Networking

Accesso Wi-Fi con Autenticazione Federata.†

Luca Ianniello,*[a] Augusto Pifferi,[a]

In questo documento viene descritta l'attività di realizzazione di un sistema Captive Portal per l'accesso a internet con Autenticazione Federata. Il progetto ha per obiettivo quello di consentire agli ospiti del Campus dell'Area della Ricerca Roma1 (CNR), che già posseggono una Identità Digitale certificata, un accesso sicuro con le proprie credenziali senza l'obbligo di una nuova registrazione dei dati personali pur mantenendo comunque il pieno rispetto delle Acceptable Use Policy (AUP) imposte da GARR che richiedono esplicitamente la tracciabilità degli utenti. Sono indicate le specifiche di progetto, l'architettura, il software e i risultati ottenuti.
Keywords: Access Point, Hotspot, Captive Portal, Wireless, IDEM, Accesso Federato, SAML, simpleSamlPhp, Service Provider, Identity Provider.

1 Introduzione

Presso l'Area della Ricerca di Roma1 (CNR) è presente una infrastruttura Wireless a 2.4Ghz/5Ghz composta attualmente da 30 Access Points distribuiti presso la maggior parte degli edifici.

La configurazione dei singoli AP è gestita in maniera centralizzata da un unico controller, un Aruba network 3600 che comprende ed implementa la possibilità di utilizzare un Captive Portal per l'autenticazione degli utenti (fig. 1).

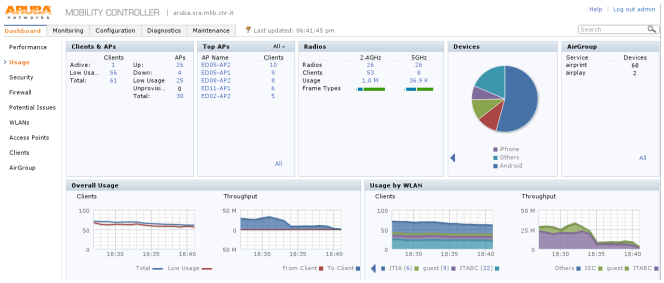


Fig. 1 Interfaccia di monitoring del controller Aruba3600

Ritenendo che il Captive Portal fornito dal controller fosse troppo restrittivo o non sufficientemente personalizzabile, oltre che oneroso in termini di licenze, si è optato per l'implementazione di software Open Source in grado di soddisfare le necessità dell'accesso a Internet via Wireless Autenticato e Autorizzato.

2 Il progetto

La tecnica "Captive Portal" consiste nel forzare un client http connesso ad una rete di telecomunicazioni ad accedere ad una speciale pagina web (di solito per l'autenticazione) prima di poter permettere la navigazione all'utente.[1]

In questo progetto, oltre alle oramai ben note dinamiche di accesso è stata prevista la possibilità di autenticare gli utenti attraverso credenziali gestite da altre Identità Federate, evitando completamente la prassi di registrazione dei dati personali. Per ottenere questo scopo occorre istituire un Service Provider e registrarlo presso la Federazione IDEM[2] del GARR.

3 Specifiche del progetto

Le specifiche del progetto sono:

- Uso di un software Open Source su piattaforma Linux;
- Implementazione del servizio sulla struttura hardware già esistente sfruttando l'Aruba3600;
- Implementazione di software per l'abilitazione alle funzioni di Service Provider SimpleSamlPHP;
- Registrazione del Service Provider presso la Federazione IDEM;
- Consentire la connessione esclusivamente verso l'Identity Provider appartenenti alla Federazione per l'ottenimento dell'Autenticazione;
- Impedire la navigazione ai client non autenticati;
- Consentire l'accesso ad account già connessi (multi-dispositivo cellulari/pc etc);
- Riepilogo dettagliato delle connessioni effettuate dall'account utente Sistemi di sicurezza per la salvaguardia del sistema operativo e dei dati;

[a] *Istituto di Cristallografia, C.N.R., via Salaria km 29.300, 00015 Monterotondo Italia.*

† Rapporto tecnico IC-RM 2016/05 protocollato in data 21/06/2016 n. 0001101

- Log degli accessi;
- Prassi di Logout fine sessione.

