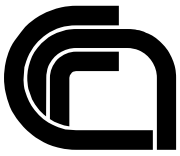

Consiglio Nazionale delle Ricerche

Accesso Wi-Fi federato dell'Area della Ricerca di Pisa WiFi@PiCNR

A. Gebrehiwot, A. De Vita

IIT TR-01/2011

Technical report

Gennaio 2011

Istituto di Informatica e Telematica

Accesso Wi-Fi federato dell'Area della Ricerca di Pisa

WiFi@PiCNR

Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche

a cura di: Ing. Abraham Gebrehiwot
dott. Andrea De Vita

reparto: Rete Telematica del CNR di Pisa
Via G. Moruzzi 1
56124, Pisa

abraham.gebrehiwot@iit.cnr.it
tel: +39-050-3152079
andrea.devita@iit.cnr.it
tel: +39-050-3158329

Rapporto Tecnico
Gennaio 2011

Sommario

Abstract:

English:

The *CNR Research Area of Pisa* has a Wi-FI coverage in the campus. The wireless network is designed and implemented by the Institute of Informatics and Telematics of CNR which is in charge of managing the network infrastructure and also providing a number of other services to researchers in the campus. The wireless network is a centralized solution based on Cisco Wireless LAN Controller (WLC).

In the campus area various wireless networks are defined, including the SSID "guest" with a Captive Portal authentication. The goal of this document is to describe the software solution developed for accessing the “guest” network using the distributed federated Web Single Sign On authentication and authorization infrastructure called *IDEM*. IDEM is an acronym of *Authentication and Authorization **Ide**ntity **M**anagement of the GARR Network*. At this time, beginning of 2011, the federation has reached the potential of 3 milion users and is rapidly growing. The federation users can now access the “guest” network using their home organization credentials.

The vision of providing local access credentials based on home organization credentials is known as ***account linking*** and involves trust relationship between the participating organizations. The account linking solution can easily be adopted to extend the management of user credentials of any network service that use standard authentication mechanisms, such as RADIUS, LDAP, etc.

This work was presented at the second IDEM DAY (https: / / www.idem.garr.it/index.php/it/idem-day-2) held in Rome at the head quarters of the Italian Ministry of Education on 2-3 December 2010 as a pilot project generating considerable interest from the participants.

Italiano:

Nell'Area della Ricerca di Pisa è possibile accedere a Internet tramite tecnologia wireless Wi-Fi. L'infrastruttura di rete senza fili, progettata e implementata dal reparto “*Rete Telematica del CNR di Pisa*”, è una soluzione centralizzata basata sul prodotto *Cisco Wireless LAN Controller (WLC)*.

Nel campus sono state definite diverse reti wireless, fra le quali la rete "*guest*" con meccanismo di

autenticazione *Captive Portal*.

In questo documento si descrive la soluzione software sviluppata per l'accesso alla suddetta rete usufruendo dei meccanismi di autenticazione e autorizzazione distribuiti dell'infrastruttura federata *IDEM*.

La soluzione descritta in questo documento è stata presentata all'*IDEM Day 2,* il secondo IDEM DAY (https://www.idem.garr.it/index.php/it/idem-day-2) tenuto a Roma presso la sede del MIUR nei giorni 2-3 Dicembre 2010 come progetto pilota suscitando un notevole interesse da parte dei partecipanti.

Descrizione del servizio Wi-Fi del CNR di Pisa

Per una migliore lettura del documento si ritiene importante introdurre brevemente l'architettura di riferimento (Fig. 1) del servizio Wi-Fi in funzione presso l'Area della Ricerca di Pisa. Gli elementi di maggior rilevanza che compongono il sistema sono:

- *Access point*, circa 50 distribuiti sull'intera area del campus;
- *2 Cisco Wireless LAN Controller (WLC),* modello 44XX;
- Server *RADIUS* (nello specifico freeRADIUS);
- Server *MySQL*.

Per i nostri scopi possiamo tralasciare gli switch e i router che formano la dorsale di Area. La seguente figura mostra in modo semplificato l'interazione fra gli oggetti in causa in fase di autenticazione. Come si può notare, gli host comunicano con gli access point dell'area, sottoponendo loro le proprie credenziali di accesso (username e password) direttamente al controller WLC tramite un canale sicuro HTTPS. Il controller trasmette tali credenziali al server RADIUS, il quale autorizza o meno l'accesso a Internet: il server RADIUS verifica la validità delle credenziali sul DBMS MySQL. L'adozione di un database come gestore di credenziali ha reso il processo di autenticazione degli utenti più flessibile e maggiormente gestibile rispetto al consueto file di testo.

