ALLEGATO C AL CAPITOLATO TECNICO

SPECIFICHE TECNICHE PER L'UTILIZZO DEL SISTEMA DI AUTENTICAZIONE FEDERATA (FEDERA)

1 Considerazioni generali

Questo documento ha lo scopo di descrivere l'integrazione delle applicazioni ospitate sulle infrastrutture della Regione Emilia-Romagna con il sistema di autenticazione federata.(fedERa).
Il sistema di autenticazione federata (fedERa) permette a utenti e cittadini di un Ente di accedere ai servizi online erogati dagli Enti della Regione Emilia-Romagna, utilizzando le credenziali rilasciate dall'ente di appartenenza. FedERa orchestra il colloquio tra i gestori federati delle identità digitali dei cittadini: i portali web aderenti alla federazione che utilizzano tali contenitori di identità digitali garantiranno l'accesso ai propri servizi con l'introduzione di una sola credenziale di autenticazione, cioè di una coppia utente/password in modalità single sign on.
I servizi offerti da FedERa sono:

- Identity Manager: gestisce la procedura di rilascio delle credenziali;
- Identity Provider: mette a disposizione un contenitore di identità digitali per i cittadini;
- Identity Gateway: consente la comunicazione tra diversi IdP e i vari servizi online aderenti alla federazione.

Ulterioni informazioni sul funzionamento di FedERa sono disponibili all'url: http://federazione.lepida.it/

2 Accesso alle applicazioni Federate attraverso il service provider della Regione Emilia-Romagna

Per rendere più semplice per le proprie applicazioni l'utilizzo dell'autenticazione federata, la Regione Emilia-Romagna si è dotata di service provider integrato con fedERa, che funge da gateway fra le singole applicazioni e l'Identity Gateway di FedERa.
Per poter accedere ad una Web Application Federata protetta da un sistema di Web SSO, l'utente deve prima aver effettuato il Logon al sistema di autenticazione del proprio gestore di identità (il proprio ente o l'IdP di Federa).
Effettuato il Logon Primario sul proprio gestore dell'Identità, attraverso il sistema fedERa l'utente può accedere alle Web Application federate esposte dal service provider della Regione Emilia Romagna.

Per le richieste di accesso per le quali viene effettuato l'enforcing (almeno la pagina di login su FedERa) vengono ripetuti i seguenti passi:

1. La richiesta viene intercettata dal Reverse Proxy.
2. L'Agent del Reverse Proxy verifica la presenza di una sessione autenticata per l'utente. Per il mantenimento della sessione viene utilizzato un cookie volatile sul client. Nel caso non esista una sessione associata alla richiesta, l'utente viene diretto sul portale federa dove l'utente sceglie il proprio Gestore dell'Identità, e viene rediretto verso il modulo di autenticazione del sistema di autenticazione del Gestore dell'Identità scelto.
3. Il Gestore dell'identità autentica l'utente e restituisce le informazioni all'Agent che a sua volta trasmette le informazioni necessarie alla web application dell'aderente utilizzando l'header http.

2.1 Requisiti di progettazione delle interfacce

Il passaggio dei parametri tra il reverse proxy e l'applicazione avviene sfruttando i meccanismi standard del Web e cioè gli header del protocollo HTTP, quindi la Web Application deve essere in grado di gestire gli header HTTP.
Nel caso in cui l'applicazione voglia filtrare ulteriormente gli accessi può prelevare gli attributi dell'utente dall'http header ed effettuare la profilazione applicativa.

2.2 Formato parametri

I parametri passati nell'header HTTP alla web application esposta servono ad identificare ed a caratterizzare l'originatore della richiesta.
I principali parametri presenti nell'header HTTP sono:

Parametro	Significato
codicefiscale	Identificativo utente (identifica l'originatore della richiesta)
firstname	Identificativo nome utente
lastname	Identificativo cognome utente
Email	Identificativo indirizzo mail utente
trustlevel	Identitificativo livello di affidabilità utente
policylevel	Identitificativo livello di affidabilità della password utente
authenticatingauthority	Ente che ha effettuato l'autenticazione/riconoscimento dell'utente
authentication method	Modalità di autenticazione dell'utente: password, smartcard, ecc.

