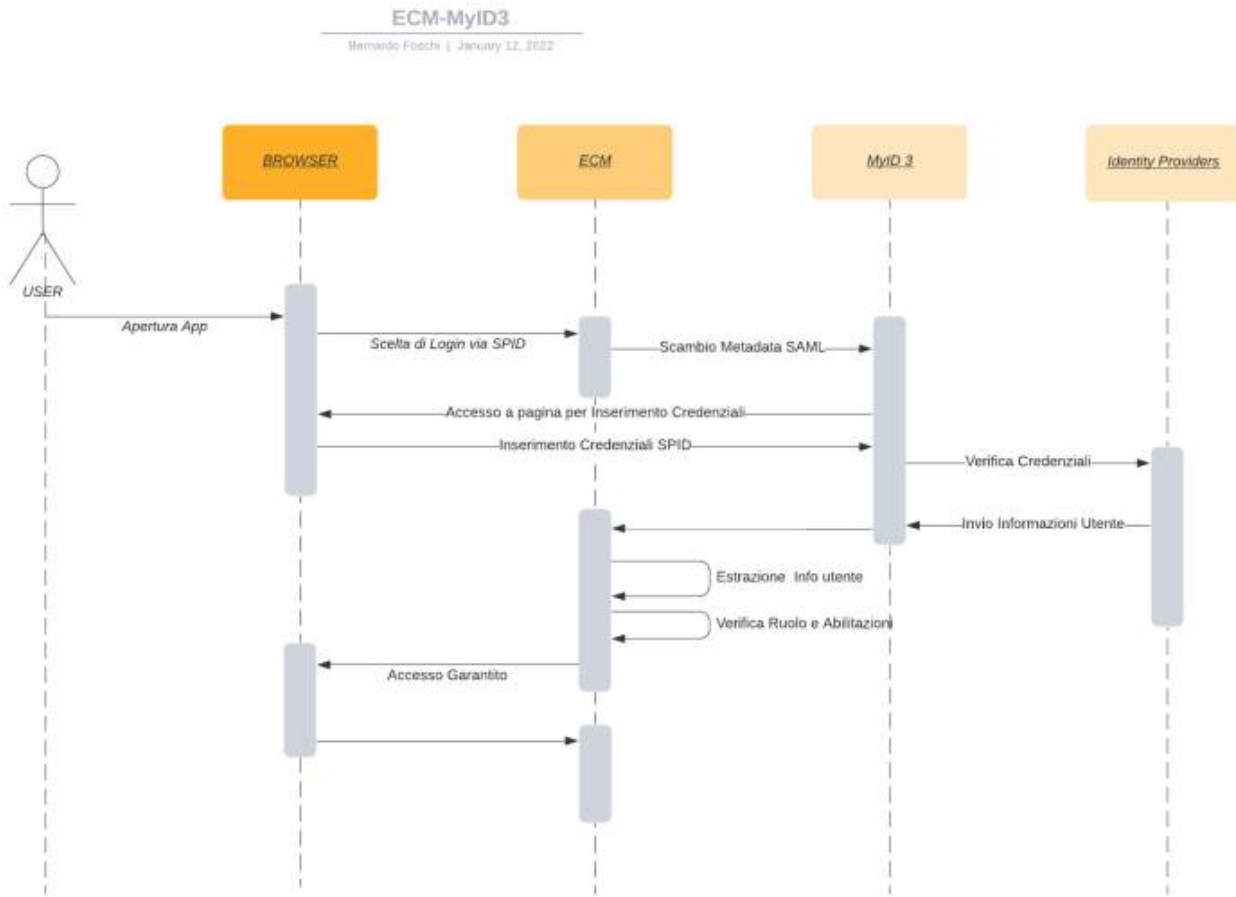


E.C.M. - Area Riservata

Integrazione Federa MyID3

Le modalita di login all'applicativo sono state estese inserendo il supporto per lo SPID, attraverso l'integrazione di MyID3. MyID3 è un applicazione web indipendente adottata dalla Regione Veneto che si occupa di accentrare in un unico pagina web diverse modalita di login ai servizi dell'ente, tra le quali la modalita SPID per tutti gli IdentityProvider (IDP) accettati dallo stesso.

L'autenticazione tramite MyID3 prevede lo scambio di informazioni tra i diverse entità: l'applicativo ECM, MyID3, l'IdentityProvider selezionato. Tale scambio è riassunto in pochi passaggi dal seguente schema.



USER INTERFACE

Al livello utente l'unica modifica richiesta è stata l'aggiunta di un pulsante "Accedi Con SPID" per il passaggio al dominio di MyID3. Ad avvenuto riconoscimento delle credenziali l'utente viene automaticamente reindirizzato all'applicativo.



TECHNICAL INFO

L'integrazione del servizio offerto avviene tramite il protocollo SAML2.

L'attivazione del protocollo e delle funzionalità di integrazione dipendono dalla chiave di properties

- authenticationType=saml

Una volta attivata è necessario fornire le relative chiavi di configurazione nel medesimo file di properties:

CONFIGURAZIONE SAML

1. saml.relayStateUrl=<https://ecm.3di.it/saml/metadata>
2. saml.targetUrl=/home
3. saml.failureUrl=/error
4. saml.logoutUrl=/logout
5. saml.keystorePath=/saml/
6. saml.keystoreFileName=ecmKeystore.jks
7. saml.keystoreAlias=ecmalias
8. saml.keystorePassword=ecmKeystorePassword
9. saml.local.metadata.path=/saml/metadataFromIdp.xml
10. saml.idpMetadataURL=<https://myid.collaudo.regione.veneto.it/gw/metadata>
11. saml.idpEntityId=<https://myid.collaudo.regione.veneto.it/gw/metadata>
12. saml.spidIdentifyingAttribute=spidCode
13. saml.identifyingAttribute=CodiceFiscale
14. saml.signingAlgorithm=<http://www.w3.org/2001/04/xmldsig-more#rsa-sha256>

Importante : saml.idpMetadataURL -> indica l'url pubblico a cui MyID3 espone il suo metadata, dovrà essere aggiornato in base agli ambienti di Collaudo/Produzione saml.idpEntityId -> è stato ricavato dal metadata sudetto. saml.identifyingAttribute -> è l'attributo identificativo univoco che viene estratto dall'info sull'utente inviate da MyID e utilizzato per ricercare l'utenza nei DB ECM.

Per la configurazione è necessario generare anche un keystore che verrà utilizzato per cifrare le comunicazioni tra idp e sp, di seguito un esempio di codice per la generazione:

```
keytool -genkeypair -alias ecmalias -keypass ecmKeystorePassword -keystore ecmKeystore.jks -keysize 2048 -keyalg RSA
```

Importante : il file così generato andrà copiato nel path indicato dalla chiave *saml.keystorePath* all'interno del progetto.