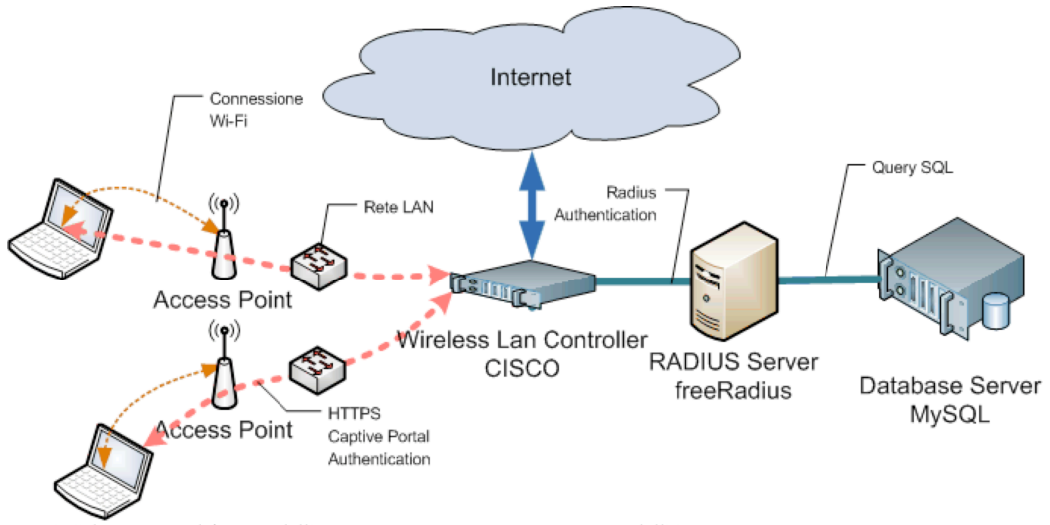

Fig. 1, Schema esemplificativo dell'accesso a Internet tramite rete Wi-Fi dell'Area

Nel file di configurazione del freeRADIUS "sql.conf" sono contenute le query SQL che il server radius esegue sul database per verificare le credenziali dell'utente. Per consentire agli amministratori di gestire in modo semplice gli account degli utenti, si è provveduto alla modifica della query *authorize_check_query* mediante l'aggiunta di varie condizioni tra cui *state="enum('enabled','disabled')", expiration="timestamp", wlan="varchar(50)".* Ovviamente tutto ciò ha comportato la modifica della tabella radcheck.

La gestione degli utenti è affidata ad un'applicazione web interamente prodotta dal servizio "Rete Telematica del CNR di Pisa", mediante la quale è possibile effettuare le operazioni di amministrazione: creazione, disabilitazione, estensione della scadenza dell'account, ecc.

Il sistema prevede diverse categorie di utenti:

- *SuperUser*, ha la gestione completa del sito web.
- *Amministratori di wireless lan*, gestiscono i propri utenti.
- *Gestori di utenti per le conferenze*, possono creare utenti validi per tutto il periodo delle conferenze a cui sono associati.
- *Utenti interni, Collaboratori e Visitatori*, sono account per l'accesso alla rete Wi-Fi, hanno una validità limitata nel tempo configurabile dal interfaccia di gestione (minimo un giorno). Queste categorie di utenti possono effettuare alcune operazioni tra cui, modifica della password, estensione del loro periodo temporale di validità, modifica dei propri attributi come indirizzo email e telefono, in base alla propria categoria di appartenenza.

Introduzione al servizio IDEM AAI GARR

IDEM (IDEntity Management per l'accesso federato) è un servizio GARR per realizzare un'*Infrastruttura di Autenticazione e Autorizzazione (AAI)* federata. IDEM utilizza *Shibboleth*, un framework basato su *SAML2* che implementa un profilo *Web Single Sign-on (SSO)*, per permettere di instaurare relazioni basate sulla fiducia all'interno della comunità dei partecipanti.

Il servizio elimina la necessità per i ricercatori, i docenti e gli studenti di dover mantenere più credenziali per poter avere accesso a diversi servizi WEB distribuiti sulla rete. I fornitori di risorse (*Service Providers, SP*) non avranno più bisogno di gestire onerose procedure di accreditamento e di amministrazione degli utenti. Le organizzazioni di appartenenza degli utenti sono i gestori delle identità (*Identity Providers, IdP*) che possono essere scambiate, fornendo le adeguate garanzie e sempre nel rispetto della privacy degli utenti.

