Università degli Studi di Camerino

SCUOLA DI SCIENZE E TECNOLOGIE

Corso di Laurea in Informatica (Classe L-31)

Accesso Wi-Fi con autenticazione Federata IDEM.

Laureando
Sandro Massini

Matricola 060648

Relatore
Prof. Fausto Marcantoni

A.A. 2020/2021

Indice

Introduzione

L'obiettivo della tesi è stato lo studio del sistema di Autenticazione e Autorizzazione Federata IDEM [1], tramite l'installazione e la configurazione di un Captive Portal [2] WiFi con la distribuzione Linux Zeroshell [3].

Il Captive Portal realizzato, integrato all'interno della federazione IDEM del GARR [4], consente agli utenti autenticati ed autorizzati di accedere alla rete WiFi del Dipartimento di Economia dell'Università degli Studi di Perugia.

IDEM è la Federazione Italiana delle Università e degli Enti di Ricerca per l'Autenticazione e l'Autorizzazione. IDEM permette di accedere a numerosi servizi federati utilizzando la propria identità digitale istituzionale. Ad esempio, si può accedere alle riviste elettroniche dovunque ci si trovi utilizzando la stessa username e password che si usa per il WiFi universitario e la posta elettronica. La maggior parte delle università e tutti i maggiori enti di ricerca italiani fanno già parte di IDEM. Il servizio IDEM GARR AAI è l'operatore di federazione. Il servizio IDEM garantisce il buon funzionamento tecnico della federazione ed il rispetto degli standard in accordo con gli altri operatori di federazione a livello europeo e mondiale.

La Federazione Italiana d'Infrastrutture di Autenticazione e Autorizzazione della rete GARR rende facile e sicuro l'accesso a servizi condivisi con una unica chiave di accesso. Questo aspetto, che caratterizza la sicurezza informatica si basa essenzialmente su tre principi fondamentali per quanto riguarda l'accesso ai dati: l'identificazione (identity), l'autenticazione (authentication) che può avvenire tra soggetti appartenenti alla stessa organizzazione oppure ad organizzazioni differenti e l'autorizzazione (authorization) che consiste nel verificare i permessi per l'accesso ai servizi disponibili.

Il sistema per l'accesso federato a IDEM GARR è basato sul software opensource Shibboleth [5]. Il Consortium GARR fa parte del Consortium Shibboleth. Quest'ultimo è stato fondato da Internet2, Janet e Switch per sostenere lo sviluppo del software Shibboleth. Attualmente il Consortium Shibboleth conta i tre soci fondatori e quindici ulteriori membri. Il GARR, in quanto coordinatore della Federazione IDEM, manifesta il proprio impegno a sostenere attivamente lo sviluppo di Shibboleth. Shibboleth è un

sistema di single sign-on (login) per reti informatiche. Consente di autenticarsi su sistemi differenti, permettendo di effettuare il login su reti di organizzazioni o istituzioni diverse, utilizzando una sola identità. Il sistema Shibboleth è composto da tre elementi fondamentali, un Service Provider, un Identity Provider e un Where Are You From.

Nell'Università degli Studi di Perugia è già esistente un servizio di Shibboleth IdP, gestito dall'Ufficio Reti per autenticare via web gli utenti dei servizi universitari protetti con Shibboleth. In questo progetto è stato installato e configurato un SP Dipartimentale sviluppando la comunicazione con il servizio di IdP d'Ateneo e lo scambio di informazioni tra i due servizi, per l'autorizzazione ed il riconoscimento dell'utente.

Nella prima parte della tesi si trattano i concetti teorici funzionali al lavoro svolto, spiegato nei capitoli finali.

Nel primo capitolo vengono descritti i concetti di AAI e di Single Sign-On.

Il secondo capitolo descrive la federazione IDEM.

Il terzo capitolo descrive il software Shibboleth.

Il quarto capitolo descrive la configurazione del Service Provider Shibboleth con la distribuzione Linux Zeroshell per la realizzazione del Captive Portal WiFi integrato con la federazione IDEM.

Il quinto capitolo descrive i risultati ottenuti con le schermate di funzionamento.

1 Infrastrutture di AAI

1.1 Le AAI (Authorization and Authentication Infrastructure)

Una AAI (Authentication and Authorization Infrastructure) è un'architettura nata per semplificare l'accesso ai vari servizi forniti da organizzazioni diverse.
Una AAI gestisce le procedure di autenticazione e di autorizzazione tra un utente, la sua organizzazione di origine e i servizi offerti, in base al concetto di gestione federata delle identità.
Una gestione delle identità federate consente di utilizzare le informazioni di identità in domini di sicurezza, per cui i fornitori di servizi possono collaborare con i fornitori di identità.
In un'infrastruttura di identità federata, coloro che forniscono i servizi e le organizzazioni di appartenenza degli utenti possono scambiarsi informazioni sull'identità degli utenti stessi in modo sicuro e rispettoso, garantendo per gli utenti finali i diritti di riservatezza.
I soggetti coinvolti scambiano informazioni sia sugli utenti sia sulle risorse disponibili formando così una federazione.
In questo modo l'utente può accedere ad un qualsiasi servizio tramite le credenziali della propria organizzazione.
Tutto ciò porterà numerosi vantaggi e consentirà:

- all'utente di utilizzare le credenziali fornite dal proprio ente di appartenenza;
- i dati di ogni utente saranno conservati unicamente dalla propria organizzazione di appartenenza;
- al fornitore di servizi di evitare di dover gestire le credenziali personali degli utenti.

Vediamo un esempio.
Generalmente tutti gli utenti che possano accedere alla WiFi devono necessariamente registrarsi sulla piattaforma in modo da potervi accedere mediante l'inserimento di username e password (il servizio dovrà memorizzare al suo interno l'indirizzo e-mail

dell'utente e la password del profilo di ricerca associati a quell'username e a quella password).
Vediamo come una AAI modifica l'approccio e quali sono i vantaggi.
Da parte dell'ente che fornisce il servizio si evita la duplicazione delle informazioni anagrafiche, e si avrà una maggiore sicurezza dal momento che gli utenti generalmente utilizzano per ogni registrazione la stessa username e la stessa password; inoltre, le credenziali risiedono soltanto nel server della propria istituzione.

1.2 Identificazione, Autenticazione, Autorizzazione

Esaminiamo questi tre concetti nel dettaglio.

Identificazione: L'identificazione è il processo di presentazione di un'identità a un sistema. Viene eseguito nelle fasi iniziali di accesso al sistema ed è ciò che accade quando si afferma di essere un determinato utente del sistema. La richiesta può assumere la forma di fornire il nome utente durante la procedura di accesso; posizionando il dito su uno scanner; assegnando il tuo nome a un elenco di invitati o qualsiasi altro formato in cui rivendichi un'identità con l'obiettivo di ottenere l'accesso. L'identificazione non è necessaria per alcuni sistemi, come le carte bancomat, in cui chiunque abbia il codice corretto può accedere al proprio account senza identificarsi.

Autenticazione: L'autenticazione è il processo che verifica l'identità di un utente in modo da poter correttamente permettere o negare l'accesso a risorse condivise e protette. Di fatto, tramite l'autenticazione, si associa un'utente con la sua identità digitale presente nel sistema. Le tecniche di autenticazione possono spaziare dal semplice login con username e password a meccanismi più complessi e forti come token, certificati digitali a chiave pubblica o sistemi biometrici. Una soluzione di IAM (Identity and Access Management) deve pertanto essere indipendente dal meccanismo di autenticazione utilizzato in modo da potersi adattare ad ogni specifica realtà tecnologica.

Autorizzazione: L'autorizzazione è il passo successivo dopo che un utente è stato autenticato. È il processo che consente l'accesso alle risorse solamente a coloro che hanno i diritti di usarle. Durante l'autorizzazione vengono quindi valutati i privilegi dell'identità digitale associata all'utente autenticato e viene consentito, limitato oppure impedito l'accesso alla risorsa, applicando opportune regole stabilite in precedenza. In ambito universitario si può pensare, a titolo d'esempio, ad una applicazione web per gestire gli esami: studenti e professori si possono autenticare entrambi a questa risorsa, ma durante il processo di autorizzazione si distinguono studenti da professori, ed i primi potranno effettuare l'iscrizione agli esami, mentre i secondi potranno aggiungere, modificare o eliminare gli esami inseriti, ma chiaramente non dev'essere possibile il contrario.

