View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Byterfly

Consiglio Nazionale delle Ricerche

CERIS ISTITUTO DI RICERCA SULL'IMPRESA E LO SVILUPPO

Maggio

2010

Rapporto tecnico N.34

Accesso Wireless Federato presso l'Infrastruttura di Rete CNR Piemonte

Giancarlo Birello, Ivano Fucile, Valter Giovanetti

RAPPPORTO TECNICO CERIS-CNR
Anno 5, N° 34, giugno 2010

Direttore Responsabile
Secondo Rolfo

Direzione e Redazione
Ceris-Cnr
Istituto di Ricerca sull'Impresa e lo Sviluppo
Via Real Collegio, 30
10024 Moncalieri (Torino), Italy
Tel. +39 011 6824.911
Fax +39 011 6824.966
segreteria@ceris.cnr.it
http://www.ceris.cnr.it

Sede di Roma
Via dei Taurini, 19
00185 Roma, Italy
Tel. 06 49937810
Fax 06 49937884

Sede di Milano
Via Bassini, 15
20121 Milano, Italy
tel. 02 23699501
Fax 02 23699530

Segreteria di redazione
Maria Zittino
m.zittino@ceris.cnr.it

Copyright © Giugno 2010 by Ceris-Cnr

All rights reserved. Parts of this paper may be reproduced with the permission of the author(s) and quoting the source.
Tutti i diritti riservati. Parti di questo rapporto possono essere riprodotte previa autorizzazione citando la fonte.

Accesso Wireless Federato presso l'Infrastruttura di rete CNR Piemonte

Federated Wireless Network Authentication at Piedmont CNR network Infrastructure

Giancarlo Birello, Ivano Fucile, Valter Giovanetti
(Ceris-Cnr)

Ceris-Cnr
Ufficio IT
Strada delle Cacce, 79
10100 Torino – Italy
Tel.: 011 3977303/388/512
Autore corrispondente: Giancarlo Birello, G.Birello@ceris.cnr.it

ABSTRACT. The CNR Ceris IT Office was an active subject in the designing phase of IDEM (federated IDEntity Management for service access), the GARR project of the Italian Federation for network authentication and authorization, and has acquired a wide experience in federated services and in the SAML platform.
IDEM has now reached a stable production level and the services accessed through our IdP are appreciated by Piedmont CNR users (for example, electronic publications or videoconferencing reservations). To improve our network services we have extended wireless access with federated authentication to simplify user login and mobility among GARR research and educational institutions.
The new feature has been developed by Shibboleth open-source software installed on a Linux Ubuntu server and some code in the PHP language, integrated with the Guest Services of the Sonicwall Network Security Appliance NSA-5500 by secure communication over HTTPS and digitally signed messages."

KEYWORDS: wireless, internet, SAML, shibboleth, federation

JEL CLASSIFICATION: Y90 - OTHER

SOMMARIO

INDICE DELLE FIGURE

1. INTRODUZIONE

Negli ultimi anni abbiamo esteso la copertura per l'accesso wireless all'intera Area della Ricerca di Torino ed alla sede del Ceris a Moncalieri. In parallelo c'è stato un uso crescente da parte degli utenti dell'accesso WiFi sia per una maggior richiesta di mobilità che per la disponibilità di apparecchiature per uso personale che prevedono di serie i dispositivi necessari.

Contestualmente siamo stati tra i partecipanti, fin dai suoi albori, alla Federazione IDEM del Garr, un servizio offerto agli enti dell'università e della ricerca per l'autenticazione e l'autorizzazione federata. Come infrastruttura di rete abbiamo partecipato da subito attivamente all'interno della federazione con un paio di *Identity Provider* (IdP), rispettivamente per l'Istituto di Ricerca sull'Impresa e lo Sviluppo (CERIS) e per l'Istituto di Virologia Vegetale (IVV).

I vantaggi sono stati subito evidenti nonostante inizialmente il numero dei Service Provider (SP) fosse limitato. La possibilità di accedere a risorse in modo indipendente dalla rete alla quale l'utente è connesso ed usando le credenziali solite che usa per accedere agli altri servizi di rete, ad esempio la posta elettronica, sono apparsi subito interessanti agli utenti e semplici nel loro utilizzo, da ciò l'uso crescente che si è riscontrato.

Dal punto di vista dei fornitori dei servizi, aderire alla Federazione implica direttamente la disponibilità di un bacino di utenza decisamente ampio, non raggiungibile diversamente. Nel caso dell'accesso wireless, come l'adesione alla rete Eduroam, implementare l'accesso federato inserendo il servizio WiFi nella Federazione Idem, significava poter estendere il servizio a tutti gli utenti degli enti afferenti al Garr senza dover instaurare accordi di cross-autenticazione con ognuno di loro, come si era fatto finora con alcuni atenei ed enti piemontesi. Non ultima la spinta data dall'entrata nella federazione, oltre ad alcuni degli atenei coi quali esistevano accordi precedenti, del CNR a livello di amministrazione centrale, in questo modo un utente CNR che si trovi sotto la nostra copertura wireless avrebbe potuto accedere alla rete con le credenziali solite di accesso al sistema Siper, con gli ovvi vantaggi per la mobilità e l'interscambio tra le strutture CNR.