Il software Open Source “CoovaChilli”[3] per le sue funzionalità di Access Control Software è già stato utilizzato con successo in altri progetti dando prova di flessibilità e robustezza e pertanto è stato deciso di riutilizzarlo in questo. Grazie al supporto di SAML (Security Assertion Markup Language)[4] è stato possibile modificare le dinamiche di autenticazione per demandarle all’IdP di appartenenza dell’utente anziché al RADIUS previsto da CoovaChilli.

4 Realizzazione del CAPTIVE

Il Captive Portal con Service Provider è stato installato su una macchina virtuale del server HP con sistema operativo di base ESXi del Servizio Reti d’Area con le seguenti caratteristiche:

Modello	Virtual Machine ESXi-VM are guest
Processore	4vCPU
MemoriaRAM	Memory 3 GB
Dischi Fissi	Virtual Disk 16 GB
Scheda Video	VMware SVGA II Adapter
Scheda Rete	3 Virtual Network Adapter

Tabella 1 Risorse a disposizione nella Virtual Machine

Per poter usufruire di un AAI (Authentication and Authorization Infrastructure) che ha il compito di razionalizzare e semplificare i sistemi di autenticazione circa gli accessi ai servizi tra organizzazioni diverse, ci si avvale dell’utilizzo di SAML attraverso un apposito framework. Visto l’elevato livello di personalizzazione richiesto dal progetto si è preferito l’uso di SimpleSamlPHP sfruttando nel contempo la sua semplicità di implementazione.

Tramite SAML è possibile realizzare il Single Sign On istituzionale autenticando gli utenti localmente e autorizzandoli ad accedere alle risorse in base ad informazioni scambiate dalle organizzazioni in modo sicuro.

L’intera piattaforma è stata installata e configurata su Sistema Operativo GENTOO LINUX.[5]

L’implementazione del software RADIUS necessario in questa piattaforma è anch’esso di origine Open Source ed è FreeRadius.[6] Per la parte dei dati relativi alle credenziali d’accesso e gli attributi richiesti a supporto per il funzionamento del protocollo “AAA” utilizzeremo quelli forniti dagli appositi IdP tramite il SP creato con SimpleSamlPHP.

Una volta configurato SimpleSamlPHP per svolgere la funzione di Service Provider, come da manuale, sono stati generati i metadati necessari alla registrazione dello stesso presso IDEM.

La registrazione alla Federazione IDEM prevede due fasi: una prima fase di test durante la quale lo staff del GARR verifica e controlla la coerenza, la completezza e la corretta forma dei Metadati del SP o dell’IdP che si sta sottoscrivendo alla Federazione, per ottemperare a questa meticolosa fase il GARR mette a disposizione un portale dedicato al controllo dei Metadati prodotti facilitando e migliorando la stesura e la verifica degli stessi.[7] (Fig. 4)

Oltre ai Metadati necessari per l’accesso alla Federazione, tra i dati richiesti, occorre indicare all’interno della descrizione delle policy, gli attributi che saranno richiesti dal SP per l’accesso al servizio che si sta proponendo. (Fig. 5)

