-ID: 1' \
--header 'Content-Type: application/json' \
--data-raw '{
    "id":"ID Chiave Tecnica",
    "digest":"sha256(sha256(ID + secret) + nonce)"
}'
```

> **Scadenza Token**
> Il token generato tramite le chiavi tecniche non ha scadenza.
> Se vengono effettuate però modifiche sulla chiave tecnica il token potrebbe invalidarsi.
> A quel punto è necessario fare un refresh della chiamata.

Per verificare che il token sia valido c'è una chiamata apposita: https://b2b-auth-service-test.agyo.io/api/v3/verify

---

> **UUID**
> Per recuperare l'UUID invece bisogna effettuare la chiamata sottostante ed inserire il CF/P.iva dell'azienda nel parametro "*vatNumber*".

```
curl --location --request GET 'https://registry-read-test.agyo.io/api/v3/items?identifier.vatNumber=48548641546&packageType=BASE&pagination.itemsPerPage=10&pagination.pageNumber=0&identifier.taxRegion=IT' \
--header 'accept: application/json;charset=utf-8' \
--header 'User-Agent: Postman' \
--header 'X-App-Name: TSxyz' \
--header 'X-App-Version: 1.0' \
--header 'X-Request-ID: 1' \
--header 'X-Correlation-ID: 1' \
--header 'Authorization: Bearer ' \
--data-raw ''
```

Nella response poi, il parametro da prendere in considerazione è **"id"**.
Esempio:
image-1649080956843.png

Switchare da TEST a PRODUZIONE

Una volta effettuate tutte le prove sull'ambiente di test TS Digital si potrà passare all'ambiente di produzione.

Per effettuare questo switch bisogna:

- Eliminare il (-test) dall'endpoint delle chiamate.
  Esempio https://b2b-auth-service-test.agyo.io/api/v3/tokens --> https://b2b-auth-service-agyo.io/api/v3/tokens
- Generare il token con le chiavi tecniche dell'ambiente di produzione.

Errori durante le chiamate

Possibili errori che possono essere restituiti dalla response:

- **400 Bad Request** - Probabilmente c'è un errore nella struttura della chiamata. Controllare che tutti i tag del body, gli header e l'endpoint siano impostati nel modo corretto.
- **401 Unauthorized** - Probabilmente c'è un errore nel token generato. Controllare che ID e Secret siano corretti e fare un refresh della chiamata per generare un nuovo token.
- **403 Forbidden** - Probabilmente non si hanno i permessi necessari per poter effettuare quella chiamata.
  In questo caso bisogna verificare i permessi attributi alla chiave tecnica da portale, eventualmente aggiungerli e poi procedere con la generazione di un nuovo token.

> A breve verranno introdotti limiti/controlli sul numero di chiamate effettuabili in un arco temporale (da definire). In caso di sforamento dei tali limiti è necessario gestire il codice http 429 Too many Requests.

Revision #50
Created 2020-03-25 09:21:26 UTC by Zittino
Updated 2023-02-06 14:43:53 UTC by Luca Zilembo