FSE 2.0 – ACCREDITAMENTO AL GATEWAY
Invocazione Gateway ambiente di accreditamento

Settembre 2023

REGIONE CAMPANIA

Invocazione Gateway
Ambiente di accreditamento

La nuova architettura del FSE prevede la presenza di un componente, denominato Gateway, adibito all'acquisizione, alla validazione, e alla traduzione di dati e documenti clinici secondo i formati definiti dalle Linee Guida FSE. Tali dati e documenti sono prodotti dai Sistemi in uso presso le Strutture Sanitarie.
Per poter inviare i dati in ambiente di produzione è necessario che gli applicativi software superino la fase di accreditamento.
Queste slide hanno lo scopo di dare indicazioni utili alle Software House sull'utilizzo dei tool messi a disposizione dal Ministero della Salute per la fase di verifica di invocazione dei servizi.
In particolare, saranno illustrati i seguenti step:

- Generazione del token JWT necessario ad invocare i servizi
- Generazione del PDF con CDA2 iniettato
- Invocazione dei servizi del Gateway

Invocazione Gateway
Ambiente di accreditamento

Per poter utilizzare il servizio di validazione finalizzato alla fase di Test Cases del processo di accreditamento, occorrerà richiamare il seguente endpoint
https://modipa-val.fse.salute.gov.it/govway/rest/in/FSE/gateway/v1/documents/validation
Il servizio di Validazione è correlato da un identificativo di transazione referenziato nel documento come "workflowInstanceId" secondo standard IHE.
Lo scopo di questa API è validare da un punto di vista sintattico, semantico e terminologico i dati forniti dal Sistema Produttore.
Il servizio è sincrono e, in caso di un esito con errore, verranno restituiti i dettagli di questo indicati nell'apposita sezione in "Response".

In caso di validazione eseguita con successo, l'esito tornato è positivo e la Validazione può ritenersi conclusa correttamente.
L'hash del documento CDA2 verrà salvato in cache con chiave "workflowInstanceId". In risposta verrà ritornato l'identificativo "workflowInstanceId".

Invocazione Gateway
Ambiente di accreditamento

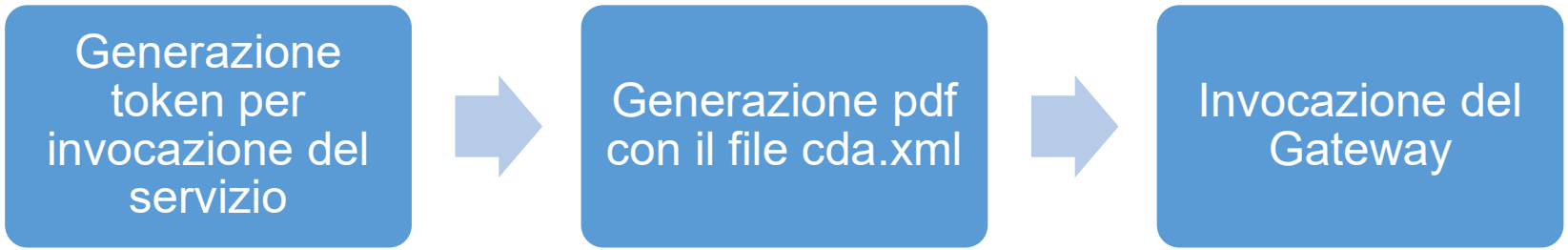
Per comunicare con il gateway è necessario essere in possesso di due certificati X.509 e delle rispettive chiavi private, ottenuto durante il primo step del processo di accreditamento.
Il certificato denominato di “autenticazione” viene utilizzato unicamente come certificato client per le chiamate https.
Il certificato denominato di “signature” viene utilizzato unicamente per la firma dei token JWT.

Ogni invocazione delle API avverrà quindi con una chiamata https protetta dal certificato di autenticazione e conterrà negli header due token JWT.
Il primo JWT è utilizzato per l’autenticazione e contiene i riferimenti all’utente che richiama il servizio e al soggetto interessato, il token viene trasportato nell’header “Authorization” di tipo “Bearer”
Il secondo JWT è di “signature” e contiene rifermenti al documento oggetto delle operazioni.
Entrambi i token devono essere firmati utilizzando il certificato “signature”.

Vista la dipendenza dei token dai valori specifici di utente/soggetto/documento è necessario generare nuovi JWT per ogni chiamata alle API.

Invocazione Gateway
Ambiente di accreditamento

Il processo di invocazione del servizio di validazione può essere suddiviso in tre passi



Grazie

REGIONE CAMPANIA