1.2.1 Approccio tradizionale ai processi di autenticazione e autorizzazione

L'approccio tradizionale ai processi di autenticazione e autorizzazione richiede che ogni utente debba effettuare l'autenticazione per ogni servizio a cui accede; quindi, ogni utente deve possedere uno o più username e una o più password ed inserirli di volta in volta per utilizzare le varie risorse.

Questo processo comporta grossi svantaggi sia da parte del fornitore dei servizi, sia da parte di chi utilizza assiduamente servizi informativi su internet (banche, riviste elettroniche, e-commerce, ...).

Infatti, per gli utenti nasce l'esigenza e la difficoltà di dover innanzitutto gestire e ricordare un numero elevato di username e password, cosa che porta molti utenti ad utilizzare la stessa password per più servizi, consentendo quindi agli esperti di intercettarle facilmente.

Inoltre, i gestori di servizi, con grande dispendio di risorse, devono continuamente mantenere tutte le informazioni di tutti gli utenti, sia interni sia esterni, che vogliono accedere al servizio.

Inoltre, tutti i dati relativi agli utenti sono noti anche al di fuori della propria organizzazione, un aspetto che va a minare la loro privacy e che aumenta il rischio di intercettare la loro identità.

Ovviamente non esiste comunicazione tra le varie organizzazioni e condivisione delle risorse offerte.

1.3 Sistema Single Sign-On (SSO)

SSO [6], acronimo di Single Sign-On, è un sistema di autenticazione e controllo accessi. È un processo di autenticazione che consente l'accesso a più risorse, servizi digitali e applicazioni con un solo set di credenziali (le classiche username e password), senza dover quindi costringere gli utenti a ricordare tante password, situazione quest'ultima che spesso rappresenta una vulnerabilità di sicurezza.

1.4 SSO, cos'è e cosa significa Single Sign-On

Il Single Sign-On è traducibile come "autenticazione unica" e rappresenta la proprietà di un sistema di controllo degli accessi di consentire ad un utente di effettuare un unico processo di autenticazione (cioè di inserire username e password una sola volta) per accedere a più sistemi software, servizi digitali e applicativi o risorse informatiche per le quali gli è consentito l'accesso, senza dover ogni volta ripetere l'autenticazione per ogni singola risorsa o applicazione.
Sono moltissime oggi le istituzioni che ricorrono a questo sistema di autenticazione, perché gli ambienti IT sono sempre più eterogeni e distribuiti e le risorse sparse in sistemi sia interni sia esterni. Ogni servizio applicativo può essere fruito dagli utenti previa autenticazione: prima dell'avvento del Single Sign-On ciò significava dover effettuare l'accesso alle risorse inserendo ogni volta username e password, per ogni singola applicazione, prestando attenzione ad utilizzare credenziali differenti per ogni risorsa. Dove ancora non si è ricorso al SSO si sperimentano conseguenze negative non solamente sulla user experience ma anche sulla sicurezza e sulla gestione del sistema di autenticazione.
Un SSO assicura una migliore user experience, da un lato, semplifica la gestione IT e della sicurezza informatica, dall'altro, con impatti diretti anche sui costi (per esempio riducendo tempi e attività dell'help desk).

1.5 Come funziona il Single Sign-On

Il Single Sign-On si basa su tre passaggi chiave.

Identificazione - CHI SEI?
Autenticazione - DIMOSTRA CHI SEI
Autorizzazione - ACCESSO ALLE RISORSE PROTETTE

In termini tecnologici il SSO è un componente delle soluzioni di Identity Management, ma per creare un sistema di Single Sing-On si possono seguire tre differenti approcci:

- Approccio centralizzato

In questo caso viene predisposto un database unico e centralizzato di tutti gli utenti e anche le policy di gestione della sicurezza vengono centralizzate. Si ricorre a questo tipo di architettura quando le risorse IT sono tutte riconducibili alla stessa rete.

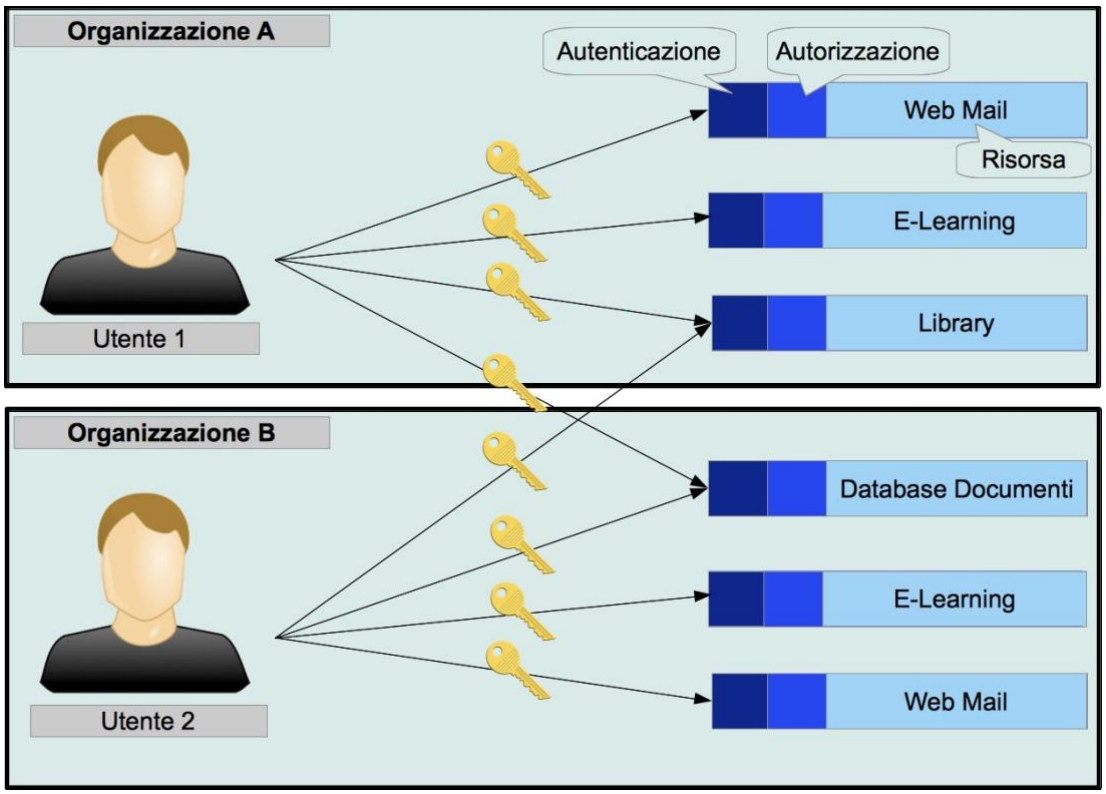


Figura 1.1 [7]

- Approccio federativo

La federazione, di fatto, consiste in un accordo tra istituzioni differenti che gestiscono i dati di uno stesso utente e consentono a quest'ultimo di poter accedere alle risorse (di istituzioni diverse) autenticandosi una sola volta. Grazie al Federated Identity Management, l'accesso ad uno dei sistemi federati permette automaticamente l'accesso a tutti gli altri sistemi collegati.
In questo caso ogni gestore federato mantiene il controllo della propria politica di sicurezza; tuttavia, per gli utenti l'accesso alle risorse diventa molto più agile e semplificato.

