Autenticazione

L'utente ESSE3 può essere autenticato in diverse modalità:

- sfruttando le credenziali registrate nella anagrafica utenti di ESSE3
- utilizzando le informazioni memorizzate in un server LDAP (OpenLDAP, Microsoft Active Directory), avendo in questo caso anche la possibilità di abilitare la gestione multi-profilo
- delegando l'autenticazione ad un sistema esterno (identity provider, opzione supportata al momento solo per il modulo WebESSE3), ad esempio Shibboleth

Il prerequisito che deve essere soddisfatto in tutti i casi è la presenza dello USER_ID nella anagrafica utenti di ESSE3, informazione dalla quale è possibile determinare la modalità con cui deve essere portata a termine l'operazione di autenticazione: la modalità di autenticazione può essere indicata sul gruppo a cui appartiene l'utente o, per casi specifici o di test, sull'anagrafica dell'utente.

Il processo di autenticazione verifica che le credenziali fornite non siano scadute (o da rinnovare) e che l'utenza non sia stata, per qualche ragione, disattivata: in questa fase viene anche verificata la presenza di alias con cui risalire all'effettivo USER_ID da utilizzare per accedere al sistema.

ESSE3

Il processo di autenticazione prevede la verifica della password fornita dall'utente, eventualmente memorizzata nella base dati utilizzando uno degli algoritmi di crypt supportati (MD5, SHA-1 e UNIXCRYPT per citarne alcuni).

LDAP

Il processo di autenticazione prevede:

- l'accesso al server LDAP configurato con una utenza "admin" che abbia i privilegi di ricerca e di lettura
- la ricerca della entry associata all'utenza fornita, al fine di determinare il DN dell'utente da autenticare
- il tentativo di accesso al server LDAP con il DN individuato e la password fornita

Il server LDAP utilizzato dal processo di autenticazione viene indicato attraverso alcuni parametri di configurazione; gli stessi parametri possono essere ridefiniti per i diversi gruppi di utenti da autenticare tramite un LDAP: in questo modo è quindi possibile autenticare, se richiesto dalla infrastruttura di rete già prevista in Ateneo, i docenti su un sistema Active Directory e gli studenti su un OpenLDAP.

Multi-profilo

Se un utente è censito in più gruppi, è possibile configurare ESSE3 affinché l'utente possa scegliere il profilo con cui accedere al sistema.

Le credenziali fornite vengono validate dal server LDAP configurato: per questioni di sicurezza, si è preferito imporre questo vincolo nella implementazione del servizio di autenticazione. Se l'utente è stato correttamente autenticato, ESSE3 propone la lista dei gruppi in cui è censito, per permetterne la selezione e consentire l'accesso al sistema.

L'autenticazione in modalità multi-profilo può essere attivata per tutte le tipologie di utenti: può quindi essere utilizzata per autenticare sia gli utenti di Segreteria che gli utenti web.

Esterna (identity provider)

Il processo di autenticazione è demandato al sistema esterno configurato (Shibboleth o sistema analogo, capace di fornire gli estremi dell'utente autenticato tramite il canale HTTP). In questo caso, ESSE3 assume come già autenticato l'utente per cui riceve la richiesta di accesso alle risorse protette (path ***/auth/***), limitandosi ad eseguire i soli controlli preliminari sopra indicati e necessari ad eseguire la login applicativa, operazione necessaria alla interazione con il sistema.

Processo - **Autenticazione e autorizzazione**

Visibilita -