Il sistema di gestione dell'Infrastruttura wireless impiegato, come descritto ampiamente nel Rapporto Tecnico N. 26 del 12 ottobre 2009, “Infrastruttura Wireless presso le Strutture CNR Piemonte”, è basato sull'apparato della Sonicwall NSA-5500. Il sistema prevede, oltre all'autenticazione 802.1x utilizzata per la rete Eduroam, un captive portal per l'autenticazione ed autorizzazione. Per federare il servizio di accesso tramite captive portal è stata scelta una soluzione open-source che ha permesso, col minimo intervento sul codice esistente, ottenere a costi molto contenuti i risultati richiesti.

2. CAPTIVE PORTAL

L'apparato Sonicwall NSA-5500 è il gestore centrale dell'infrastruttura wireless, permette l'amministrazione centralizzata degli Access Point, la loro configurazione in modo sincronizzato e l'annuncio di più reti wireless grazie all'uso delle VLAN.

Come descritto nel Rapporto Tecnico N. 26, 12 ottobre 2009, “Infrastruttura Wireless presso le Strutture CNR Piemonte”, sono annunciate due reti il cui accesso è regolato dal protocollo 802.1x, una per gli utenti locali (SSID=“TOCNR-Staff”) ed una per la rete Eduroam (SSID=“eduroam”), ed una rete open (SSID=“TOCNR-Ospiti”) che permette l'accesso ad internet a seguito dell'autenticazione ed autorizzazione su captive portal.

L'accesso tramite *captive portal* è denominato dal NSA-5500 “Guest services” e permette definire, nella configurazione, l'url delle pagine web che dovranno fornire l'interfaccia verso l'utente per la sua autenticazione, eventualmente residenti su un server esterno all'apparato.

2.1 Autenticazione radius

Nella prima implementazione dei servizi di accesso wireless, per quanto riguarda l'accesso tramite captiva portal, si è scelta l'autenticazione sul server radius già presente presso la nostra infrastruttura e che dava la possibilità, grazie ad accordi di cross-autenticazione, di estendere la disponibilità del servizio anche per gli utenti di altri enti locali e nazionali.

Nella figura seguente è riassunto il flusso delle operazioni di accesso tramite captive portal e autenticazione radius.

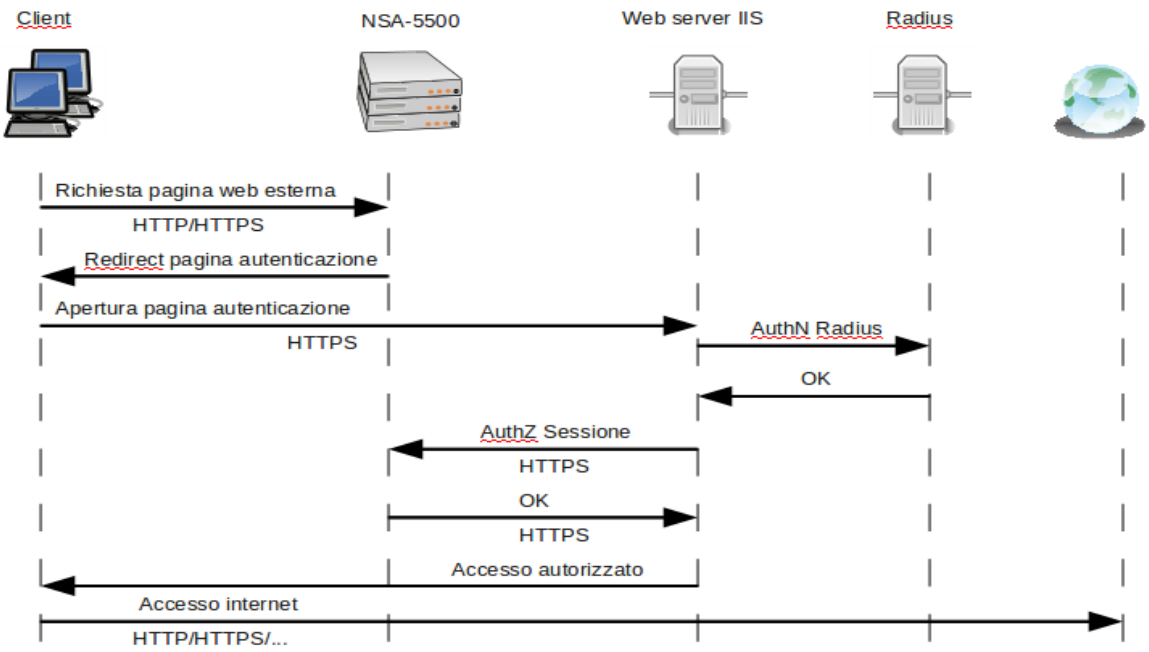

FIGURA 1: FLUSSO AUTENTICAZIONE RADIUS

Dopo aver agganciato la rete wireless TOCNR-Ospiti, il primo tentativo del client di navigare verso pagine esterne all'organizzazione, cioè i cui indirizzi IP non sono inclusi nella lista di quelli permessi pre-autenticazione (cfr. configurazione NSA-5500, Guest services), viene intercettato dal firewall e reindirizzato alla pagina di autenticazione predisposta su un web server esterno come definito nella configurazione dei Guest Services.