L'Istituto di Informatica e Telematica attraverso il servizio “Rete Telematica del CNR di Pisa” ha attivamente partecipato nella fase della creazione della federazione IDEM. L'infrastruttura fornisce vari servizi ai partecipanti alla federazione accessibili con meccanismi di autenticazione e autorizzazione distribuiti. L'IIT ha partecipato inizialmente per la messa in opera di un IdP (Identity Provider) che ha consentito l'adesione alla federazione IDEM eseguendo tutti i test necessari. Questo ci ha permesso di acquisire una buona conoscenza dei sistemi di autenticazione federati basati sul protocollo SAML2.

Inoltre, da dicembre 2010, l'IIT è accreditato come Service Provider per fornire l'accesso alla rete wireless del CNR di Pisa agli utenti della federazione IDEM. Tale servizio è noto alla federazione con il nome di “WiFi@PiCNR”.

Realizzazione del servizio WiFi@PiCNR

L'obiettivo del progetto è stato quello di utilizzare l'infrastruttura IDEM per estendere il servizio Wi-Fi del CNR di Pisa agli utenti della federazione.

Il sistema nel complesso è stato implementato utilizzando il Wireless LAN Controller CISCO, software di pubblico dominio Shibboleth SP, freeRADIUS, Apache Server e codice sviluppato in PERL. Ad esclusione del WLC, il quale è un sistema hardware/software “chiuso”, gli altri servizi sono installati su server Linux CentOS-5.

La figura 2 descrive il meccanismo di accesso Web Single Sign-on (SSO) del infrastruttura IDEM.

Nei paragrafi successivi sarà descritto in dettaglio il funzionamento del sistema.

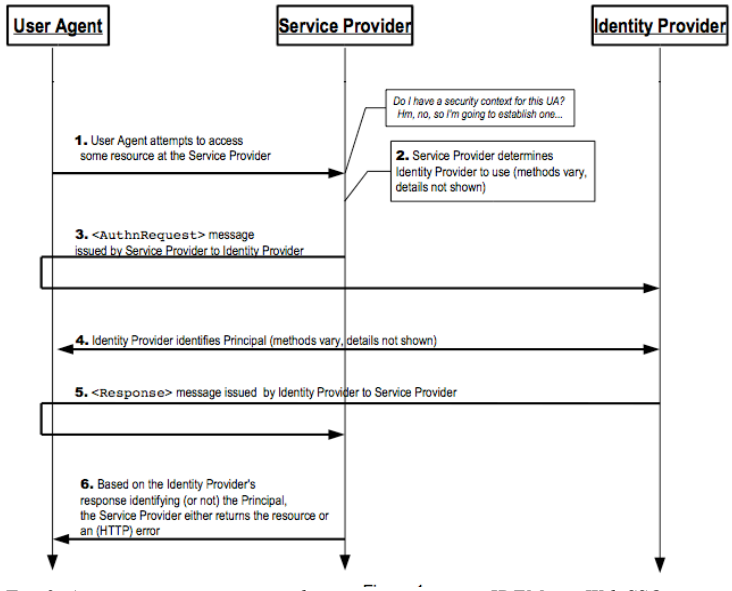

Fig. 2, Autenticazione e accesso ad un servizio generico IDEM con Web SSO

La seguente immagine (Fig. 3) mostra in modo semplificato l'architettura modificata per dare accesso Wi-Fi federato e, come sarà spiegato successivamente, mette in evidenza la necessita di interazione del *web browser* dell'utente Wi-Fi non autenticato con l'infrastruttura IDEM.