Il parametro codicefiscale è presente nell'header HTTP di ogni richiesta. La presenza degli altri parametri dipende dal gestore di identità sul quale l'utente si è autenticato. I parametri trustlevel e policylevel possono assumere i seguenti valori:

- Alto
- Medio
- Basso

Per il parametro trustlevel, Basso significa utenti che si sono registrati online, Medio utenti che si sono registrati online con prova del possesso di un numero di cellulare ed Alto utenti che hanno effettuato la registrazione con riconoscimento de-visu. Per il parametro policylevel Basso significa nessuna password policy, Medio significa password policy adatta alla lettura di dati personali ed Alto significa password policy adatta all'accesso a dati sensibili.
Un utente che si autentica con smartcard direttamente sull'Identity gateway di fedERa senza passare da un IdP non avrà valorizzati gli attributi trustlevel e policylevel, ma avrà l'attributo authenticatiomethod valorizzato a "smartcard".
Nel caso in cui gli attributi non siano valorizzati sono da considerare con livello Basso. Gli utenti dell'ente Regione Emilia Romagna avranno un livello di affidabilità alto sia per quanto riguarda il policylevel che il trustlevel.

La modalità di accesso alle variabili dell'header sono legate al linguaggio utilizzato per la creazione e la gestione delle pagine web.

2.3 Vincoli

Sono riportati di seguito i vincoli a cui le Web Application devono attenersi per poter essere protette dal sistema di Web SSO.

2.3.1 Identificazione e Autenticazione dell'utente

La web application esposta non deve richiedere il login agli utenti che accedono attraverso autenticazione federata, in quanto il processo di identificazione e autenticazione viene già effettuato nella fase di Logon Primario che l'utente effettua sul proprio gestore delle identità. In particolare, l'applicazione non deve richiedere l'immissione esplicita da parte dell'utente di un username e di una password, ma può utilizzare le informazioni di identificazione dell'utente contenute nell'header HTTP di ogni richiesta.

E' possibile per le applicazioni, in base a specifiche esigenze, utilizzare in parallelo all'autenticazione federata, anche altri metodi (es. user/password, openId, ecc.). A tale proposito si veda il paragrafo 3.4.2. Autorizzazione dell'utente
L'applicazione dovrà gestire l'autorizzazione, poiché tutti gli utenti autenticati da un ente partecipante alla federation avranno accesso alle applicazioni esposte dal service provider della Regione Emilia Romagna, indipendentemente dal trust level o dal policy level assegnato all'utente.
L'applicazione potrà utilizzare le informazioni contenute nell'header HTTP, quali il trust level o il policy level per realizzare specifiche regole di autorizzazione locali.

2.3.2 Uso di Cookie

Il meccanismo di Logon e le verifiche effettuate dal Reverse Proxy si basano sullo scambio di *cookie* con la Postazione di Lavoro dell'utente che necessariamente deve permettere l'utilizzo di *cookie*.

2.4 Modalità di esposizione

2.4.1 Esposizione dell'intera applicazione attraverso Reverse Proxy

2.4.1.1 Convenzione sui nomi dei domini

Una web application esposta dalla RER potrà essere accessibile, sia da Internet che dalla rete interna, mediante una URL così strutturata:

https://<dominio>/<*percorso-applicazione*>/

dove <percorso-applicazione> è il path (al limite costituito da un singolo nome) scelto per identificare la web application (è ammesso il passaggio di parametri nella URL) e <dominio> è il nome con il quale l'applicazione viene pubblicata, di solito servizifederati.regione.emilia-romagna.it.

2.4.1.2 Convenzioni sui nomi delle web application

Qualora un servizio esponga più di una web application, gli URL corrispondenti si differenziano solo relativamente alla componente <*percorso applicazione*>.
Esempio:

https://<dominio>/<percorso applicazione -1>/

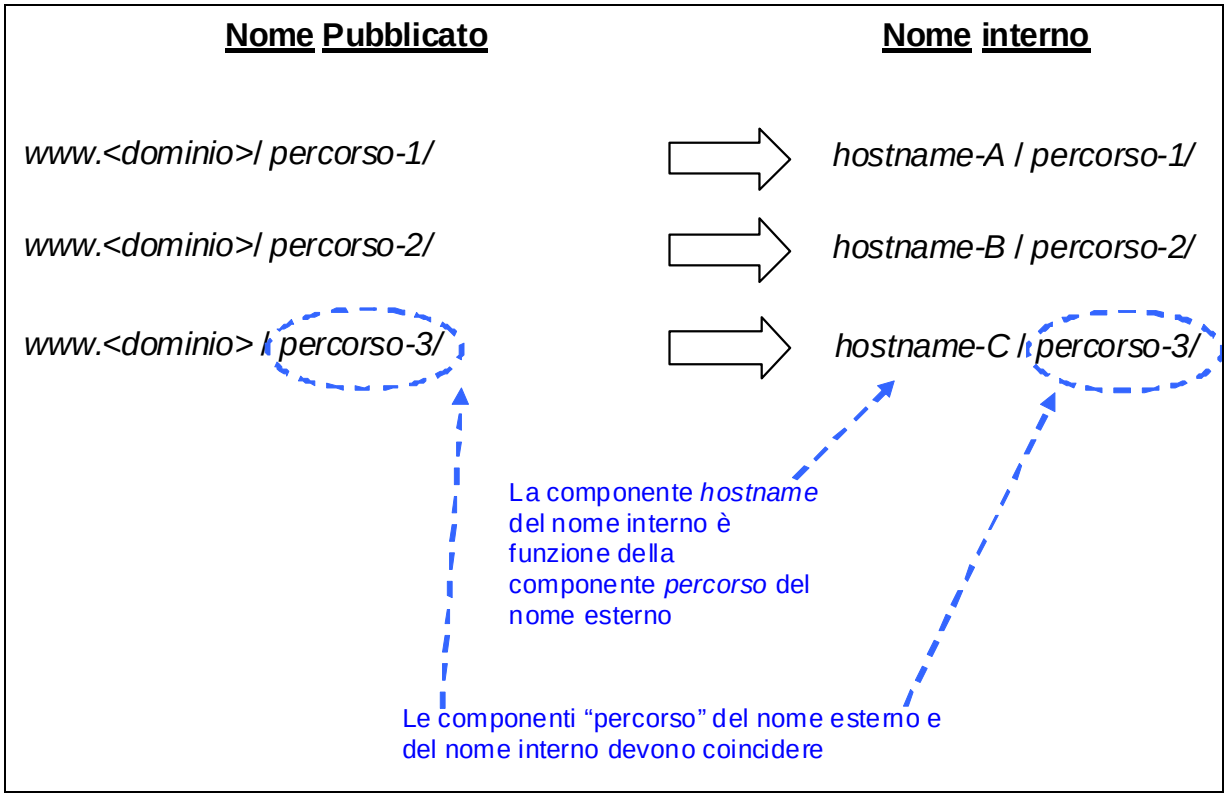
https://<dominio>/<percorso applicazione -2>/

https://<dominio><percorso applicazione -3>/

2.4.1.3 Regole d'instradamento del Reverse Proxy

La convenzione sui nomi degli URL si riferisce all'esposizione delle web application, ovvero al modo in cui tali applicazioni sono esposte tramite Reverse Proxy e non implica che la medesima convenzione debba necessariamente essere adottata internamente all'applicativo.
Internamente all'applicativo, le web application possono risiedere su uno o più host. La corrispondenza tra il "nome esterno" e il "nome interno" dell'applicazione viene effettuata dal Reverse Proxy tramite le *regole di instradamento*. Tali regole consentono di collocare le proprie web application sui server della rete interna, svincolandosi dall'*hostname* con cui sono visibili.
Nell'instradamento, il path dell'applicazione (cioè la porzione dell'URL che viene dopo l'*hostname*) del "nome esterno" deve coincidere con il path del "nome interno".

La figura seguente rappresenta le regole suddette:



E' ammesso il passaggio di parametri nell'URL, se previsto dalla web application, mentre non è ammesso utilizzare i parametri per identificare la web application esposta.

Esempio di utilizzo di URL non è ammesso:
https:// www.<dominio>/entrypoint?applicazione=applicazione1

2.4.1.4 Accessibilità dell'applicazione tramite proxy

Si descrivono di seguito i vincoli che la web application dell'Aderente deve rispettare per poter essere esposta attraverso il Reverse Proxy (requisiti di *proxability*).
Laweb application da esporre non deve contenere riferimenti assoluti alle proprie risorse, ma solo puntamenti relativi.
In altri termini le eventuali risorse referenziate all'interno dell'applicazione (quali., ad esempio, immagini o link ad altre pagine) devono essere indirizzate tramite **URL relativi**, ovvero URL in cui viene esplicitata solamente la componente *path* senza le componenti *protocollo* ed *hostname*. Oltre agli URL anche **i PATH devono essere relativi**, ovvero non devono iniziare con il carattere "/".