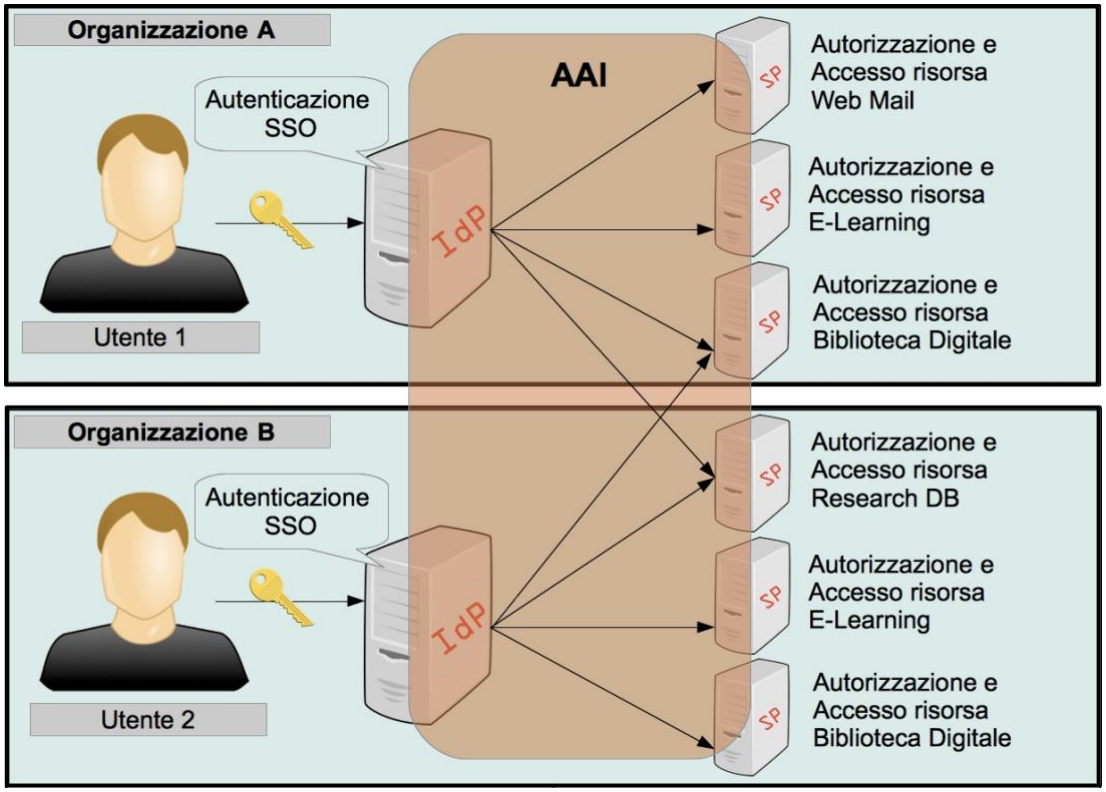


Figura 1.2 [7]

- Approccio cooperativo

Simile all'approccio federativo che consente a ciascun gestore di governare in modo indipendente la propria politica di sicurezza, il modello cosiddetto cooperativo di SSO tiene conto della relazione di "dipendenza" tra un utente ed un'entità (università, laboratori di ricerca, amministrazioni, ecc.). Tenendo dunque conto che ciascun utente

dipende, per ciascun servizio, da uno solo dei gestori cooperanti, nel caso di richiesta di accesso alla rete locale, l'autenticazione viene effettuata dal gestore che ha in carico l'utente per quel tipo di richiesta/accesso; verrà fatta da un gestore differente nel caso in cui la richiesta di acceso ad un servizio dipenda da un altro gestore ma in modo trasparente per l'utente e senza penalizzazioni sul fronte della user experience.

1.5.1 I vantaggi del SSO

Le istituzioni che decidono di adottare sistemi di autenticazione basati su Single Sign-On lo fanno principalmente con obiettivi differenti:

- semplificare la gestione delle password: maggiore è il numero delle password da gestire, maggiore è la possibilità che vengano utilizzate password simili le une alle altre e facili da memorizzare, abbassando così il livello di sicurezza;
- semplificare la gestione degli accessi ai vari servizi;
- semplificare la definizione e la gestione delle politiche di sicurezza.

Il Single Sign-On presenta diversi vantaggi: lato utente, si agevola la gestione e l'utilizzo di numerose risorse a cui deve accedere per lavorare. Il beneficio di facilitare la gestione delle password attraverso il Single Sign-On rappresenta un traguardo importante che evita i problemi succitati di creazione e memorizzazione di infinite password e credenziali, il rischio di smarrimento delle stesse e il conseguente abbassamento del livello di sicurezza.
L'uso del SSO aiuta a semplificare quindi tanto la gestione degli accessi ai vari servizi, quanto la definizione e la gestione delle politiche di sicurezza.
Sempre lato utente, nell'implementazione del modello SSO che rappresenta ad oggi una modalità di identificazione molto richiesta dalle aziende, diventa più trasparente anche all'utente stesso il processo di autenticazione, senza lasciargli più la responsabilità della gestione sicura dei suoi accessi. Inoltre, con questa procedura le proprie credenziali non lasciano mai il dominio di autenticazione, si riducono i costi operazionali così come il tempo per accedere ai dati. Lato provider di soluzioni digitali, il maggior vantaggio dell'implementazione del Single Sign-On, è rappresentato

dall’elemento cruciale di affidare ad altri l’intero processo di autenticazione dell’utenza e la sicurezza ad esso correlata. Lato amministratori di sistema, la procedura con SSO permette una più efficace gestione e manutenibilità della sicurezza ottimizzata e facilitata.

2 La Federazione IDEM

2.1 La Federazione

La Federazione può essere vista come un accordo tra organizzazioni e fornitori di risorse.
Con tale accordo i partecipanti decidono di fidarsi reciprocamente delle informazioni che si scambiano nei processi di AA (Autenticazione e Autorizzazione), sulla base di regole e norme stabilite per gestire le relazioni di fiducia.
Un ambiente federato rappresenta un sistema di sicurezza in grado di far interagire fra loro differenti sistemi informatici, utilizzando protocolli che garantiscano l'identità degli utenti appartenenti a ciascuna organizzazione facente parte della Federazione.
L'Identità Federata si basa sul fatto che si ha piena fiducia dei sistemi di autenticazione e autorizzazione tra le associazioni federate al fine di consentire l'accesso alle proprie applicazioni.

2.2 Funzionamento generale di un'infrastruttura AAI

Un'AAI (Authentication and Authorization Infrastructure) consente di centralizzare la gestione dei profili digitali degli utenti, all'interno di un'organizzazione, centralizzando anche il processo di autenticazione (chi è?) per l'accesso alle risorse on-line.
Una volta accertata l'identità è necessario decidere se l'utente può, e con quali diritti, accedere alla risorsa.
Questa fase (autorizzazione) resta a carico del fornitore della risorsa o servizio (Service Provider) che potrà però disporre, nel processo decisionale, di informazioni affidabili rilasciate da chi ha autorità a farlo (es. Ufficio del Personale, Ufficio Progetti ecc.).

L’accesso federato permette agli utenti di accedere a diversi servizi in modo sicuro, tutelando allo stesso tempo la privacy, attraverso un insieme di credenziali fornite dalla loro organizzazione, generalmente un’università o un centro di ricerca (il fornitore di identità).
Infatti, solo gli utenti che sono in possesso di credenziali valide fornite e registrate precedentemente da ogni organizzazione alla propria utenza, possono aver accesso ai servizi forniti dalla federazione.
L'idea è quella di favorire l'accesso alle risorse evitando che ogni utente debba inserire ogni volta per tutti i servizi di interesse le sue credenziali, questo evita di dover gestire e ricordare tante credenziali quanti sono i servizi a cui si ha accesso.
In una AAI ogni servizio è accessibile tramite un solo login gestito dall’organizzazione di appartenenza dell'utente.
La creazione di una federazione che accoglie diverse organizzazioni collegate alla propria rete, permette agli utenti di accedere a svariati servizi tramite una procedura standard di autenticazione, che consiste nell'inserimento di un solo username e una sola password rilasciata dalla propria organizzazione di appartenenza.