Il web server raccoglie le credenziali dell'utente tramite connessione protetta HTTPS ed interroga con una chiamata di sistema il server radius, che a sua volta risponderà in modo affermativo qualora l'autenticazione vada a buon fine.

In tal caso il web server procede con richiedere al NSA-5500 l'apertura della sessione e la sua autorizzazione. In caso affermativo, all'utente verrà comunicato, sulla stessa pagina web di autenticazione, la riuscita dell'intero processo e la disponibilità di accesso ad internet.

Nel caso di utilizzo di credenziali di un'istituzione con la quale esistano accordi di cross-autenticazione, il flusso verrebbe esteso con un'interrogazione dal radius locale fino al radius dell'istituzione terza da cui attendere la conferma dell'autenticazione. In questo caso non esiste una comunicazione diretta tra client e radius esterno, quindi non sono necessarie modifiche alcune all'elenco degli indirizzi IP accedibili prima dell'autenticazione da parte del client.

2.2 Autenticazione federata

Nel caso invece di voler procedere con l'autenticazione federata occorre basare il sistema di autenticazione ed autorizzazione su una struttura diversa dalla tipologia radius.

Innanzitutto il sistema di accesso deve prevedere un servizio (SP) inserito all'interno di una federazione di autenticazione ed autorizzazione, nel caso specifico, la federazione in questione è IDEM del Garr, alla quale il CNR ed il Ceris in particolare, ha partecipato attivamente fin dalla sua fase iniziale risalente ad alcuni anni fa.

In una struttura di questo tipo esistono due elementi fondamentali: gli Identity Provider (IdP) ed i Service Provider (SP). I primi incaricati della gestione digitale delle identità ed i secondi fornitori di servizi ai quali accedere previa autenticazione presso la propria istituzione, cioè presso il proprio IdP. Quest'ultimo fornirà al SP una serie di attributi relativi all'utente autenticato, in base ai quali il SP deciderà se autorizzare o meno l'accesso al servizio che l'utente sta richiedendo.

Nello specifico la Federazione IDEM del Garr è basata sullo standard Oasis Security Assertion Markup Language (SAML) v2.0, su cui si basa il software open source Shibboleth di Internet2, che permette implementare IdP e SP su piattaforme linux per realizzare servizi di web single sign-on all'interno di federazioni e aderenti allo standard.

In questo scenario, il server radius verrà sostituito da un SP inserito in federazione e l'autenticazione dell'utente che sta accedendo alla rete wireless avverrà presso l'IdP della propria istituzione, aumentando così il livello di sicurezza e privacy a livelli paragonabili a quelli del protocollo 802.1x.

Questo amplia ovviamente anche il bacino dell'utenza che può accedere al servizio wireless, senza necessità di cross-autenticazioni, essendo queste implicite nella federazione, ma comunque filtrabili a livello di SP, potendo autorizzare o meno i singoli utenti in base alla loro appartenenza istituzionale.

3. AUTENTICAZIONE FEDERATA IDEM (SAML2)

La soluzione prescelta è stata individuata tenendo conto di alcuni fattori quali mantenere parallelamente l'autenticazione radius, rispettare alcuni vincoli dettati dal NSA-5500 e non modificabili, ridurre al minimo l'intervento sugli script esistenti ma nello stesso tempo introdurre una piattaforma distinta da quella .NET per poter implementare il SP su piattaforma linux open source.

Volendo sfruttare la disponibilità di SP tra i pacchetti linux (distribuzione Ubuntu), si è pensato attivare un server linux Apache con Shibboleth come SP, mettere la pagina

PHP, incaricata di ricevere gli attributi a seguito dell'autenticazione sull'IdP e rispondere alla pagina del captive portal originaria, protetta dietro il Service Provider Shibboleth. Inoltre per elevare il livello di sicurezza, la comunicazione tra la pagina PHP e la pagina ASPX è stato scelto di effettuarla tramite POST firmato digitalmente con certificato del server sul quale risiede il SP, essendo questa risposta quella che determina l'accesso o meno dell'utente alla rete wireless.

Nella figura riportiamo lo schema di accesso tramite la federazione, semplificando la parte propria dell'autenticazione Shibboleth non essendo tra gli scopi del presente documento.