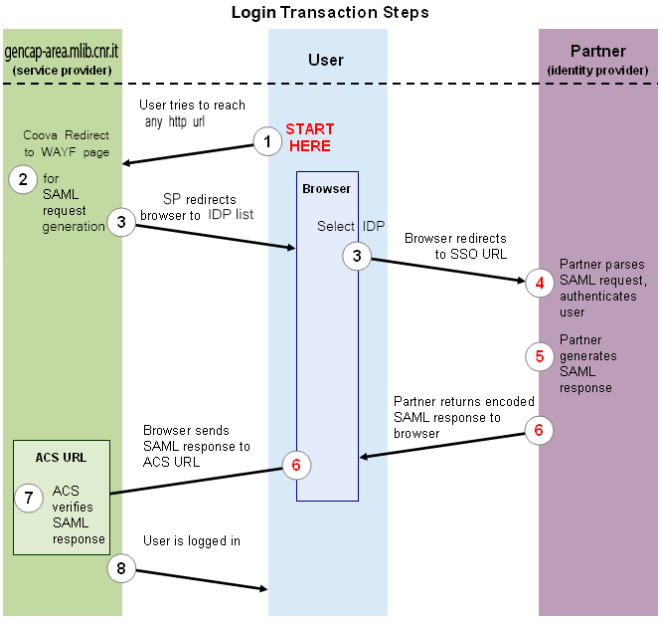


Fig. 2 Fasi di autenticazione e autorizzazione

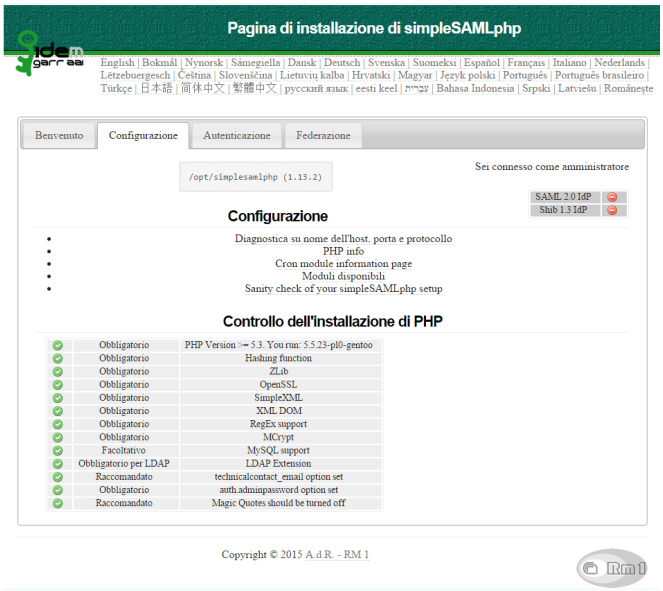


Fig. 3 Interfaccia di controllo SimpleSamlPHP

Una volta conclusa la fase di Test il SP appena creato entrerà a far parte della lista dei Service Provider autorizzati dalla Federazione abilitando così lo stesso allo scambio di asserzioni SAML, con gli IdP già registrati in IDEM, volte all’ Identificazione e Autenticazione degli utenti.

Questo tipo di asset prevede che ogni entità che si registra con la federazione per fornire identità digitali (IDP) fornisca queste tramite un apposito server tipicamente gestito in casa. Questo fa sì che l’utente che vorrà autenticarsi tramite il nostro Captive Portal, per ottenere l’accesso a internet, deve essere messo nella condizione di poter raggiungere l’Identity Provider di appartenenza.

Il Captive Portal, come già spiegato precedentemente, inibisce le connessioni verso qualsiasi host fintanto che l’utente non viene identificato, autenticato e autorizzato. Per poter ottemperare la procedura di identificazione e autenticazione Federata è stata sfruttata la capability chiamata “Walled Garden” messa a