2.3 La federazione IDEM

IDEM (IDEntity Management per l’accesso federato), è la Federazione italiana di Infrastrutture di Autenticazione e Autorizzazione della comunità dell’istruzione e della ricerca. La Federazione IDEM è gestita e coordinata da GARR.
La Federazione IDEM è la terza parte fidata (Trusted Third Party - TTP) che permette di stabilire in modo efficace relazioni di fiducia tra gli enti di formazione e di ricerca italiani e i partner che forniscono le risorse on-line.
La Federazione IDEM è costituita da organizzazioni della comunità GARR al fine di facilitare le operazioni di autenticazione e di autorizzazione per l’accesso a risorse di interesse per la comunità della ricerca e dell’educazione.

Le organizzazioni stabiliscono regole e linee di condotta comuni per la gestione di relazioni di fiducia basate su di una terza parte fidata, l'operatore di Federazione.
I partecipanti alla Federazione inoltre concordano su una serie di regole finalizzate allo scambio di informazioni sugli utenti finali e sulle risorse, per consentire l'accesso e l'utilizzo delle risorse e dei servizi, condivisi in modo sicuro e nel rispetto della privacy dell'utente finale e delle norme in materia di protezione dei dati.
Il Consortium GARR ha il ruolo di operatore di Federazione e autorità di registrazione al quale ogni Organizzazione richiede l'adesione alla Federazione. GARR mette a disposizione un servizio tecnico-amministrativo di supporto denominato "Servizio IDEM GARR AAI".
La Federazione IDEM implementa gli standard di identità federata basati su SAML [8] 2.0 e riconosciuti ed utilizzati a livello internazionale. La Federazione IDEM partecipa alle attività di REFEDS, il gruppo degli operatori di federazioni di identità del mondo della ricerca e dell'educazione.
IDEM opera all'interno della comunità dell'istruzione e della ricerca connessa alla rete GARR, supportando l'adozione di un framework comune per l'accesso alle risorse on line.
IDEM è una federazione di identità basata sullo standard SAML (Security Assertion Markup Language), tecnologia che permette lo scambio di dati di autenticazione e autorizzazione (asserzioni) tra domini di sicurezza distinti denominati identity provider (entità che fornisce informazioni di identità) e service provider (entità che fornisce servizi). Il formato delle asserzioni SAML è basato su XML [9].
L'uso dello standard SAML è dedicato a risolvere il problema del web Single Sign-On (SSO).
Grazie al servizio di federazione gli Identity Provider possono fornire ai propri utenti meccanismi di SSO e protezione della privacy e i Service Provider possono ottenere un miglior controllo degli accessi verso risorse protette eliminando la gestione account utenti che viene demandata ai sistemi di gestione delle identità degli Identity Provider.

Esempio di accesso federato.

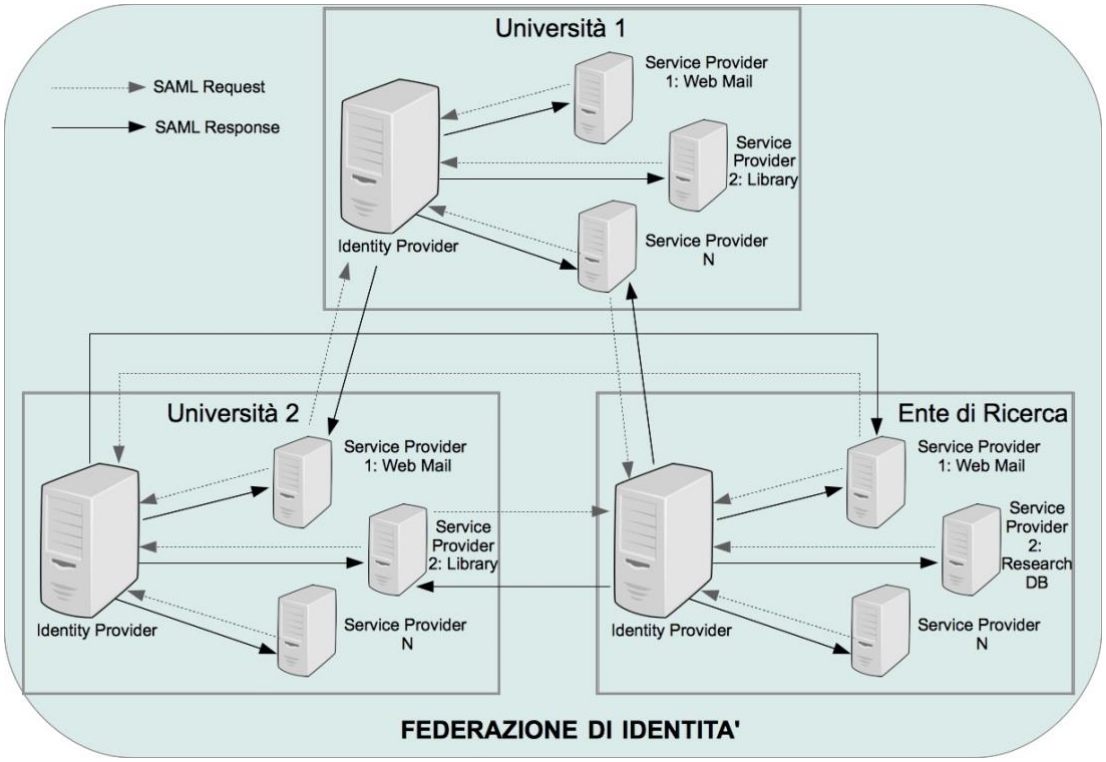


Figura 2.1 [7]

Un utente si collega ad una risorsa web offerta da un fornitore di servizi di terze parti, ad esempio un servizio di consultazione di una rivista elettronica di uno specifico editore. Scegliendo la modalità di login "Accesso istituzionale" l'utente viene rediretto alla pagina di login della propria Istituzione di appartenenza ed usa le credenziali istituzionali, le stesse usate per l'accesso ai servizi interni.

Dopo un'autenticazione con successo, il sistema di identità istituzionale trasmette al fornitore di servizi l'identità dell'utente, rappresentata da un insieme minimo di attributi. Il fornitore di servizi utilizza queste informazioni per autorizzare l'utente all'accesso alla risorsa web.

2.3.1 Scopi e obiettivi

L'obiettivo principale di IDEM è di creare e supportare un framework comune agli enti di formazione e di ricerca italiani per l'accesso alle risorse on-line tramite l'identità digitale istituzionale.
La Federazione si propone di svolgere le seguenti attività:

- permettere agli utenti della comunità GARR (ad esempio ricercatori, docenti, studenti) l'accesso alle risorse in rete tramite procedure di autenticazione e autorizzazione che semplifichino la condivisione e l'utilizzo delle risorse stesse anche tra diverse organizzazioni;
- garantire all'utente finale il trattamento dei propri dati personali nel rispetto della privacy e con la necessaria sicurezza nella trasmissione delle informazioni;
- ridurre o eliminare la necessità per gli utenti finali della Federazione di mantenere più credenziali per poter accedere a risorse in rete offerte da fornitori diversi;
- ridurre l'onere per i fornitori di risorse di gestire le complesse procedure di accreditamento e di amministrazione degli utenti;
- facilitare la collaborazione grazie alla condivisione di risorse accessibili tramite connessioni protette ovvero attraverso rapporti di fiducia e regole concordate;
- favorire la disponibilità di servizi diffondendo una cultura di interoperabilità;
- favorire l'aggregazione secondo una logica a rete;
- promuovere la Federazione attraverso interventi mirati a far conoscere e pubblicizzare le sue finalità, la sua conoscenza e i suoi obiettivi ivi inclusa la partecipazione della Federazione a progetti di ricerca in ambito nazionale ed internazionale.

2.3.2 Il Servizio IDEM GARR AAI

Il Consortium GARR mette a disposizione un servizio tecnico e amministrativo di supporto denominato "Servizio IDEM GARR AAI". Il Servizio IDEM GARR AAI, in termini tecnici, svolge le funzioni di operatore di federazione (Federation Operator).