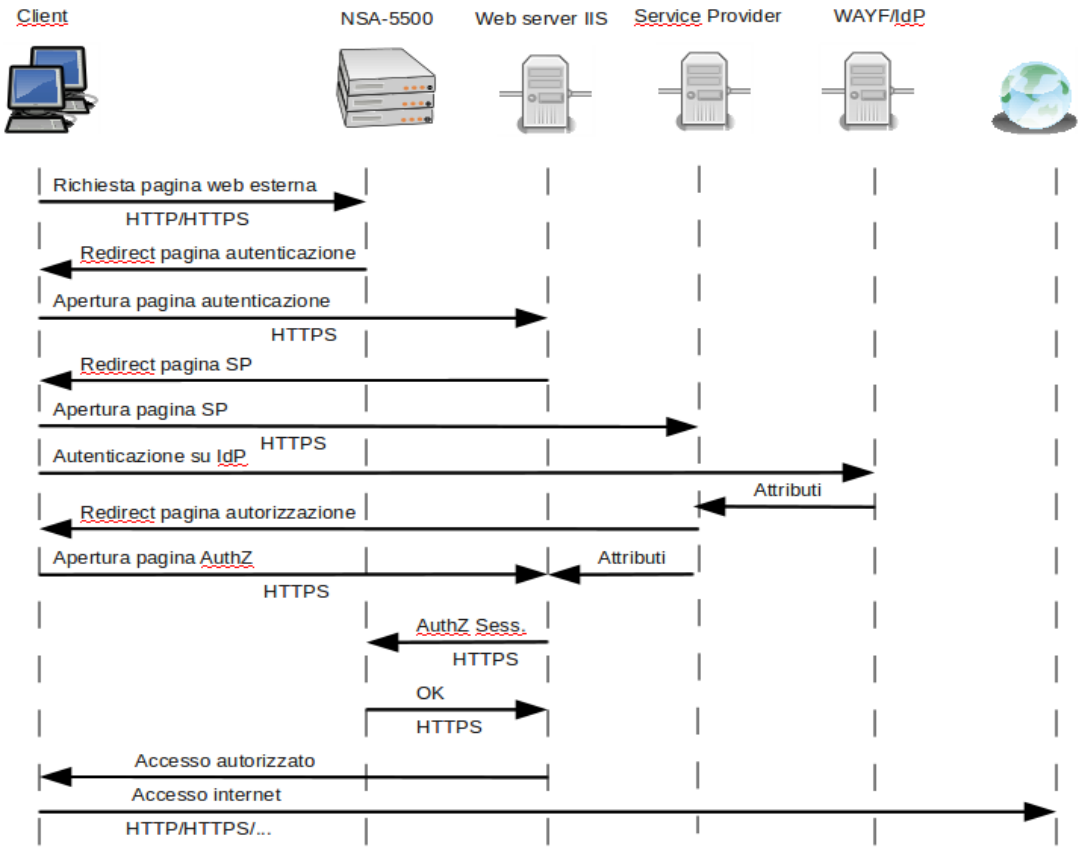

FIGURA 2: FLUSSO AUTENTICAZIONE FEDERATA

3.1 Configurazione NSA-5500

Nella configurazione del NSA-5500 occorre tener presente delle seguenti modifiche:

- le nuove pagine aspx a cui i Guest Services devono puntare, cioè le pagine modificate che includono l'autenticazione federata in aggiunta a quella radius

- i client prima dell'autenticazione devono comunque poter accedere sia al WAYF della Federazione che al loro IdP, ovviamente esterni alla rete locale, quindi dovrà essere aperto il traffico verso questi IP.

I Guest Services si gestiscono dalla pagina *Zones* della voce *Network* del pannello di configurazione del NSA-5500, in particolare, nel nostro caso, essendo abbinati alla rete wireless TOCNR-Ospiti, dalle proprietà di quest'ultima.

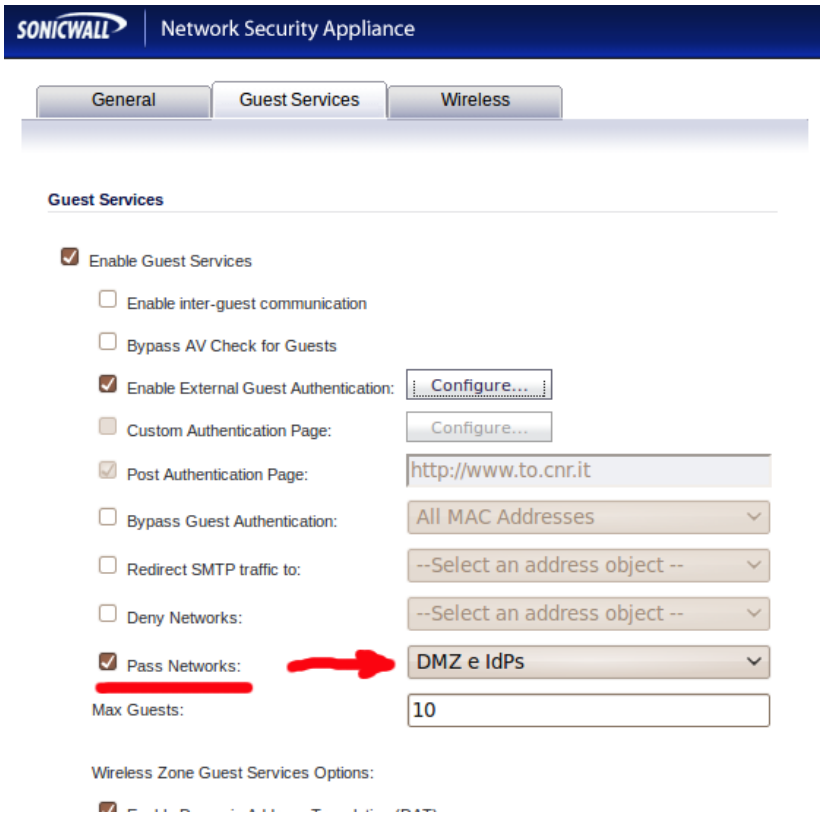

FIGURA 3: CONFIGURAZIONE WALLED GARDEN

Nella figura precedente è indicato dove impostare gli indirizzi IP verso i quali è aperta la navigazione prima dell'autenticazione/autorizzazione dell'utente (walled garden). SI è scelto inizialmente di avvalersi degli oggetti network messi a disposizione dal NSA-5500, costituendo un gruppo popolato manualmente con gli indirizzi IP del WAYF e dei vari IdP della Federazione.