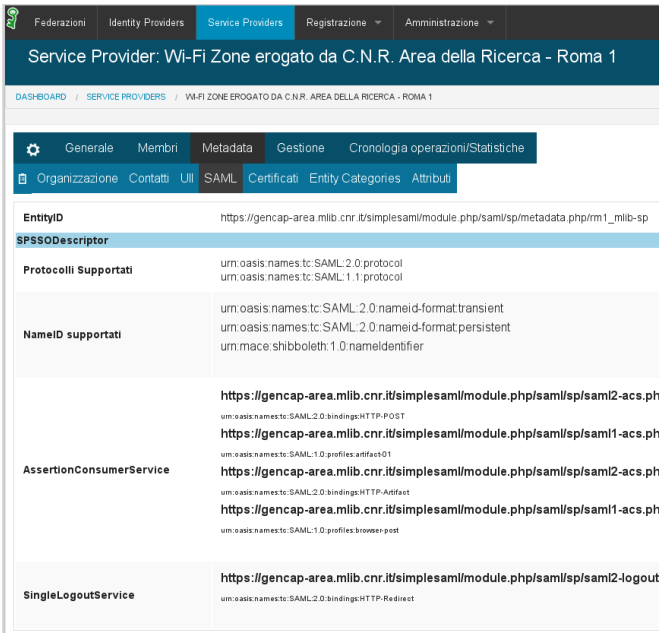


Fig. 4 Portale GARR sezione verifica Metadati

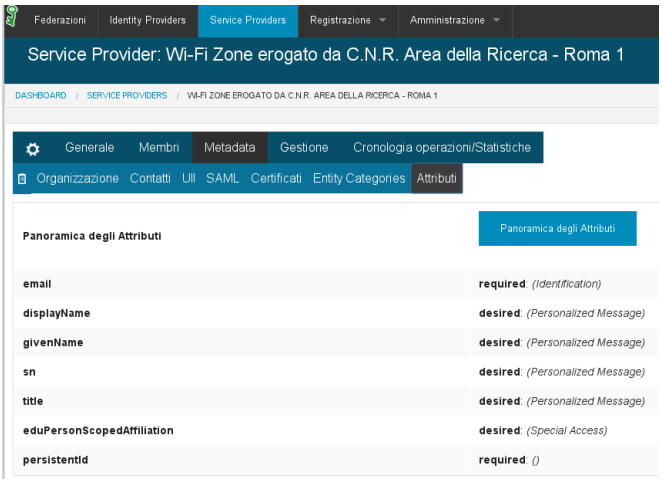


Fig. 5 Portale GARR sezione Attributi richiesti

disposizione da CoovaChilli.

All'interno di CoovaChilli esiste la possibilità di stilare una lista degli host raggiungibili dall'utente a monte dell'autorizzazione altresì obbligatoria (appunto chiamato Walled Garden), la lista degli host concessi può essere implementata per singolo utente tramite gli attributi Radius della connessione oppure può essere stilata all'interno della configurazione di CoovaChilli per essere sfruttata da tutti gli utenti collegati al Captive. Entrambe queste soluzioni sono risultate inefficienti o inutilizzabili al nostro scopo in quanto allo stato attuale si possono contare oltre 3000 Identity Provider (quindi 3000 hosts) e non è pensabile consentire preventivamente la connessione verso un così alto numero di host anche per via del limite stesso del software in uso che prevede un massimo di 1024 slot per lo static garden e altri 1024 per il dynamic garden (max 2048 hosts).

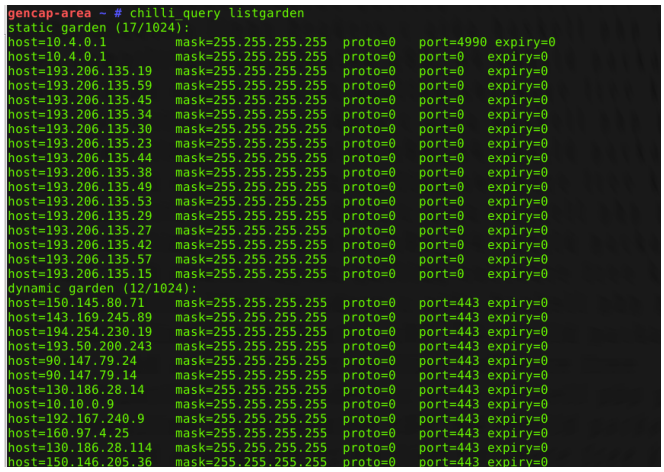
L'altra metodologia non è tuttavia applicabile in quanto è necessario conoscere l'IdP di appartenenza prima che l'utente si colleghi all'HotSpot in modo da comunicare il corretto attributo al server Radius da associare all'utente ancor prima della fase di autenticazione. La soluzione applicata in questo frangente consiste nello sviluppo di una funzione, in codice PHP, che intercetta la scelta dell'IdP di appartenenza da parte dell'utente dalla pagina di WAYF (Where Are You From) del nostro SP e l'aggiunta dell'IdP selezionato al garden globale di CoovaChilli come mostrato in figura 6.

```
<?php

function addgarden($entity){
        $addo=parse_url($entity);
        $garden=$addo['host'];
        if (!isset($addo['port'])){
                $addo['scheme']=="https" ? $port="443" : $port="80";
                }
        else{
                $port=$addo['port'];
        }
        shell_exec("/usr/sbin/chilli_query addgarden data $garden:$port");
}
isset($_GET['idpentityid'])?addgarden($_GET['idpentityid']):null;
$discoHandler = new SimpleSAML_XHTML_IdPDisco(array('saml20-idp-remote', 'shib13-idp-remote'), 'saml');
$discoHandler->handleRequest();
~
~
~
~
```