Il Servizio IDEM GARR AAI ha il compito di:

- gestire i servizi offerti dal GARR alla Federazione ed indicati nelle Norme di Partecipazione;
- valutare, per quanto di sua competenza, il possesso dei requisiti di partecipazione delle Organizzazioni ai fini dell'ingresso e della persistenza in Federazione;
- controllare e verificare la persistenza dei requisiti tecnici e il buon funzionamento dei Servizi registrati dai Partecipanti;
- eseguire attività di monitoraggio e auditing;
- contribuire a mantenere la Federazione allo stato dell'arte degli standard e delle tecnologie disponibili partecipando attivamente a gruppi di lavoro nazionali ed internazionali;
- supportare gli organi di governo della Federazione con rapporti periodici e nella redazione dei documenti legali, della documentazione tecnica e dei rapporti annuali.

2.3.3 Servizi e contenuti accessibili tramite la FEDERAZIONE IDEM

Il numero di servizi accessibili tramite la Federazione IDEM cresce sempre di più. Ne sono un esempio:

- servizi di biblioteca digitale come ad esempio banche dati, articoli full text, document delivery;
- servizi e-learning;
- strumenti di community (wiki e blog);
- servizi di prenotazione (prenotazione ed utilizzo di stanze virtuali per multivideoconferenze, ecc.).

Per elaborare tale struttura, la Federazione IDEM ha scelto di adottare la tecnologia Shibboleth, un software open source attualmente più diffuso per l'accesso a risorse e servizi web.

2.3.4 Partecipanti della Federazione

Ai fini dell'adesione alla Federazione è indispensabile la partecipazione con un Servizio, che può essere:

- un Servizio di gestione e verifica delle identità, tramite la messa in opera di un componente software denominato Identity Provider (IdP);
- una Risorsa accessibile in rete a seguito di una procedura di autenticazione e autorizzazione, tramite la messa in opera di un componente software denominato Service Provider (SP).

La partecipazione alla Federazione è gratuita.

Esistono due tipologie di Partecipanti: Membri e Partner:

- le organizzazioni facenti parte della comunità GARR ed in possesso dei requisiti possono richiedere l'adesione alla Federazione in qualità di Membri;
- ogni Ente aderisce alla Federazione come organizzazione unitaria;
- le organizzazioni esterne a GARR, ed in possesso dei requisiti, possono richiedere di partecipare alla Federazione in qualità di Partner.

Ogni Membro deve nominare un Referente Organizzativo (RO) che rappresenti a tutti gli effetti l'organizzazione partecipante ed un Referente Tecnico (RT) di raccordo con l'infrastruttura tecnica della Federazione che farà le veci del RO in sua assenza.
Il Referente Tecnico deve avere autorevoli competenze tecniche riguardo la configurazione complessiva dei sistemi informativi dell'organizzazione di appartenenza.
Ogni Partner può nominare un Referente Organizzativo (RO) che rappresenti a tutti gli effetti l'organizzazione partecipante.
Possono entrare a far parte della Federazione IDEM, in qualità di membri, tutti gli enti connessi alla Rete Italiana dell'Università e della Ricerca GARR. Possono inoltre partecipare alla Federazione IDEM, in qualità di partner, organizzazioni terze (ad esempio editori, fornitori di software o servizi online, ecc), purché forniscano contenuti o servizi che siano ritenuti utili alla Comunità GARR.

Per partecipare alla Federazione IDEM come Membro o come Partner occorre sottoscrivere il Modulo di Adesione e sottomettere contestualmente la Richiesta di registrazione di un servizio (IdP o SP).
Le Organizzazioni, richiedendo l'adesione alla Federazione con la sottoscrizione della Richiesta di Adesione (RA) o dell'Accordo di Collaborazione (AC), accettano il Regolamento della Federazione IDEM (RFI) e le Norme di Partecipazione (NdP).
Al ricevimento della richiesta di adesione, il Servizio IDEM GARR AAI provvede ad effettuare i necessari controlli tecnici e di sicurezza e comunica al richiedente l'esito della richiesta.
All'avvenuta approvazione della richiesta di adesione del nuovo partecipante, il Servizio IDEM GARR AAI provvederà ad assistere il richiedente nel trasferimento del suo servizio dalla Federazione di Test alla Federazione di Produzione.

2.3.4 Entrare nella federazione IDEM

Gli enti che possono aderire alla Federazione sono quelli appartenenti alla comunità GARR (membri) e quelli interessati a condividere i propri servizi (partners).
La condizione necessaria per partecipare alla Federazione è la registrazione di almeno uno dei servizi scelti tra l'Identity Provider e il Service Provider.
I requisiti per entrare a far parte della Federazione sono:
- per le organizzazioni GARR:

- implementazione di un Identity Provider o di un Service Provider conforme allo standard SAML;
- conservazione dei log per associare un utente ad una sessione di autenticazione;
- disponibilità a fornire informazioni in merito al sistema di accreditamento e gestione degli utenti adottato;

- per i fornitori di servizi e contenuti:

- adeguamento agli standard tecnici scelti dalla Federazione;
- riservatezza verso i terzi rispetto alle informazioni utente di cui si entri in possesso tramite i servizi della Federazione IDEM;
- realizzazione del servizio in conformità alle specifiche tecniche IDEM GARR AAI.

2.3.5 Impegni dei partecipanti

Tutti i partecipanti si impegnano ad accettare le condizioni e le regole sotto riportate per il periodo di durata dell'accordo:

- effettuare le modifiche che saranno decise dalla Federazione, incluse quelle relative alle specifiche tecniche o alle regole di partecipazione, entro i tempi previsti;
- riconoscere alla Federazione il diritto di pubblicare e utilizzare i metadati necessari al suo funzionamento;
- riconoscere alla Federazione il diritto di pubblicare il nome dell'Organizzazione per scopi di promozione della Federazione stessa;
- evitare ogni atto che abbia come conseguenza un danno, una violazione delle misure di sicurezza o un effetto negativo sulla reputazione per gli altri Partecipanti e la Federazione;
- collaborare con la Federazione nel momento in cui si effettuano dei controlli periodici (auditing);
- adottare regole tecniche e organizzative al fine di favorire il rispetto del diritto d'autore e della legislazione correlata ai contenuti e ai servizi messi a disposizione dagli altri Partecipanti e dalla Federazione.

L'appartenenza alla Federazione non garantisce agli utenti finali del Partecipante l'accesso alle Risorse della Federazione. Per avere libero accesso, infatti, bisogna che gli accordi siano concordati tra le parti stesse.

2.3.6 Servizi della Federazione

Il GARR, tramite il Servizio IDEM GARR AAI, mette a disposizione della Federazione i seguenti servizi:

- il catalogo e i metadati dei servizi disponibili. I partecipanti si impegneranno a comunicare eventuali aggiornamenti di tali informazioni;

- fornisce alle Organizzazioni della Comunità GARR il know-how per la realizzazione dei servizi attraverso attività di help-desk, formazione e aggiornamento;
- fornisce ai potenziali Partner la documentazione e il supporto necessario all'interoperabilità delle Risorse;
- rende disponibile il Discovery service (WAYF) [10];
- gestisce e mantiene il sito web ufficiale della Federazione;
- gestisce e mantiene il registro delle entità;
- effettua attività di monitoraggio e auditing.

2.4 Certificati digitali

Il certificato digitale è un documento elettronico emesso da un'Autorità di Certificazione (Certification Authority) che, nel gergo, è conosciuta come CA [11]. L'Autorità Certificativa è un ente fidato che si interpone tra le parti, ovvero tra chi richiede il certificato e chi lo verifica.
Il certificato vale per una durata limitata, trascorsa la quale, diventa invalido. Il certificato può essere anche revocato o sospeso in caso di compromissioni delle chiavi private o di cambiamenti avvenuti in capo al soggetto che identifica. Chiunque può verificare un certificato digitale perché quelli emessi sono archiviati in registri pubblici dove si trovano anche le revoche e le sospensioni.

2.4.1 A cosa servono i certificati digitali

Molto semplicemente i certificati digitali servono ad attestare l'identità di un sito web e verificare chi c'è dietro lo schermo.
L'uso più diffuso dei certificati digitali per i siti web è quello del protocollo HTTPS, grazie al quale si proteggono tutte le informazioni che circolano sul server quando le persone si collegano.
In pratica quando il certificato è stato rilasciato da un'autorità riconosciuta il browser prende la chiave pubblica che è indicata nel certificato e la utilizza per fornire una navigazione sicura, al riparo dai malintenzionati.