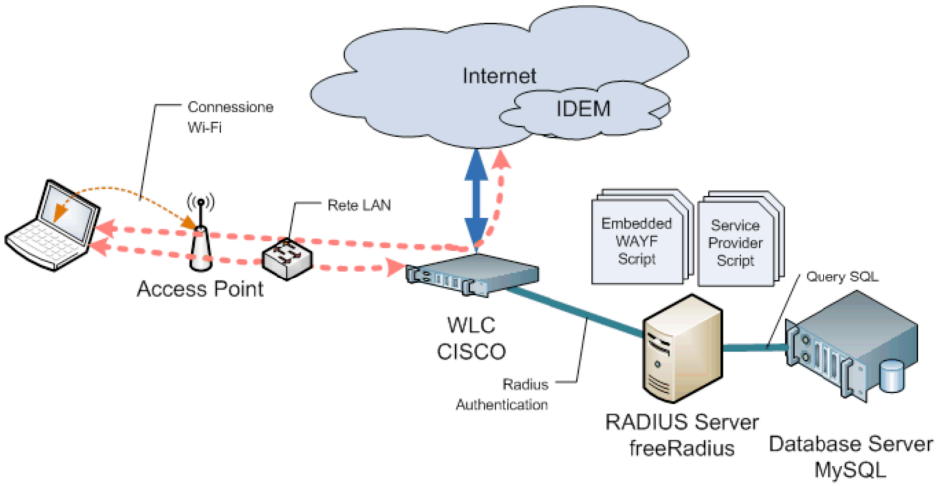

Fig. 3, Autenticazione accesso federato al Wi-Fi "guest" del CNR di Pisa

Descrizione del servizio Wi-Fi federato dal punto di vista dell'utilizzatore

Un utente della federazione IDEM in visita presso l'Area della Ricerca di Pisa può usufruire dell'accesso alla rete Wi-Fi "guest" seguendo i passaggi descritti di seguito:

1) Selezionare dal proprio computer la rete Wi-Fi "guest" come mostrato in figura 4. La configurazione IP deve essere impostata per l'acquisizione automatica tramite DHCP.

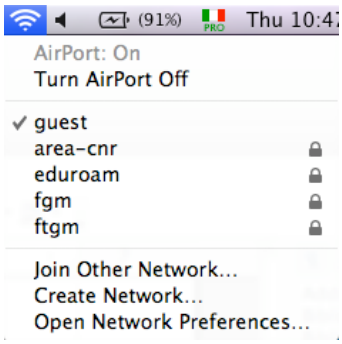

Fig. 4, scelta della WLAN "guest"

2) Aprire un browser e digitare l'indirizzo web del sito che si desidera visitare. In questa situazione il Captive Portal del WLC redirige l'utente su una pagina di autenticazione dove sarà possibile immettere le credenziali di un account locale oppure accedere tramite le credenziali della federazione IDEM, Fig. 5.

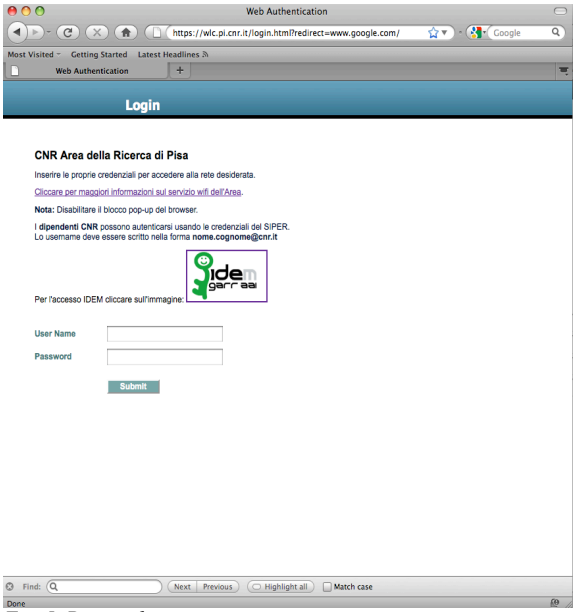

Fig. 5, Pagina di autenticazione

3) L'utente che desidera accedere con le credenziali IDEM dovrà cliccare sull'apposito logo e seguire la procedura di autenticazione.

La Fig. 6 mostra l'embedded WAYF (Where Are You From), componente dell'infrastruttura IDEM sviluppato localmente che consente all'utente finale la scelta dell'organizzazione di appartenenza (home organizzation).

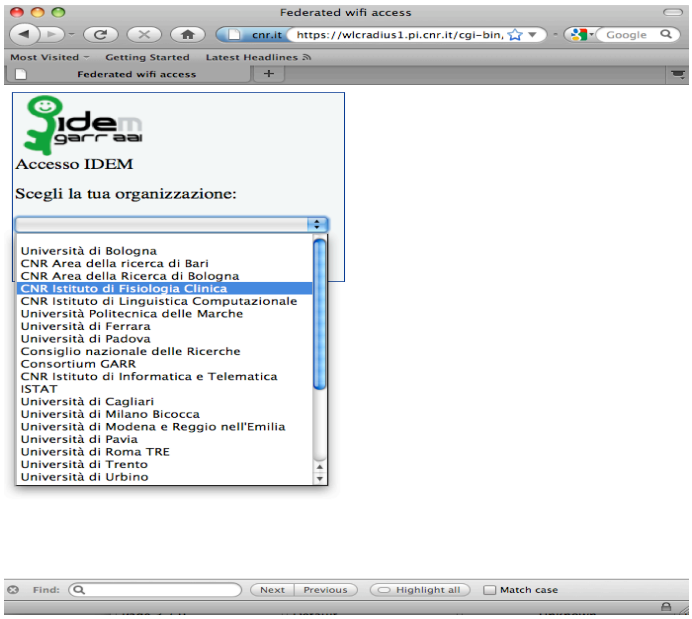

Fig. 6, Scelta della home organization, WAYF

La Fig. 7 riporta a titolo esemplificativo la pagina di autenticazione della home organization selezionata dall'utente (in questo caso Idea, home organizzation di IFC).