Fig. 6 Funzione PHP per l'aggiunta dell'IdP al Walled Garden

Questa funzione si avvale del comando "addgarden" della suite CoovaChilli ed è stata inserita all'interno del file disco.php, presente nell'installazione di SimpleSamlPhp, garantendo così l'accessibilità esclusivamente verso l'Identity Provider di turno.



```
gencap-area ~ # chilli_query listgarden
static garden (17/1024):
host=10.4.0.1          mask=255.255.255.255  proto=0   port=4990 expiry=0
host=10.4.0.1          mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.19    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.59    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.45    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.34    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.30    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.23    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.44    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.38    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.49    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.53    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.29    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.27    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.42    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.57    mask=255.255.255.255  proto=0   port=0    expiry=0
host=193.206.135.15    mask=255.255.255.255  proto=0   port=0    expiry=0
dynamic garden (12/1024):
host=150.145.80.71     mask=255.255.255.255  proto=0   port=443 expiry=0
host=143.169.245.89    mask=255.255.255.255  proto=0   port=443 expiry=0
host=194.254.230.19    mask=255.255.255.255  proto=0   port=443 expiry=0
host=193.50.200.243    mask=255.255.255.255  proto=0   port=443 expiry=0
host=90.147.79.24      mask=255.255.255.255  proto=0   port=443 expiry=0
host=90.147.79.14      mask=255.255.255.255  proto=0   port=443 expiry=0
host=130.186.28.14     mask=255.255.255.255  proto=0   port=443 expiry=0
host=10.10.0.9         mask=255.255.255.255  proto=0   port=443 expiry=0
host=192.167.240.9     mask=255.255.255.255  proto=0   port=443 expiry=0
host=160.97.4.25       mask=255.255.255.255  proto=0   port=443 expiry=0
host=130.186.28.114    mask=255.255.255.255  proto=0   port=443 expiry=0
host=150.146.205.36    mask=255.255.255.255  proto=0   port=443 expiry=0
```

Fig. 7 Lista degli host aggiunti al Walled Garden

L'unico limite di questa implementazione è che qualora si presentassero, nella stessa giornata, più di 1024 utenti che richiedono accesso presso altrettanti diversi IdP il 1025 esimo utente non riuscirebbe a contattare il proprio IdP. Poiché questi casi sono statisticamente molto improbabili, riteniamo che la soluzione adottata sia sufficientemente valida.

Al termine dell'autenticazione da parte dell'IdP, un token SAML viene generato e spedito al SP che lo aveva generato, il quale a seguito della verifica del token garantisce o meno l'accesso al servizio; nel nostro caso l'accesso alla rete. Per implementare le dinamiche AAI fornite da SAML con quelle del Captive Portal, a seguito dell'autenticazione da parte dell'IDP si reindirizza il client ad un'apposita landing page che contiene la porzione di codice necessaria alla verifica del token SAML per l'eventuale autorizzazione dell'utente che tenta di accedere.(Fig. 8) I casi d'uso di questo tipo di accesso sono prevedibilmente durante le conferenze che si svolgono presso il Campus o la presenza come ospite all'interno di una determinata struttura, questo presupposto rende evidente che un eventuale utente può sfruttare il medesimo accesso da più dispositivi anche contemporaneamente (ad es. un pc portatile ed il cellulare).

Fig. 8 Codice PHP di verifica token SAML

Per questo motivo è stato di proposito disabilitato lo switch di controllo sessione singola presente nel Radius.

Per dare la possibilità a tutti gli utenti che si collegano di controllare gli accessi: quando e quanti, ma soprattutto da quale dispositivo sono stati effettuati tramite le proprie credenziali è stata realizzata un pagina di riepilogo(Fig. 10), dove è possibile visionare tutti gli accessi effettuati con particolare attenzione alla data, durata della connessione e al MAC-Address del dispositivo utilizzato. Per accedere a questa schermata basta fare click sul link “More info” (indicato dalla freccia rossa nella figura 9) dalla pagina di benvenuto una volta effettuato l’accesso.