2.4.2 Crittografia a chiave asimmetrica

In crittografia asimmetrica il certificato digitale è definito come un documento elettronico che associa una chiave pubblica ed un soggetto privato o pubblico.
Le chiavi asimmetriche funzionano attraverso stringhe di caratteri di varia lunghezza che vengono generate da un complesso algoritmo matematico. Per le chiavi asimmetriche accade che una è resa pubblica e, quindi, è leggibile da chiunque.
L'altra viene tenuta segreta e deve essere protetta perché è quella che decodifica il certificato. Quindi per decifrare un messaggio con una chiave pubblica ed una privata occorreranno sempre entrambe le chiavi e, quindi, un passaggio doppio.

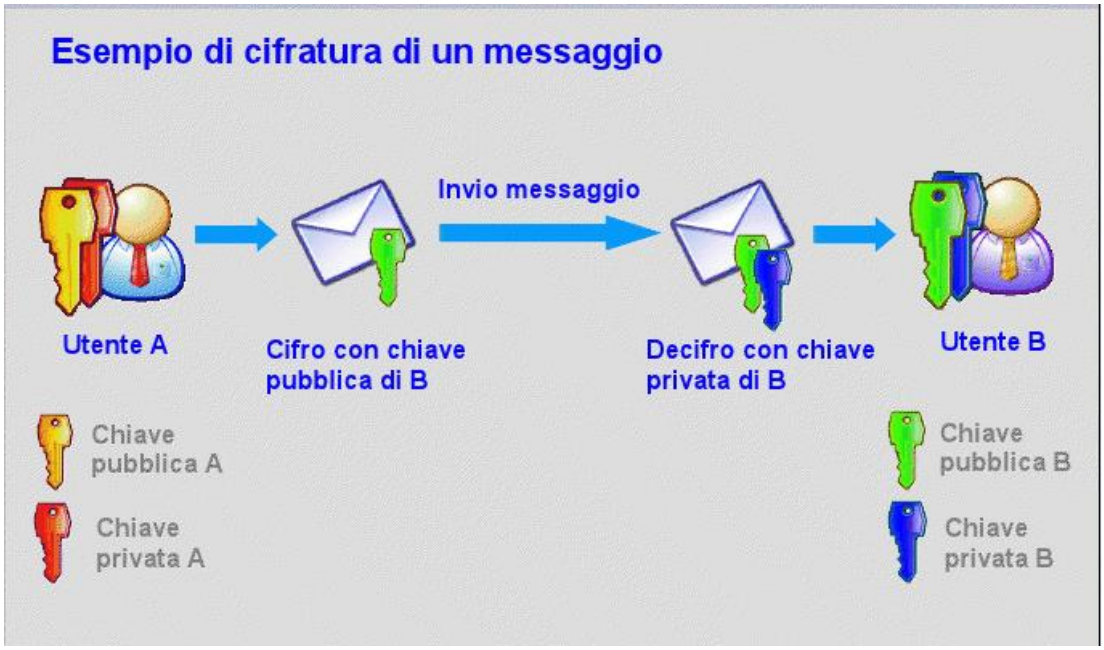


Figura 2.2 [12]

Tutto il sistema si fonda sull'affidabilità della Certification Authority.
È a questa che ci si rivolge per acquisire un certificato digitale ed anch'essa ha una propria coppia di chiavi.
Quando la Certification Authority fornisce i dati del certificato ne cifra le chiavi con la propria chiave privata.
Quindi sarà possibile decifrarle con la corrispondente chiave pubblica della Certification Authority.

Questo garantisce che, una volta consegnate al legittimo proprietario, non sarà possibile alterare le chiavi.

Le Autorità di Certificazione emettono un certificato a seguito di una richiesta solo dopo aver attestato l'identità del richiedente. L'operazione di verifica telematica dei certificati può essere effettuata da chiunque in quanto le CA mantengono un registro pubblico dei certificati digitali emessi e una dei certificati digitali revocati (Certification Revocation List o CRL).

Figura 2.3 [13]

Il formato più ricorrente nel panorama dei certificati digitali è basato sullo Standard X.509. Si tratta di un certificato a chiave pubblica e a firma digitale che contiene anche altre informazioni come l'identità di chi è associato al certificato e le informazioni relative alla CA.

Tra le varie tipologie di certificato digitale Standard X.509 c'è l'SSL/TLS che serve a proteggere il sito web attraverso il sopra citato protocollo HTTPS. Questo è un certificato provvisto di chiave pubblica, nome del dominio da proteggere e livello di convalida.

Lo stesso vale per il certificato TLS che è la versione più attuale del precedente protocollo SSL, ormai in disuso. Quindi per i siti web l'unica tipologia di certificato a cui fare riferimento è il TLS che, talvolta, viene ancora chiamato SSL/TLS.

2.4.3 Come è composto un certificato X.509

Un certificato emesso da una CA, successivamente ad una richiesta di un utente, generalmente contiene:

• la chiave pubblica del client;

• il nome reale del client, dove si differenziano due casi:

- se il client è una persona fisica si avrà nome e cognome, data di nascita, ecc...
- se invece il client è rappresentato da un server web sarà presente l'indirizzo web e il nome della compagnia titolare del dominio;

• la data di scadenza della chiave pubblica;

• il nome della CA che ha emesso il certificato;

• la firma digitale della CA che ha emesso il certificato.

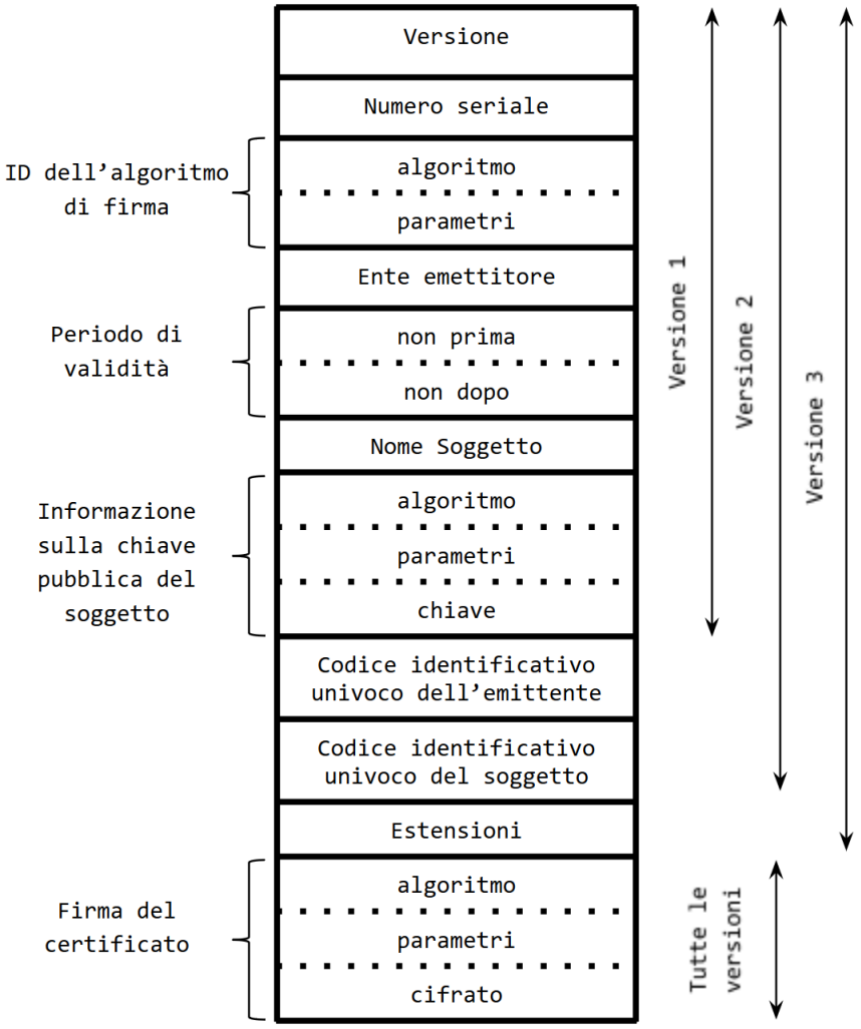


Figura 2.4 [14]