Fig. 7, Home organizzation Idea di IFC

La Fig. 8 mostra la pagina che viene presentata all'utente dopo l'avvenuta autenticazione da parte della propria home organization. Questa pagina contiene i dati dell'account locale per accedere alla rete Wi-Fi "guest" generati dinamicamente e validi per la giornata. L'operazione è totalmente trasparente per l'utente finale, il quale, dopo aver cliccato sul pulsante "enter", verrà autenticato e autorizzato potendo così accedere a Internet.

I dettagli del funzionamento della procedura vengono descritti nel paragrafo successivo.

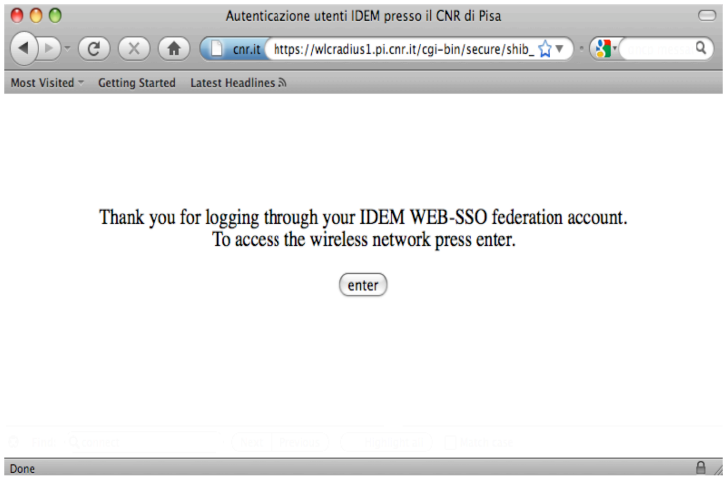

Fig. 8, Pagina per accedere alla rete Wi-Fi "guest" tramite WEB-SSO

Funzionamento del Wi-Fi federato: WiFi@PiCNR

Il WLC permette varie tecniche di autenticazione degli utenti alle reti wireless tra cui: utenti definiti localmente, autenticazione sulla base di MAC filtering o tramite l'interrogazione di server esterni Radius, Tacacs+ e LDAP. Come accennato precedentemente, per implementare il servizio si è scelto la tecnica che prevede un server di autenticazione RADIUS, nel dettaglio, realizzato tramite software open-source FreeRADIUS.

Come descritto nel precedente capitolo, l'utente non autenticato che ha selezionato la rete Wi-Fi "guest", quando inizia a navigare con il suo browser viene rediretto verso la pagina di autenticazione del Captive Portal presente sul WLC. Per rendere possibile l'autenticazione con le credenziali IDEM sono necessarie delle interazioni tra il browser dell'utente e i vari servizi della federazione IDEM come:

- L'embedded WAYF service, per la scelta della home organizzation di appartenenza;
- Il Service Provider, che genera le credenziali per l'accesso alla rete Wi-Fi;
- I vari IdP della federazione distribuiti in rete ed infine il WLC stesso.

L'impostazione di default del WLC non permette queste interazioni agli utenti non ancora autenticati, per questo motivo è necessario configurare delle Access Control Lists (ACL) sul controller in modo che tali utenti possano raggiungere le porte HTTPS degli IdP, dell'embedded WAYF service ed infine del Service Provider.

Di seguito si riporta un esempio di una configurazione di ACL impostata sul WLC ed applicata alla rete Wi-Fi "guest" per raggiungere un server HTTPS che implementa un IdP.

11	Permit	146.48.68.189 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0
12	Permit	0.0.0.0 / 0.0.0.0	146.48.68.189 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0

Fig. 9, ACL su Wireless LAN Controller

L'operazione di creazione delle ACL è abbastanza gravosa per l'amministratore di rete in quanto non è possibile automatizzarla utilizzando un metodo standard (ad esempio SNMP). Ogni volta che si

aggiunge, modifica o cancella un IdP alla federazione è necessario intervenire manualmente sulla configurazione delle ACL, tramite interfaccia Web o command line. Inoltre, bisogna sottolineare il fatto che le ACL presenti sul WLC non supportano il protocollo IPv6. Di conseguenza se l'IPv6 venisse abilitato sulla rete Wi-Fi “guest” un utente sarebbe in grado di accedere alla rete usando questo protocollo senza alcuna autenticazione.