Su questo punto sono comunque in fase di studio soluzioni alternative, che rendano automatico l'aggiornamento del walled garden della Federazione, ma non ancora disponibili al momento. Inoltre occorre anche attendere la nuova release del firmware

del NSA-5500 che metterà a disposizione per i Guest Services anche gli oggetti FQDN, potendo così pensare di appoggiarsi eventualmente su record del DNS, aggiornati dinamicamente.

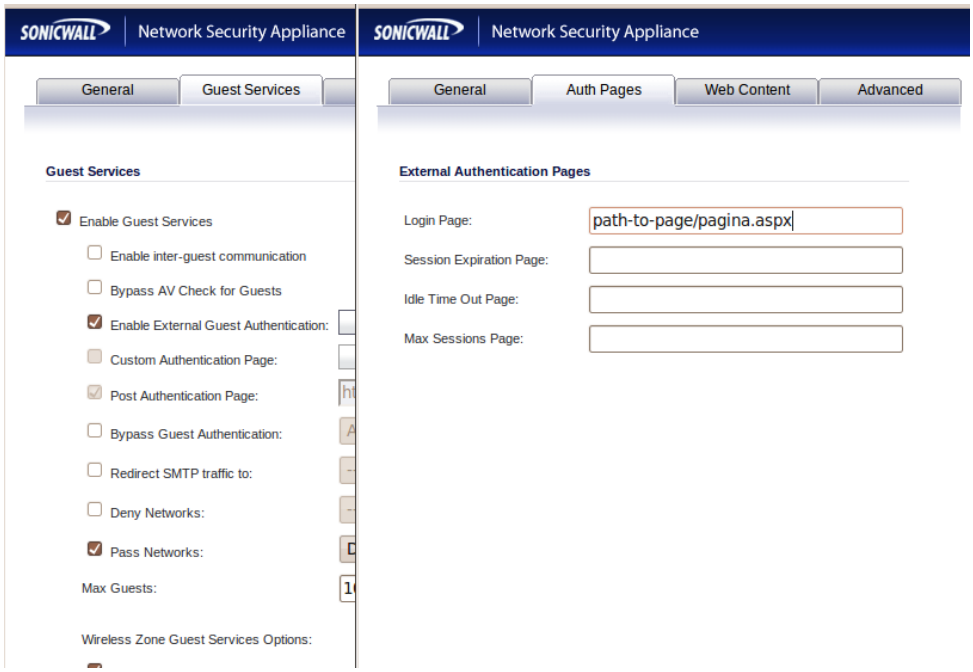

FIGURA 4: CONFIGURAZIONE PAGINA AUTENTICAZIONE

Avendo abilitato i Guest Services e l'autenticazione esterna, selezionando Configure, si ottiene la finestra riportata nella figura sopra, tramite la quale è possibile inserire il percorso, sul server web esterno, della pagina incaricata di gestire l'autenticazione per l'accesso alla rete wireless TOCNR-Ospiti.

Per una trattazione più approfondita della configurazione della rete TOCNR-Ospiti cui si ha accesso tramite captive portal, si rimanda al Rapporto Tecnico N. 26, 12 ottobre 2009, “Infrastruttura Wireless presso le Strutture CNR Piemonte”.

3.2 Configurazione Web server IIS

Sul web server (IIS, Windows Server 2003R2), è stata modificata la pagina di autenticazione aspx esistente (*pagina.aspx*), aggiungendo la possibilità di autenticazione federata tramite IDEM, come si evidenzia nella figura 5:

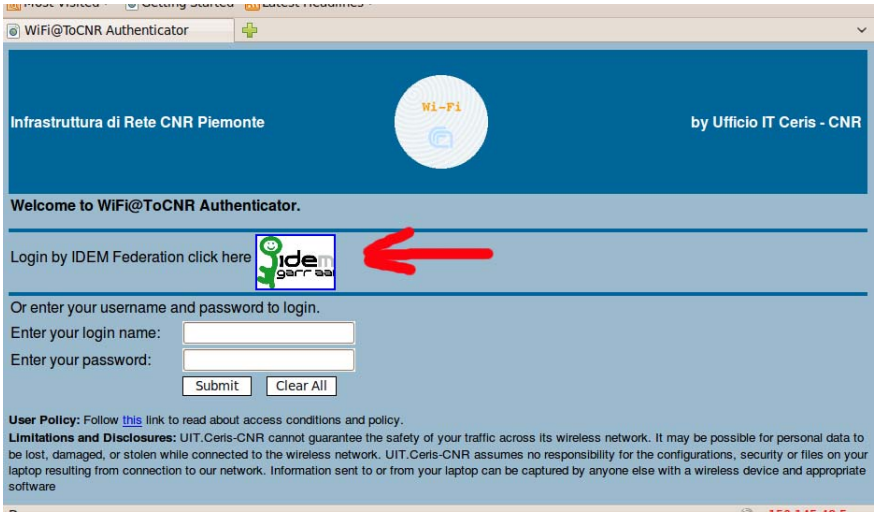

FIGURA 5: PAGINA AUTENTICAZIONE CAPTIVE PORTAL

Nel codice della pagina, il link è stato fatto puntare alla pagina PHP protetta dal SP sul server linux aggiunto, passando tramite una GET un paio di parametri essenziali per la parte finale del processo, l'identificativo della sessione e l'URL a cui la pagina incaricata deve mandare la richiesta al NSA-5500 per ottenere l'autorizzazione. Nel codice di *pagina.aspx* sono state inserite le seguenti linee:

```
<td>Login by IDEM Federation click here
        <a href = "https://server2.to.cnr.it/secure/authn.php<%
response.write("?par1=" & sessionId & "&par2=" & mgmtBaseUrl)
%>"><img width="10%" height="10%" src="IDEM_logo.jpg"
align="middle"/></a>
</td>
```

mentre l'URL a cui viene re-indirizzato l'utente, una volta selezionato il link, risulta ad esempio:

"https://server2.to.cnr.it/secure/login.php?par1=d415bc80ea73ccc5cb64b2b7b48b46a8&par2=https://123.123.123.1:4043/"

È stata invece necessario aggiungere una seconda pagina (pagina2.aspx), per provvedere alla fase di autorizzazione, alla quale l'utente viene re-indirizzato una volta autenticato tramite il SP presso l'IdP della propria istituzione.

A questa pagina l'utente giunge a seguito dell'autenticazione e a questa stessa pagina il SP, tramite la pagina PHP che vedremo in seguito, invia gli attributi dell'utente, ricevuti dall'IdP e necessari all'autorizzazione. Per ovvie ragioni di sicurezza si è deciso di inviare gli attributi a questa pagina tramite un POST firmato digitalmente. Il codice che

sottende alle operazioni di estrazione e decodifica dei parametri inseriti nel POST ed alla verifica della firma digitale è il seguente:

```
[…]
'recupero indirizzo IP server e parametri del POST
ra = Request.ServerVariables("REMOTE_ADDR")
ePTI=Request.Form("ePTI")
ePSA=Request.Form("ePSA")
sessionId=Request.Form("sessId")
mgmtBaseUrl=Request.Form("mgmtBaseUrl")
enc=Request.Form("dsig")

[...]
'verifica della firma digitale dell'ID della sessione
Dim signData As Byte()
signData = New Byte(255){}
Dim i as integer
for i=0 to 255
        signData(i) = Convert.ToByte(enc.substring(i*2,2),16)
next i
Dim verify() As Byte = Encoding.UTF8.GetBytes(sessionId)
Dim certificate As X509Certificate2 = New X509Certificate2(MapPath("pk.crt"), "",
        X509KeyStorageFlags.MachineKeySet)
Dim rsacp As RSACryptoServiceProvider = New RSACryptoServiceProvider
Dim sha As New SHA1CryptoServiceProvider()
Dim pKey As String = certificate.PublicKey.Key.ToXmlString(False)

rsacp.FromXmlString(pKey)
Dim ok1 As Boolean = rsacp.VerifyData(verify, sha, signData)

[…]
'per procedere con autorizzazione verifica IP, firma e attributi
If (ra = "150.145.48.2") AND (ok1 = true) AND (ePTI <> "") AND (ePSA <> "")
        LHM()
else
        LHMResult.Text = "<b><font color=""red"">Session creation
        failed:</font></b> The request for authorization failed due to IP error,
        signature failure or attribute incomplete. Sorry for the inconvenience. Please
        close and relaunch your browser to try again."
end if
```

Una volta verificati i requisiti, la pagina provvede a chiamare la procedura LHM che richiede l'autorizzazione dell'accesso al NSA-5500. Tale procedura è quella originale degli script forniti da Sonicwall e non è stata necessaria alcuna modifica, avendo già adattato allo scopo il codice illustrato precedentemente. Se tutto va a buon fine, apparirà la pagina di conferma e l'eventuale finestra di logout come nella figura 6:

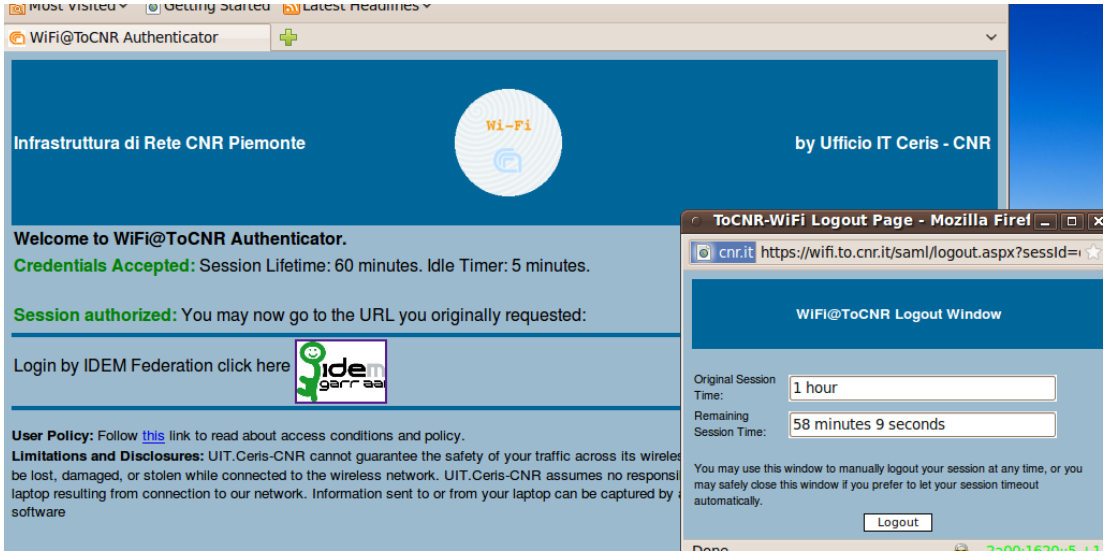

FIGURA 6: PAGINA AUTORIZZAZIONE E LOGOUT

3.3 Configurazione Service Provider Shibboleth

Come Service Provider SAML2 compatibile è stato scelto Shibboleth, installato su un server linux Ubuntu, release 10.04 LTS, sfruttando la disponibilità del pacchetto per questa distribuzione, in particolare la versione del SP Shibboleth in questo caso è la 2.3.1.

Per la configurazione del SP si è agito praticamente solo sul file *shibboleth2.xml* presente nella cartella */etc/shibboleth*, in particolare le parti principali modificate sono:

```
[...]
<RequestMapper type="Native">
    <RequestMap applicationId="default">
      <Host name="server2.to.cnr.it">
        <Path name="secure" authType="shibboleth" requireSession="true"/>
      </Host>
    </RequestMap>
  </RequestMapper>
[...]
  <ApplicationDefaults id="default" policyId="default"
    entityID="https://server2.to.cnr.it/sp"
    REMOTE_USER="eppn persistent-id targeted-id"
    signing="false" encryption="false">
      [...]
    <Sessions lifetime="28800" timeout="3600" checkAddress="false"
      handlerURL="/Shibboleth.sso" handlerSSL="false"
      exportLocation="http://localhost/Shibboleth.sso/GetAssertion"
exportACL="127.0.0.1"
      idpHistory="false" idpHistoryDays="7">
```

```
        <SessionInitiator type="Chaining" Location="/WAYF" id="WAYF"
relayState="cookie">
            <SessionInitiator type="SAML2" acsIndex="1"
template="bindingTemplate.html"/>
            <SessionInitiator type="Shib1" acsIndex="5"/>
            <SessionInitiator type="WAYF" acsIndex="5"
URL="https://wayf.idem.garr.it/WAYF"/>
        </SessionInitiator>
[...]
    </Sessions>
[...]
    <MetadataProvider type="Chaining">
            <MetadataProvider type="XML"
                    uri="https://www.idem.garr.it/docs/conf/signed-metadata.xml"
                    backingFilePath="signed-metadata.xml"
reloadInterval="7200">
            <SignatureMetadataFilter certificate="signer_bundle.pem"/>
            </MetadataProvider>
    </MetadataProvider>
[...]
    <CredentialResolver type="File" key="/etc/ssl/private/server2.to.cnr.it.TCS.key"
      certificate="/etc/ssl/certs/cert-242-server2.to.cnr.it.pem"/>
  </ApplicationDefaults>
[...]
```

Si è poi proceduto con la configurazione del web server le cui pagine potranno essere protette tramite il SP Shibboleth. È stato scelto come web server Apache con il supporto per PHP, installato sempre tramite i pacchetti di Ubuntu, nello specifico la versione fornita è la 2.2.14 e per PHP la versione 5.3.2.

Si è quindi configurato il web server per rispondere alle interrogazioni sulla porta 80 (HTTP) e sulla porta 443 (HTTPS) tramite protocollo SSL. La cartella da proteggere col SP si è stabilito fosse /web-root/secure alla quale si deve poter accedere solo tramite protocollo sicuro SSL. Per ottenere queste configurazioni sono stati definiti due siti all'interno del web server, in particolare evidenziamo dei due siti le impostazioni che differiscono dal default d'installazione del pacchetto:

site default

```
<VirtualHost *:80>
[...]
        RewriteEngine   on
        RewriteCond     %{SERVER_PORT} ^80$
        RewriteRule     ^/secure(.*)$ https://%{SERVER_NAME}/secure$1 [L,R]
        RewriteLog      "/var/log/apache2/rewrite.log"
        RewriteLogLevel 2
</VirtualHost>
```

con il modulo rewrite si re-indirizzato l'utente, che cerchi di accedere alla cartella *secure* ed alle sue sottocartelle tramite HTTP sulla porta 80, verso la porta 443 in SSL