2.4.4 Estensioni tipiche dei file con certificati X.509

Estensioni comuni per i file contenenti i certificati X.509 sono:

- .pem - Privacy-Enhanced Mail, è un certificato codificato con Base64, racchiuso tra "-----BEGIN CERTIFICATE-----" e "-----END CERTIFICATE-----";
- .cer, .crt, .der - certificato codificato con DER, a volte sequenze di certificati;
- .p7b, .p7c - struttura SignedData PKCS#7 senza dati, solo il/i certificato/i o la/le CRL (Certificate revocation list);
- .pfx, .P12 - PKCS#12, può contenere certificati e chiavi pubbliche e private (protette da password);

3 Il modello federato Shibboleth

3.1 Shibboleth

Shibbboleth è un pacchetto software open source e standardizzato che ha per obbiettivo il web Single Sign-On, molto ricco per quello che riguarda lo scambio degli attributi, basato su standards aperti tra cui, prevalentemente, SAML2.
È un sistema federato che supporta l'accesso sicuro a risorse attraverso il web: le informazioni relative all'utente vengono trasmesse dall'Identity Provider (IdP) aziendale al Service Provider (SP) esterno che le prepara per la protezione dei dati sensibili e per l'utilizzo da parte delle applicazioni.
Il processo di autenticazione avviene, in buona sostanza, nei seguenti termini:
a) l'utente richiede la connessione ad una risorsa protetta facendo sì che il SP intercetti la richiesta (la risorsa da proteggere è definita nei files di configurazione del web server che la ospita);
b) il SP, basandosi sulla configurazione di cui sopra, determina a quale IdP far riferimento e quale protocollo utilizzare attraverso un meccanismo di "scoperta" noto come servizio WAYF (acronimo di Where Are You From): la richiesta di autenticazione è così delegata al WAYF che la passa all'IdP selezionato dall'utente;
c) come risultato delle azioni precedenti, una richiesta di autenticazione via browser è inviata dal SP all'IdP selezionato dall'utente: l'IdP decide se l'utente può autenticarsi e quali attributi inviare al SP, scelta questa basata prevalentemente sulle caratteristiche del SP che fornisce il servizio e su quelle dell'attributo principale dell'utente;
d) l'IdP impacchetta e firma i dati che trasmette sotto forma di asserzione SAML al SP che la spacchetta e la decodifica eseguendo poi una serie di controlli di sicurezza per decidere infine se il richiedente abbia o meno diritto di accesso alla risorsa desiderata;
e) infine, se il processo di verifica del punto precedente ha esito positivo, l'utente viene finalmente rediretto alla risorsa richiesta.

La figura 3.1 illustra il processo di autenticazione.

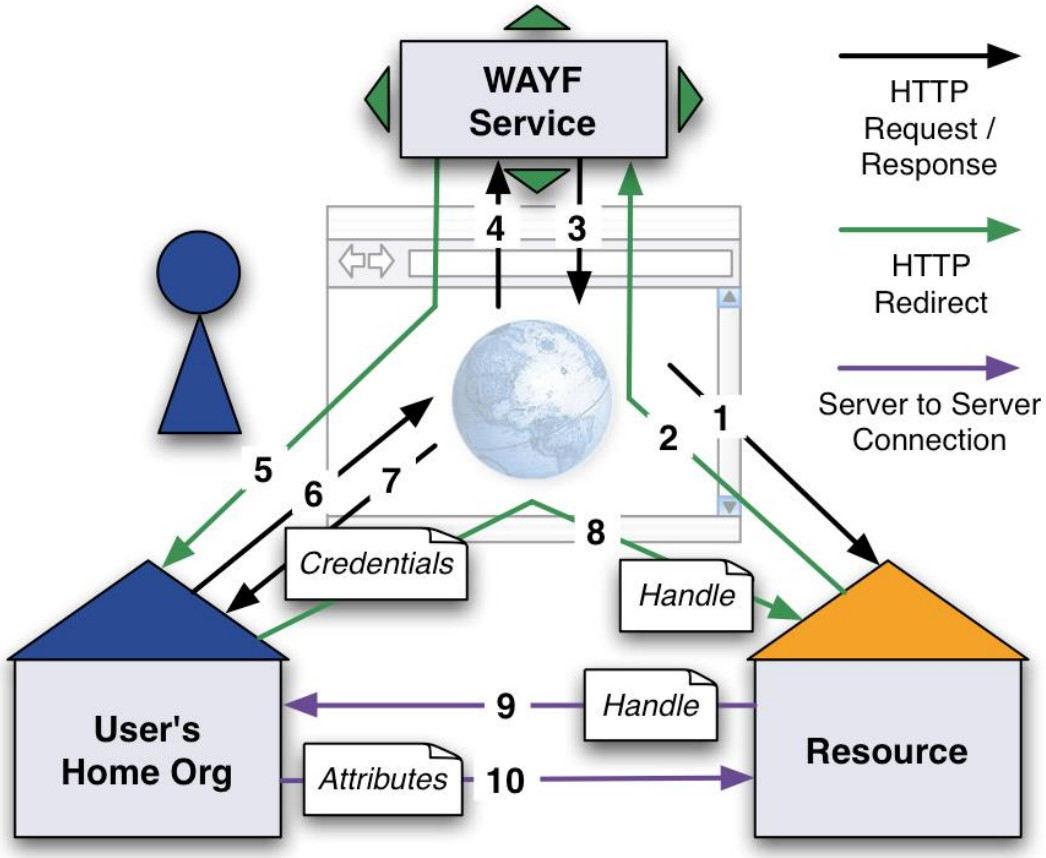


Figura 3.1 [15]

Come si può vedere da quanto sopra esposto, il processo di autenticazione avviene sull'IdP del richiedente e non sul SP che tale risorsa distribuisce; in parole semplici, l'utente si autentica presso la propria organizzazione, utilizzando una sola coppia di credenziali per più servizi ed evitando di dover allocare una coppia di credenziali per ogni fornitore di servizi.

Affinché ciò avvenga, occorre che gli attori del processo siano consorziati in quelle che vengono dette Federazioni, istituzioni collaborative di fornitori ed utilizzatori di servizi.

In Italia tale obbiettivo è raggiunto dalla Federazione IDEM-GARR-AAI (IDEM = IDEntity Management).

L'Università di Perugia ha aderito alla fase pilota del progetto sin dalla sua nascita avvenuta nel 2008 ed ora è a pieno titolo membro della Federazione IDEM-GARR-AAI, mettendo a disposizione un IdP per l'accesso ai servizi offerti dalla Federazione

ed ha realizzato SP in maniera da diventare anche fornitore di servizi e non soltanto fruitore.

Come precedentemente detto, il progetto IDEM si serve della tecnologia Shibboleth per realizzare i suoi obiettivi.

Shibboleth rappresenta un software open source per l'accesso a risorse e servizi web condivisi tramite credenziali di autorizzazione.

Il sistema Shibboleth è composto da diversi elementi che separano la gestione delle identità degli utenti dalla gestione delle risorse autenticate; è un sistema basato su standard affidabili e collaudati e offre adeguate garanzie di funzionamento e di aderenza agli standard.

Permette al client di accedere ai servizi protetti che si trovano all'interno della propria organizzazione attraverso una singola autenticazione (web Single Sign-On).

Tali servizi possono trovarsi anche in altre organizzazioni purché appartenenti ad una determinata Federazione in cui vigono regole condivise per l'identificazione degli utenti e l'autorizzazione per l'accesso a risorse e servizi.

Shibboleth in sostanza modifica il modo in cui vengono controllati gli accessi e sposta verso le strutture di appartenenza degli utenti il compito di dare garanzie sulla loro identità (autenticazione) e sui loro diritti (autorizzazione) attraverso la realizzazione di una Infrastruttura di Autenticazione ed Autorizzazione (AAI).