Di seguito descriviamo in dettaglio il funzionamento dei vari script realizzati per rendere possibile il funzionamento del servizio. Quando l'utente clicca sul logo IDEM presente sulla pagina di login del Captive Portal richiama un primo script cgi che implementa parte dell'embedded WAYF. La funzione di questo script è quella di restituire il valore della URL relativa all'entityID dell'IdP selezionato dall'utente. Per svolgere questa funzione lo script elabora i metadati della federazione IDEM, estrae l'elenco delle URL relative agli entityID di tutti gli IdP della federazione e prepara un menù a tendina. Per facilitare la consultazione, all'utente viene visualizzato l'elenco corrispondente all'OrganizationDisplayName corrispondente a ciascun IdP. In assenza del valore OrganizationDisplayName verrà visualizzato l'entityID dell'IdP.

Una volta che l'utente ha selezionato l'organizzazione di appartenenza viene redirezionato verso un secondo script, a cui viene passato il parametro "entity_id" contenente la URL relativa all'entityID dell'IdP selezionato. Tale script effettua la semplice operazione di comporre la URL di redirezione verso il Session Initiator del SP passando come argomenti il target e l'entityID.

Esempio:

"https://wlcradius1.pi.cnr.it/Shibboleth.sso/DS?target=https://wlcradius1.pi.cnr.it/cgi-bin/secure/shib_guest.pl&entityID=https://idea.ifc.cnr.it/idp/shibboleth"

La stringa di sopra è sufficiente per redirezionare e autenticare l'utente presso la sua home organization. Una volta autenticato, il browser dell'utente verrà rediretto al SP il quale esegue il target script che genera l'account di login locale (valido per un solo giorno) e restituisce una pagina che comunica l'avvenuta autenticazione tramite IDEM Web SSO. A questo punto per proseguire con l'accesso al servizio Wi-Fi basterà premere il tasto “enter”, come mostrato in figura 8.

Per accedere al servizio l'IdP dell'utente deve rilasciare i seguenti attributi obbligatori “eduPersonTargetedID” e “eduPersonScopedAffiliation” ed opzionalmente l'attributo “mail”. Il SP è configurato per accettare come valore di REMOTE_USER il valore degli attributi “eduPersonTargetedID” oppure “mail”, nel rispettivo ordine di preferenza. Questo indica che se il campo “eduPersonTargetedID” esiste tra le variabili di *environment shibboleth* verrà utilizzato come valore di REMOTE_USER; in assenza di “eduPersonTargetedID” verrà controllato se esiste il campo successivo, in questo caso “mail”. Se nessuno degli attributi shibboleth richiesti sono presenti, REMOTE_USER assume valore nullo di conseguenza sarà negato l'accesso e non verrà creato alcun account locale.

La prima volta che il visitatore si autentica presso l'Area di Ricerca di Pisa, durante la creazione dell'account locale lo script target "shib_guest.pl" utilizza il campo della variabile di environment Apache REMOTE_USER per generare lo username locale con una password casuale. Al fine di mantenere una traccia storica degli accessi effettuati dall'utente visitatore, l'account non verrà cancellato anche dopo la scadenza. Nel caso in cui l'utente ha effettuato in precedenza un accesso al servizio Wi-Fi, se il valore della variabile REMOTE_USER non è cambiato, esiterà uno username valido nel database locale. Per questi accessi verrà soltanto estesa la validità dell'account per la giornata in corso, rigenerando una nuova password.

Nel caso in cui per l'utente autenticato scada la sessione Captive Portal mentre la sessione Web SSO è ancora valida, nella fase di riautenticazione IDEM non verrà richiesto di autenticarsi nuovamente tramite la propria home organization in quanto entrerà in funzione la sessione Web SSO. La

password locale viene comunque resettata dal targert script ogni volta che si effettua un login locale alla rete "guest" tramite le credenziali IDEM.

Attualmente l'attributo “eduPersonScopedAffiliation” non viene utilizzato ma è nostra intenzione utilizzare questo campo per distinguere la classe di appartenenza qualora si renda necessario.

