Dedalus
HEALTHCARE SYSTEMS GROUP

D-four

PROGETTO COVID-19

PATIENT SYNOPTIC – Apertura in contesto

STORICO REVISIONI

Revisione	Data	Note
1.0.0	20/04/2020	Prima versione

Sommario

Sommario 3
PATIENT SYNOPTIC – Introduzione 4
Chiamata in contesto 4
Transazioni 4
AUTH - Authentication 4
AUTH-001: Get Token By Credentials 5
AUTH-006: Enrich Token with Context 6
CTX - Context Sharing 6
CTX-001: Launch Web Component with Context Transfer 6
Workflow e parametri supportati 7

PATIENT SYNOPTIC – Introduzione

Il PATIENT SYNOPTIC in seguito definito PATSYN è il visualizzatore della soluzione COVID-19. Consente attraverso una prospettiva definita “dashboard” la visualizzazione aggregata delle informazioni salienti relative allo stato clinico del paziente. Di seguito una schermata esemplificativa:

Figura 1- "Dashboard" del Patient Synoptic

Chiamata in contesto

Il modulo PATSYN può essere chiamato in contesto da un’applicazione esterna. In questo modo è possibile accedere ad una specifica configurazione della “dashboard” senza effettuare la ricerca del paziente. Per ottenere questo risultato è necessario che l’applicativo chiamante condivida l’identificativo anagrafico del paziente e che sia in possesso di un token di autenticazione in grado di identificare l’operatore sanitario che sta lavorando sull’applicativo chiamante. Per ottenere il token è necessario essere in possesso di credenziali sul sistema centrale di autenticazione.

Nel paragrafo che segue sono definite le specifiche e le transazioni necessarie per effettuare la chiamata in oggetto verso il modulo PATSYN.

Transazioni

AUTH - Authentication

Authentication Client

“Authentication client” identifica un qualsiasi client che deve eseguire l'autenticazione prima di utilizzare un servizio o un’interfaccia utente. Il client può essere di due eventuali tipologie:

- “Web authentication client”: questo tipo di client viene eseguito in un browser, ed è così in grado di effettuare l’autenticazione con un single sign-on basato sul web;
- “Desktop authentication client”: questo tipo di client viene eseguito su un processo dedicato all’interno del sistema operativo e non può utilizzare il single sign-on basato sul web.

Authentication Manager

Questo componente gestisce l'autenticazione di altri componenti, la creazione e il ciclo di vita dei token. Fornisce un livello di astrazione per l'autenticazione e l'autorizzazione, tramite l'integrazione con una **Identity Provider** e una anagrafe degli operatori è in grado di convalidare le credenziali, recuperare i ruoli e generare token.

AUTH-001: Get Token By Credentials

Questa transazione consente ad un client (**Authentication Client**) di recuperare un access token da un authentication manager, fornendo un set di credenziali (nome utente e password) come input. L’authentication manager si integra con un identity provider per verificare l'autenticazione e successivamente l’anagrafica degli operatori (Attribute Authority) per recuperare i ruoli.

Una volta verificata l'autenticazione e recuperato l'elenco dei ruoli, l’authentication manager li restituisce al client come parte della risposta http creando un access token JWT e un “refresh token” che successivamente può essere utilizzato per rinnovare l’access token.

Il diagramma seguente riepiloga la transazione completa:

Figura 2- Schema AUTH-001

AUTH-006: Enrich Token with Context

Questa transazione viene utilizzata da un client che ha già effettuato l'autenticazione per ottenere un "ID Token". L'ID Token viene fornito dall'Authentication Manager a partire da un Access Token che viene arricchito con le informazioni di contesto passate dal client.

Il diagramma seguente riepiloga la transazione:

Figura 3 - Schema AUTH-006

CTX - Context Sharing

Context Provider

L'applicativo che esegue il passaggio di contesto verso un "context receiver".

Context Receiver

L'applicativo destinatario del passaggio di contesto da parte del "context provider".

CTX-001: Launch Web Component with Context Transfer

Con questa transazione un applicativo client (**Context Provider**) effettua la chiamata all'applicativo che desidera aprire in contesto (**Context Receiver**). Il metodo utilizzato è HTTP GET e tutte le informazioni di contesto necessarie al servizio chiamato vengono passate attraverso un parametro in queryString all'interno dell'ID Token.

Questa transazione prevede che, prima di effettuare la chiamata all'applicazione che si desidera aprire in contesto, l'applicativo client abbia ottenuto dall'Authentication Manager un ID Token. Il seguente diagramma riepiloga la transazione:

Figura 4 - Schema CTX-001

Workflow e parametri supportati

Per maggior dettagli tecnici sulle transazioni AUTH si faccia riferimento al file OpenAPI/Swagger "auth_manager.yaml contenuto nell'allegato PATSYN_CTX.zip.

Di seguito il workflow delle transazioni con il dettaglio dei parametri necessari per effettuare l'autenticazione e la chiamata in contesto verso il PatientSynoptic.

AUTH-001

- *client_id:* identificativo dell'applicativo che intende effettuare la chiamata in contesto. Ogni applicativo deve essere censito sul Authentication Manager. Tale identificativo sarà fornito in fase di test e produzione;
- *credenziali*: username e password che l'utente deve utilizzare nella chiamata all'Authentication Manager per ottenere il token JWT di autenticazione (Access Token). (Da inserire nell'Authorization header);

AUTH-006

- *client_id:* identificativo dell'applicativo che intende effettuare la chiamata in contesto
- *access Token:* è il token JWT ritornato dall'autenticazione effettuata con la transazione AUTH-001. (Da inserire nell'Authorization header);
- *context:* è un file JSON contenente tutti gli elementi che l'applicativo client intende passare al PATSYN nella apertura in contesto. Tale oggetto deve essere inserito all'interno del parametro *selfextensions.* Di seguito un dettaglio della struttura relativa a *context*:

Elemento	Tipo	Descrizione

key	string	Identificatore univoco dell'elemento di contesto	
resource	array of object	Elemento da condividere	
resource.resourceType	string	Tipologia dell'elemento da condividere	
resource.id	string	Id relativo all'istanza dell'elemento da condividere.	Rappresenta un valore assoluto valido all'interno dell'integrazione.
resource.identifier	array of objects	Identificativo relativo all'elemento da condividere	

Per il PATSYN sono supportate le seguenti *key*:

key	resource.resourceType	resource.id	resource.identifier
currentPatient	Patient	N/A	value= Codice fiscale assistito System= "urn:oid:2.16.840.1.113883.2.9.4.3.2"
clinicalUseCase	ClinicalUseCase	COVID-19; HLCM	
action	Action	Fisso a "dashboard"	

CTX-001

Di seguito un esempio di URL:

http://[PATSYN_URL]?token=[IDToken]&locale=it-IT

e di seguito i parametri da utilizzare per la chiamata verso il PATSYN:

- token: contiene l'ID Token JWT ottenuto con transazione AUTH-006;
- locale: la lingua da utilizzare nel PATSYN, eg.: it-IT.