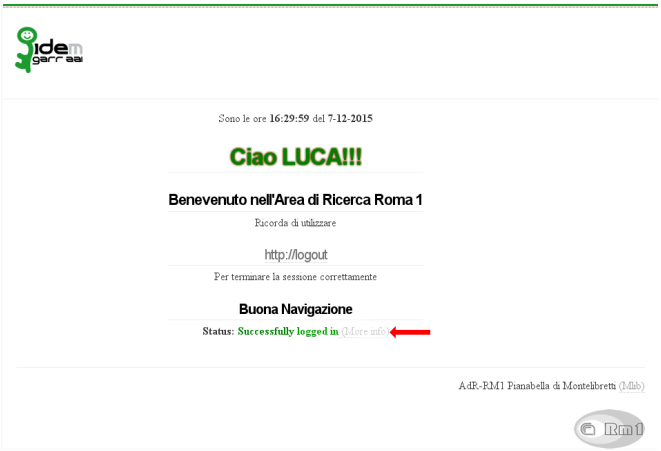


Fig. 9 Messaggio di benvenuto, in evidenza il link alla pagina di riepilogo accessi

La struttura del Portale fa si che tutti gli utenti che ottengono l’accesso alla navigazione vengano identificati su internet attraverso lo stesso indirizzo IP. Per garantire comunque la rintracciabilità dell’utilizzatore finale, nel caso di eventuali infrazioni delle normative vigenti, e stato installato e configurato un software, sempre di matrice Open Source, dal nome Conntrackd.

Questo demone si occupa di registrare l’indirizzo IP sorgente e quello di destinazione di tutte le connessioni che avvengono attraverso il Captive Portal.

Durante il primo accesso alla procedura AAA qui illustrata, è possibile incappare in un errore non gestibile in maniera automatizzata: se l’utente che fa accesso al portale tenta di raggiungere una pagina con connessione protetta (HTTPS) il portale non sarà in grado di effettuare correttamente il redirect alla pagina di login, si otterrà invece un errore di errato certificato e pagina non raggiungibile a causa delle dinamiche SSL e dell’accesso ancora non garantito. In CoovaChilli è previsto il redirect per le connessioni SSL ma anche abilitando questa opzione si incapperebbe in un errore dei certificati di sicurezza, anche per questo motivo è preferibile non abilitare questa opzione. L’utente che vuole effettuare l’accesso dovrà provare ad accedere ad una pagina non protetta da SSL per essere correttamente reindirizzato alla pagina di login.