Codice sorgente degli script PERL

Di seguito riportiamo gli script generati per integrare il servizio Wi-Fi dell'Area del CNR di Pisa con l'infrastruttura federeata IDEM.
Il primo script implementa l'embedded WAYF (1^ parte):

“https://wlcradius1.pi.cnr.it/cgi-bin/Wi-Fi-access.cgi”

```
#!/usr/bin/perl -w

use GetRc;
use CGI qw/:standard/;
use XML::Parser;
use XML::SimpleObject;
use Socket;

my $file = '/var/run/shibboleth/idem-metadata.xml';
my $q = CGI->new( );

print header,
$q->start_html(-title=>'Federated Wi-Fi access');


my $parser = XML::Parser->new(ErrorContext => 2, Style => "Tree");
my $xso = XML::SimpleObject->new( $parser->parsefile($file) );

foreach my $metadata ($xso->child('EntitiesDescriptor')->children('EntityDescriptor')) {
      if ($metadata->child("IDPSSODescriptor")) {
            # Per enti che non hanno messo l'Organization Name
            # ecco preche questo if, altrimenti non servirebbe
            if ($metadata->child('Organization')) {
                  $input{$metadata->attribute('entityID')} = $metadata->child('Organization')->child('OrganizationDisplayName')->value;
            }
            else {
                  $input{$metadata->attribute('entityID')} = $metadata->attribute('entityID');
            }
      }
}

print '<div id="wayf_div" style="background:  #F4F7F7 ;border-style: solid;border-color:  #00247D ;border-width: 1px;padding:
2px;height: auto;width:  270px ;text-align: left;overflow: hidden;">';
print '<img id="wayf_logo" src="https://wlcradius1.pi.cnr.it/idem-garr-1.jpg" alt="Federation Logo" style="border:0px">';
print '<br>Accesso IDEM<br><br>';

@entity_id = sort keys %input;
print       start_form(-method=>'post', -action=>'https://wlcradius1.pi.cnr.it/cgi-bin/Wi-Fi-access1.cgi' ),
            "Scegli la tua organizzazione:<br><br> ", popup_menu(-name=>'entity_id', -values=>['',@entity_id], -labels=>\%input), " ",
            p;
print   submit('cerca','Avvia')," ",
            defaults('Reset'),
            end_form;
```

Il secondo script implementa l'embedded WAYF (2^ parte) e redireziona l'utente alla pagina di

autenticazione della sua home organization:

“https://wlcradius1.pi.cnr.it/cgi-bin/Wi-Fi-access1.cgi”

```
#!/usr/bin/perl -w

use CGI qw/:standard/;
my $q = CGI->new( );
if(param('entity_id')) {
	$entity_id = param('entity_id');
	print $q->redirect( -URL => "https://wlcradius1.pi.cnr.it/Shibboleth.sso/DS?target=https://wlcradius1.pi.cnr.it/cgi-
bin/secure/shib_guest.pl&entityID=$entity_id");
}
else {
	print $q->redirect( -URL => "https://wlcradius1.pi.cnr.it/cgi-bin/Wi-Fi-access.cgi");
}
```

Script protetto dall'SP Shibboleth che crea le credenziali locali per accedere alla rete Wi-Fi “guest” (target script):