Ad esempio:

URL ASSOLUTI (NON UTILIZZABILI)	**URL RELATIVI (DA UTILIZZARE)**
http(s)://hostname/logo.gif	logo.gif
http(s)://hostname/subdir1/index.html	subdir1/index.html **NOTA :** non è possible utilizzare URL relativi del tipo /subdir1/index.html, i quali, pur essendo URL relativi (non vengono infatti indicati protocollo ed hostname), sono comunque PATH assoluti.

Inoltre, ogni singola Web Application deve prevedere un unico punto di ingresso da cui si diramano i diversi sottoservizi.
Non sono quindi consentiti collegamenti a sottoservizi non appartenenti all'albero che ha come radice la URL di ingresso della Web Application: ad esempio, supponendo che l'URL di "ingresso" della Web Application *sia* ***http(s)://hostnameX/directoryY***, non è consentito il collegamento a pagine che non risiedano sotto il path

directoryY quali ***http(s)://hostnameX/directoryZ/pageJ.jsp*** (sempre che l'applicazione che ha come "ingresso" della WebApplication l'URL ***http(s)://hostnameX/directoryZ*** non sia stata esposta a sua volta).

2.4.2 Esposizione dietro Reverse Proxy della sola pagina di login

Questo tipo di soluzione prevede la protezione della sola pagina di login dell'autenticazione federata, permettendo così di utilizzare in parallelo all'autenticazione federata, anche altri metodi (es. user/password, openId, ecc.). In particolare, per l'autenticazione federata, l'applicazione deve esporre una pagina di login che gestisca il riconoscimento dell'utente tramite gli attributi presenti nell'header http, creando poi una sessione applicativa che permetta all'utente la navigazione all'interno dell'applicazione, L'applicazione indirizza a tale pagina l'utente che non abbia una sessione valida.
La pagina di login sopra descritta non deve essere accessibile direttamente, ma deve essere esposta solo attraverso Reverse Proxy. A tale proposito si veda il paragrafo 3.5 Sicurezza.
Il sistema di Single Sign On regionale viene configurato per proteggere la sola pagina di login e non si preoccupa di effettuare il controllo sulle restanti risorse dell'applicazione.
Ulteriori dettagli o approfondimenti legati alla particolarità della singola applicazione verranno definiti in fase di integrazione.

2.5 Sicurezza

Ogni applicazione dovrà accettare, per le richieste di accesso per le quali viene effettuato l'enforcing, solo le richieste pervenute dal reverse proxy. Il controllo dovrà essere effettuato mediante un meccanismo di autenticazione con certificato client. Il certificato pubblico del reverse proxy verrà installato sui server sulle quali è installata l'applicazione e l'applicazione, l'application server o il web server dovranno essere configurati in modo da concedere l'accesso all'applicazione solo se il certificato client viene riconosciuto essere quello del reverse proxy. Nel caso questo non fosse possibile occorrerà verificare, a livello applicativo e, ove possibile, a livello sistemistico (con un firewall o sul web server) che le richieste provengano dall'ip del reverse proxy. L'applicazione dovrà riconoscere l'utente, tramite i parametri passati nell'http Header, solo nel caso la richiesta gli venga inoltrata dal reverse proxy, in tutti gli altri casi l'applicazione non dovrà permettere l'accesso all'utente.

2.5.1 Gestione del logout applicativo

L'applicazione non si preoccuperà di gestire il logout, non sarà presente nessun link/pulsante di logout.

2.5.2 Definizione delle regole di autorizzazione

Le regole di autorizzazione da parte dell'applicazione possono essere definite in base alle informazioni contenute nell'header http, oppure in un database locale.

1. Header http:
   L'applicazione può discriminare l'accesso in base ai valori contenuti negli attributi trustlevel e policylevel. Gli attributi vengono valorizzati (Vedi paragrafo 4.2) in base al livello di affidabilità dell'utenza.

2. Profilazione Locale:
   Ogni applicazione gestisce un proprio database dove vengono memorizzati specifici profili autorizzativi relativi agli utenti. In questo caso l'utente deve essere prima profilato per poter accedere all'applicazione. Per la gestione ed il provisioning dell'utente è possibile utilizzare il sistema di Identity Management (rimandiamo al capitolo 2 di questo documento).