site default-ssl

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
[...]
        <Location /secure>
                AuthType Shibboleth
                ShibRequireSession On
                require valid-user
                ShibUseHeaders On
                require shibboleth
                Order allow,deny
                Allow from all
        </Location>
</VirtualHost>
</IfModule>
```

questa parte di configurazione serve per richiedere che l'accesso alla cartella secure sia protetto dal SP shibboleth.

Occorre ovviamente ricordarsi, terminate le configurazioni, di attivare i due siti ed i moduli richiesti (shib2 e rewrite) tramite i comandi messi a disposizione dal pacchetto Apache, cioè a2ensite e a2enmod, e procedere col riavvio del web server.

A questo punto, nella cartella *secure* protetta dal SP, può essere inserita la pagina PHP da noi realizzata (*authn.php*) allo scopo di raccogliere gli attributi rilasciati dall'IdP, qualora l'autenticazione vada a buon fine, e richiamare la pagina aspx (pagina2.aspx) sul web server IIS a cui invierà contemporaneamente tramite POST gli attributi e l'ID di sessione firmato digitalmente.

Questa pagina consiste di tre parti principali:

- il recupero dei parametri passati tramite GET dalla pagina iniziale di autenticazione sul web server IIS (*pagina.aspx*) e il recupero degli attributi passati dall'IdP
- la firma digitale dell'ID di sessione affinché la pagina di autorizzazione (*pagina2.aspx*) possa verificare l'autenticità del POST
- il POST alla pagina di autorizzazione (*pagina2.aspx*) ed il re-indirizzamento del client

Il codice relativo alla prima parte di recupero delle variabili è:

```
<?php
[...]
        $sessionId= $_GET["sessId"];
        $mgmtBaseUrl= $_GET["mgmtBaseUrl"];
```

```
        $ePTI = $_SERVER['persistent-id'];
        $ePSA = $_SERVER['affiliation'];
[...]
```

A cui segue la parte relativa alla firma digitale dell'ID della sessione, effettuata tramite la chiave primaria del certificato in possesso del server:

```
[...]
        /*sign*/
        $source = $sessionId;
        $fp=fopen('/path-to-cert-key/server.key','r');
        $priv_key=fread ($fp,8192);
        fclose($fp);
        $privid=openssl_get_privatekey ($priv_key);
        $signature = "";
        openssl_sign($source, $signature, $privid, OPENSSL_ALGO_SHA1);
        $hsignature=bin2hex($signature);
[...]
```

Vengono infine assemblati i parametri e la firma digitale per il POST, effettuato il POST alla pagina di autorizzazione (*pagina2.aspx*) tramite le librerie curl che permettono anche il contestuale re-indirizzamento del client alla pagina relativa.

```
[...]
        /*Assemble the data to post back*/
        $loginParams = "par1=".
        $sessionId."&par2=".urlencode($ePTI)."&par3=".urlencode($ePSA)."&par4=
".                      $mgmtBaseUrl."&par5=".$hsignature;
        $byteArray = utf8_encode($loginParams);
[...]
        $ch = curl_init("https://path-to-captive-portal/pagina2.aspx");
        curl_setopt ($ch, CURLOPT_POST, 1);
        curl_setopt ($ch, CURLOPT_POSTFIELDS, $byteArray);
        curl_setopt ($ch, CURLOPT_FOLLOWLOCATION, 1);
        curl_setopt ($ch, CURLOPT_SSL_VERIFYPEER, 0);
        curl_setopt ($ch, CURLOPT_SSL_VERIFYHOST, 0);
        $risposta = curl_exec ($ch);
        curl_close ($ch);
[...]
?>
```

4. CONCLUSIONI

Il risultato ottenuto è quello che ci aspettava, cioè integrare i servizi di accesso alla rete wireless con l'autenticazione federata di modo da offrire un servizio più versatile per i nostri utenti e per gli organi CNR afferenti alla nostra infrastruttura.

Seppur partendo da una soluzione iniziale legata ad un vendor specifico e con un'implementazione proprietaria, si è potuto con poco sforzo abbinare ed integrarla con la soluzione open-source prescelta, sicuramente la più adatta all'ambiente federato del quale il CNR è membro.

La soluzione individuata può essere per sua natura anche utilizzata in contesti diversi da quello specifico del NSA-5500 e come tale può essere di interesse all'interno della comunità Garr. Per questo verrà presentata come soluzione all'interno del Working Group “WiFi federato” del Comitato Tecnico-Scientifico della Federazione Idem. All'interno del quale si affronterà anche la discussione su come fornire a tutti coloro che offro un servizio WiFi federato, in modo pratico e centralizzato, il walled garden necessario alla configurazione degli apparati, di cui alcuni soluzioni possibili sono script di interrogazione dei metadati o record multipli nel DNS.

Va ancora sottolineato il doppio vantaggio ottenuto con la partecipazione alla Federazione Idem: come IdP, la possibilità per i nostri utenti di poter accedere alle risorse della federazione, alcune gratuite come il servizio di videoconferenza e l'accesso wireless di alcuni atenei; come SP WiFi@ToCNR, offrire al pari di altri enti ed in aggiunta alla rete Eduroam, punti di accesso ad internet aperti alla comunità Garr e nel rispetto della sicurezza, cioè solo a persone autenticate e delle quali si conosca la provenienza.