https://wlcradius1.pi.cnr.it/cgi-bin/secure/shib_guest.pl

```
#!/usr/bin/perl -w

use strict;
use HTML::Template::Expr;
use CGI;
use DBI;
use Config::Simple;
use Data::Random qw(:all);
my $cfg = new Config::Simple('radius_config');
my %parametri_db = %{$cfg->param(-block=>'PARAMETRI_DB')};
my $username = $parametri_db{username};
my $password = $parametri_db{password};


my $q = new CGI;
my $template = HTML::Template::Expr->new(filename => "../../html/secure/create_shib_guest.tmpl");

my $min_chars_psw = 8;
my $max_chars_psw = 8;

my @random_chars = rand_chars(set => 'alphanumeric',min => $min_chars_psw,max => $max_chars_psw);
my $pass = join "", @random_chars;


my $date = `date +"%Y-%m-%d"`;
my $insert_radcheck = "";
my $insert_radcheck1 = "";
my $user_shib = $ENV{REMOTE_USER};
#my $Common_Name = $ENV{cn};

my $dbh = DBI -> connect('DBI:mysql:radius', $username, $password);
my $usernameq = $dbh->quote($user_shib);
my $select = $dbh->prepare("SELECT username FROM radcheck WHERE username=$usernameq");
my $id_username = $dbh -> selectrow_array($select);

$template->param(buttonClicked => '4');
```

```
$template->param(err_flag => '0');
$template->param(err_msg => '');
$template->param(info_flag => '0');
$template->param(info_msg => '');
$template->param(redirect_url => 'http://www.area.pi.cnr.it');
$template->param(username => $user_shib);
$template->param(password => $pass);

if ($id_username) {
$insert_radcheck = $dbh->prepare(qq{ update radcheck set  Value = ? where username = ? and Attribute = ?});
$insert_radcheck1 = $dbh->prepare(qq{ update radcheck set expiration = timestampadd(day,1,?)  where username = ? });

$insert_radcheck->execute($pass, $user_shib, "User-Password");
$insert_radcheck1->execute($date, $user_shib);
$dbh -> disconnect();
}
else {
$insert_radcheck = $dbh -> prepare("INSERT INTO radcheck (username,attribute,op,value,wlan,state,expiration) VALUES
(?,?,?,?,?,?,?,timestampadd(day,1,?))");

$insert_radcheck -> execute($user_shib, 'User-Password', '==', $pass, 'guest', 'enabled', $date );
$insert_radcheck -> execute($user_shib, 'Airespace-Wlan-Id', '==', 1, 'guest', 'enabled', $date);
if ($user_shib =~ m/\@ifc.cnr.it$/) {
        my $insert_radreply = $dbh -> prepare("INSERT INTO radreply (username,attribute,op,value) VALUES (?,?,?,?)");
        $insert_radreply -> bind_param(1, $user_shib);
        $insert_radreply -> bind_param(2, 'Tunnel-Private-Group-ID');
        $insert_radreply -> bind_param(3, '==');
        $insert_radreply -> bind_param(4, '68');
        $insert_radreply -> execute();
        $insert_radreply -> bind_param(1, $user_shib);
        $insert_radreply -> bind_param(2, 'Tunnel-Medium-Type');
        $insert_radreply -> bind_param(3, '==');
        $insert_radreply -> bind_param(4, '802');
        $insert_radreply -> execute();
        $insert_radreply -> bind_param(1, $user_shib);
        $insert_radreply -> bind_param(2, 'Tunnel-Type');
        $insert_radreply -> bind_param(3, '==');
        $insert_radreply -> bind_param(4, '13');
        $insert_radreply -> execute();
}
$dbh -> disconnect();
}

print "Content-type: text/html\n\n";
print $template->output();
```

Il template che prepara il form finale (nascosto) per l'accesso al WLC: create_shib_guest.tmpl

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Autenticazione utenti IDEM presso il CNR di Pisa</title>
  </head>
  <body>
    <center>
    <br />
        <FORM method="post" ACTION="https://wlc.pi.cnr.it/login.html">
        <!-- <input type="TEXT" name="id_username" SIZE="32" value="<TMPL_VAR name=id_username>" /> -->
        <input type="hidden" name="buttonClicked" value="<TMPL_VAR name=buttonClicked>" />
        <input type="hidden" name="err_flag" value="<TMPL_VAR name=err_flag>" />
        <input type="hidden" name="err_msg" value="<TMPL_VAR name=err_msg>" />
        <input type="hidden" name="info_flag" value="<TMPL_VAR name=info_flag>" />
```

```
            <input type="hidden" name="info_msg" value="<TMPL_VAR name=info_msg>" />
            <input type="hidden" name="redirect_url" value="<TMPL_VAR name=redirect_url>" />
            <input type="hidden" name="username" value="<TMPL_VAR name=username>" />
            <input type="hidden" name="password" value="<TMPL_VAR name=password>" />
            <P>Thank you for logging through your IDEM WEB-SSO federation account. <br>To access the wireless network press enter.
            <P><INPUT TYPE=SUBMIT value="enter" NAME="enter"> </form>
    <br /><br />
  </center>
  </body>
</html>
```

Conclusione e considerazione generale sul servizio

La messa in opera del servizio di accesso alla rete Wi-Fi tramite l'interazione con la federazione IDEM consente potenzialmente ai quasi 3 milioni di utenti ad oggi appartenenti alle organizzazioni aderenti, di poter accedere alla rete “guest” dell'Area senza la necessità di dover interagire con gli amministratori di rete locali.

A fronte delle costanti richieste di adesione alla federazione IDEM, il vantaggio apportato da questa soluzione diventa sempre più evidente sia in termini di alleggerimento del carico di lavoro per i gestori dei servizi sia in termini di mobilità.

Un ulteriore aspetto dell'architettura proposta è dato dalla semplicità con cui può essere estesa per dare accesso a qualsiasi servizio di rete che fa uso di sistemi di autenticazione standard, come ad esempio RADIUS, LDAP ecc.

In generale, la visione di concedere l'accesso ai propri servizi locali a partire da credenziale remote viene detta *account linking* e comporta la fiducia tra le organizzazioni partecipanti. Organizzazioni che forniscono servizi di rete come i più noti social network e grossi ISP usano questi concetti per estendere il bacino dei potenziali utilizzatori.