API Servizi di Fatturazione Elettronica Agyo

Autenticazione

Documentazione tecnica

Ed. 1 - Maggio 2018

Informazioni documento

Versione	1.0
Autore	
Descrizione	Versione iniziale

Sommario

Introduzione

Lo scopo di questo documento è fornire la documentazione tecnica sui Web Services di Autenticazione esposti dall'hub B2B di TeamSystem.
Questo documento è rivolto agli utenti accreditati e registrati che vogliono gestire autenticazione tramite digest e token per poter comunicare correttamente con le API principali dell'hub B2B.

Tecnologia utilizzata

Le API sono realizzate utilizzando **Apache CXF** versione 3.1.4.

Il protocollo di scambio implementato è **SOAP 1.2**.

I Web Services implementati restituiscono i dettagli sull'interfaccia implementata se richiamati con il queryString "**?wsdl"**

Endpoint

I servizi esposti dall'hub in questo momento sono raggiungibili attraverso **https**.

Ambiente di test:

https://soap-b2b-auth-service-test.agyo.io/AuthApi_v1/AuthAp i.ws

Ambiente di produzione:

https://soap-b2b-auth-service.agyo.io/AuthApi_v1/AuthAp i.ws

Descrizione del servizio

Il servizio di autenticazione serve ad ottenere un token valido per la comunicazione diretta tra ERP e hub B2B. Il token attualmente non ha scadenza temporale ma può essere invalidato da un nuovo processo di ottenimento oppure da un cambio sulle autorizzazioni di quello esistente generate dall'utente o dall'hub stesso.
Le credenziali da utilizzare sono quelle chiamate "**credenziali tecniche**" ottenute via email all'atto dell'iscrizione e validazione dell'azienda oppure generate attraverso la sezione "Applicativi" del portale.

Operations

Operation *getNonce*:

Ritorna un codice, il nonce, da utilizzare per la generazione del digest. Tale digest è generato secondo la formula:

- Digest = **SHA256**(**SHA256**(*LowerCase*(id) + password) + nonce)

Input : ***getNonce***

Nome	Tipo	Descrizione
Id	String	Identificativo dell'utenza

Output: ***getNonceResponse***

Nome	Tipo	Descrizione
nonce	String	Nonce di autenticazione

Operation verifyDigest:

Verifica il digest costruito dal client sulla base del nonce ottenuto dalla chiamata precedente. Restituisce un token da utilizzare nelle successive chiamate alle api, che richiedono una utenza attiva per poter essere eseguite.

Input : ***verifyDigest***

Nome	Tipo	Descrizione
Id	String	Identificativo dell'utenza
digest	String	digest da controllare

Output: ***verifyDigestResponse***

Nome	Tipo	Descrizione
token	String	token da utilizzare nelle chiamate alle api

Operation verifyToken:

Verifica che il token associato all'utenza sia valido. Operation usata dalle altre api per potere verificare l'esistenza e l'attivazione dell'utente richiedente. Ritorna risposta vuota in caso di esito positivo oppure uno dei fault dichiarati.

Input : ***verifyToken***

Nome	Tipo	Descrizione

token	String	token da verificare

Gestione degli errori

In caso di errore il servizio invia al client una risposta di tipo fault conforme allo standard SOAP 1.2 in cui sono previsti due nodi, Code e Reason. Questo tipo di errore nel caso del servizio di Authentication è rialzato dall'infrastruttura in automatico e rientra negli errori tecnici.

Per gli errori applicativi tutte le operation esposte dal servizio sollevano un tipo di errore:

- AuthenticationException

Gli errori sono definiti come:

Nome	Tipo	Descrizione
code	String	Codice dell'errore
message	String	Messaggio descrittivo

Elenco errori

Code	Message
400	Bad request. Richiesta non valida
401	Unauthorized. Utenza non autorizzata
403	Forbidden. Accesso negato
404	Not found. Utenza non trovata
500	Internal server error. Errore generico
502	Bad gateway. Errore di comunicazione layer SOAP con layer Thrift