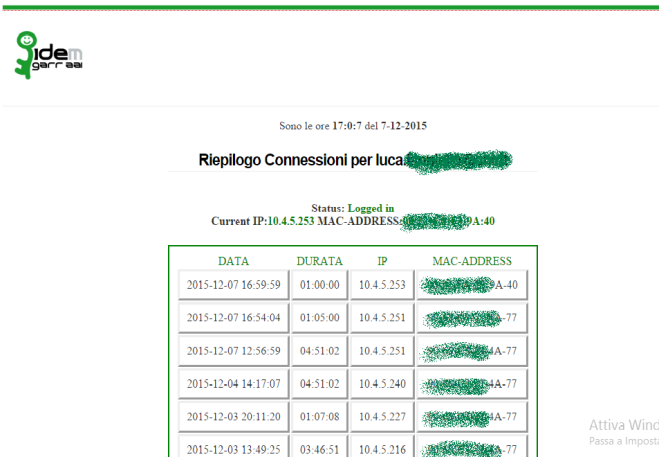


Fig. 10 Pagina riepilogo accessi effettuati

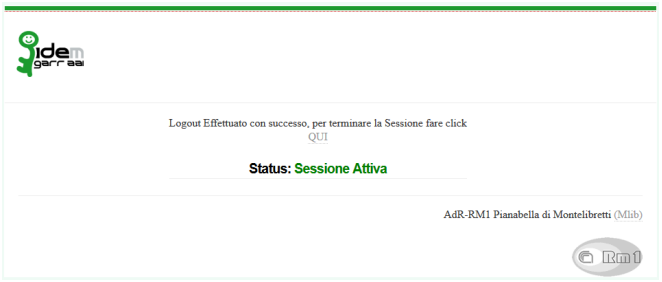


Fig. 11 Pagina di verifica sessione a seguito del logout

Un’altra accortezza che occorre utilizzare nel caso più utenti utilizzino la medesima PDL in condivisione è la procedura di Logout: una volta effettuato l’accesso tramite il portale viene instaurata una sessione che rimane attiva fintanto che l’utente mantiene aperto il browser, questo comporterebbe che un utente potrebbe navigare attraverso il portale tramite la sessione ancora attiva dell’utente che lo ha preceduto. I browser di ultima generazione, come Chrome, hanno sviluppato una capacità intrinseca che permette ad un eventuale utente di mantenere la sessione attiva nonostante il browser venga chiuso e successivamente riaperto, molto utile per l’utente singolo che non dovrà reimmettere le proprie credenziali ove richieste, male invece nel caso di una PDL utilizzata da più utenti, in questo caso viene consigliato l’utilizzo di Mozilla Firefox, che se correttamente utilizzato, evita di lasciare sessioni attive riutilizzabili da altri utenti che potrebbero navigare con la sessione dell’utente che lo ha preceduto. Per chiudere correttamente la sessione con il Captive Portal è previsto l’utilizzo di un URL speciale: http://logout

Visitando questa url speciale verrà visualizzata la procedura di Logout.

L’utilizzo di questo indirizzo fa si che il SP chiuda la sessione attiva dell’utente, tuttavia si riscontra che se l’IdP utilizzato per l’autenticazione è privo del servizio di SingleLogOut, come nella maggior parte dei casi, lo stesso continua a mantenere la ses-

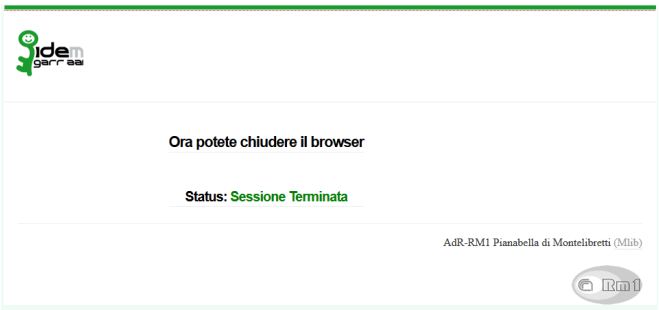


Fig. 12 Messaggio di conferma di avvenuta chiusura sessione

sione utente attiva. In questo caso se dal browser Chrome con il quale è stata effettuato il "logout" e successivamente chiuso, si tentasse di accedere nuovamente tramite il medesimo IdP ed il medesimo Chrome, verrà ripristinata in maniera automatica la sessione dell'utente precedente a causa dell'IdP sul quale la vecchia sessione risulta ancora attiva. Se per la navigazione si utilizza Mozilla Firefox tutto funziona "as aspected".

5 Conclusioni

Anche in questa occasione ciò che risulta evidente è l'estrema flessibilità ed adattabilità dei software utilizzati in completa armonia con l'ambiente che lo contraddistingue: l'OpenSource.

Il servizio di accesso alla rete Federato risulta essere un utile strumento per consentire a coloro che si trovano al di fuori della propria sede operativa di potersi connettere ad internet digitando le proprie credenziali senza dover richiedere permessi ai responsabili delle infrastrutture ospitanti. Soprattutto nell'ambito della ricerca e dell'università, dove esiste una continua e numerosa mobilità, l'accesso alla rete per mezzo di un IdP federato.

Un caso pratico è quello dell'AdR-RM1 ove è presente una Foresteria ed una infrastruttura di accesso wireless, l'Ospite è in grado di collegarsi autonomamente ad Internet utilizzando le credenziali fornite dal proprio Ente di appartenenza qualora questo ultimo appartenga alla Federazione IDEM.

6 Glossario

AAI	(Authentication and Authorization Infrastructure)
AUP	(Acceptable Use Policy)
IDEM	(IDEntity Management per l'accesso federato)
RADIUS	(Remote Authentication Dial-In User Service)
SAML	(Security Assertion Markup Language)
SP	(Service Provider)
IdP	(Identity Provider)
PDL	(Postazione Di Lavoro)

Riferimenti

1 A. Pifferi, G. Nantista, L. Ianniello, C. Ricci, L. Rossi, M. Simonetti, Un captive portal per l'utenticazione su reti wifi dedicate agli internet access point liberi., Smart eLab 2 (2013) 15–19. doi:10.30441/smart-elab.v2i0.55.
2 https://www.idem.garr.it/.
3 https://www.coova.github.io/.
4 http://saml.xml.org/saml-specifications/.
5 https://www.gentoo.org/.
6 http://freeradius.org/.
7 https://registry.idem.garr.it/.