Il ruolo di Shibboleth all'interno della federazione IDEM è quello di un framework per creare relazioni di fiducia tra le comunità dei partecipanti.

Shoftim - Libro dei Giudici Cap 12, 5-6

וַיִּלְכֹּד גִּלְעָד אֶת־מַעְבְּרוֹת הַיַּרְדֵּן לְאֶפְרָיִם וְהָיָה כִּי יֹאמְרוּ פְלִיטֵי אֶפְרַיִם אֶעְבֳּרָה וַיֹּאמְרוּ לוֹ אַנְשֵׁי־גִלְעָד הַאֶפְרָתִי אָתָּה וַיֹּאמֶר לֹא: 5

וַיֹּאמְרוּ לוֹ אֱמָר־נָא שִׁבֹּלֶת וַיֹּאמֶר סִבֹּ֫לֶת וְלֹא יָכִין לְדַבֵּר כֵּן וַיֹּאחֲזוּ אוֹתוֹ וַיִּשְׁחָטוּהוּ אֶל־מַעְבְּרוֹת הַיַּרְדֵּן וַיִּפֹּל בָּעֵת הַהִיא מֵאֶפְרַיִם אַרְבָּעִים וּשְׁנָיִם אָלֶף: 6

5 Gli uomini di Galaad si impadronirono dei guadi del Giordano prima che quei di Efraim arrivassero; così, quando uno dei fuggiaschi di Efraim diceva: «Lasciatemi passare», gli uomini di Galaad gli chiedevano: «Sei tu un Efraimita?». Se quegli rispondeva: «No», i Galaaditi gli dicevano

5 «Allora di' Scibboleth»; se quegli diceva «Sibboleth», perché non poteva pronunciare correttamente, essi lo afferravano e lo uccidevano presso i guadi del Giordano. In quel tempo perirono quarantaduemila uomini di Efraim.

Figura 3.2 [16]

3.2 Componenti di Shibboleth: IdP, SP, WAYF

I componenti fondamentali del sistema Shibboleth sono i seguenti:
Identity Provider (IdP) e Service Provider (SP).

Identity Provider (IdP):
è un servizio creato tramite un componente software che si interfaccia con il registro delle identità dell'Organizzazione (LDAP, database relazionale o altro), quindi generalmente uno per ogni struttura che aderisce alla federazione.
Si occupa della registrazione degli utenti e di mantenere le loro informazioni, di gestire le sessioni di autenticazione (inserimento delle credenziali oppure verifica di una sessione già attiva per l'utente - Single Sign-On), del rilascio degli attributi degli utenti autenticati. Tali informazioni sono infatti richieste dai Service Provider (SP) per consentire all'utente di accedere al servizio. L'IdP invia effettivamente al SP solo i dati necessari, proteggendo i dati personali che non dovrebbero mai essere inviati.

Service Provider (SP):
è un servizio che si occupa di proteggere e condividere una risorsa o un servizio web da mettere in comune tra i vari utenti della federazione; inoltre provvede ad indirizzare l'utente al servizio WAYF, e successivamente al relativo IdP, raccoglie le informazioni inviategli dall'IdP, le utilizza per proteggere il servizio e permette l'autorizzazione all'utente che ha effettuato una richiesta.
Queste due entità agiscono sostanzialmente in questo modo: le informazioni relative all'utente vengono trasmesse dall'Identity Provider (IdP) al Service Provider (SP) il quale a sua volta le usa per proteggere il servizio e per concedere l'autorizzazione all'utente che ne ha fatto richiesta.

Esiste inoltre un terzo componente Where Are You From (WAYF):

WAYF:
è un servizio che, interpellato dal Service Provider, permette all'utente di selezionare la propria istituzione di appartenenza scelta tra un elenco di istituzioni possibili. Esso,

infatti, contiene l'elenco completo di tutti gli IdP e le coordinate dei siti di autenticazione presso le corrispondenti organizzazioni di appartenenza. Una volta che l'utente ha selezionato la propria organizzazione, lo redirige sulla propria "home organization".

Il servizio WAYF è unico per tutta la federazione ed è anche chiamato Discovery Service (DS).

Sostanzialmente, i Service Provider (risorsa accessibile in rete) sono coloro che mettono a disposizione i servizi internet; con questa tecnica non avranno più bisogno di gestire difficoltose prassi di amministrazione degli utenti.

Mentre gli Identity provider (servizio di gestione e verifica delle identità) da organizzazioni di appartenenza diventano veri e propri gestori delle identità; tali identità possono essere scambiate, fornendo sempre le adeguate garanzie e rispettando la privacy degli utenti.

Il servizio centralizzato WAYF è gestito e mantenuto dalla Federazione.

Esso contiene l'elenco completo di tutti gli IdP e le coordinate dei relativi siti di autenticazione presso le corrispondenti Home Organization.

La comunicazione col WAYF server avviene in modo protetto tramite https.

Il servizio può memorizzare permanentemente la scelta dell'organizzazione dell'utente.

La Federazione garantisce l'uniformità della nomenclatura delle istituzioni appartenenti alla Federazione e di come esse compaiono nella lista del WAYF o nei metadati, eventualmente modificando le descrizioni proposte per uniformarle con gli altri partecipanti.

Se i fornitori di servizi partecipano a più federazioni è necessario gestire un proprio servizio WAYF, cosa di cui se ne occupa la Federazione. Essa, infatti, comunicherà ai suddetti fornitori i riferimenti da inserire e le relative parti descrittive in modo che l'utente possa scegliere in maniera uniforme la propria struttura di appartenenza quando si autenticherà presso il fornitore.

Le informazioni all'interno del WAYF saranno inserite dalla Federazione a seguito della procedura di adesione dell'organizzazione.

In altre parole, la federazione si occupa di:

- concedere l'inserimento di nuovi utenti che vogliono aderire;
- gestire l'elenco di tutti i partecipanti;

- aderire agli standard tecnici tradizionali;
- assicurare una politica di controllo;
- fornire consigli e supporto tecnico.

3.2.1 Shibboleth Identity Provider

L'Identity Provider Shibboleth è un'applicazione web java, che comprende i seguenti elementi legati tra loro:

- Handler Manager: è un servizio che amministra i vari endpoint dai quali l'IdP può ricevere messaggi;
- Attribute Resolver: si occupa di recuperare gli attributi da un database e provvede alla loro combinazione e trasformazione in un insieme di dati relativi ad uno specifico utente; successivamente li invia, tutti o in parte, al client dell'IdP;
- Attribute Filter: è utilizzato per creare una collezione filtrata di attributi, sulla base di un insieme di regole. Queste regole rappresentano quali attributi e valori un client può ricevere;
- Attribute Authority (AA): questo servizio, che dipende dall'Attribute Resolver, riceve un insieme di attributi e li codifica in un'asserzione di attributi SAML.

Inoltre, se i metadati SAML del richiedente contengono informazioni sul tipo di attributi che egli richiede, il servizio sceglierà e rilascerà solo gli attributi richiesti.

3.2.2 Shibboleth Service Provider

Il Service Provider Shibboleth è un demone, chiamato *shibd*, con cui il server web dialoga. Come detto precedentemente, il SP Shibboleth riceva la richiesta per l'accesso ad una risorsa protetta e redirige l'utente al WAYF o all'IdP. Dopo aver ricevuto le informazioni di autenticazione, inizia una comunicazione con l'Attribute Authority dell'IdP al fine di prelevare gli attributi.

Il SP Shibboleth è composto da tre elementi:

- Resource Manager (RM): si occupa della gestione delle richieste di accesso alle risorse protette del servizio, che vengono compiute dall'utente mediante un browser;

- Assertion Consumer Service (ACS): ha il compito di comunicare con l'handler dell'IdP, di elaborare asserzioni SAML e di estrarre da esse i contenuti;
- Attribute Requester (AR): ottiene attributi aggiuntivi sull'utente autenticato e delinea politiche di accettazione degli attributi (Attribute Acceptance Policy o AAP).

Nello specifico, l'utente, mediante il browser, genera al RM una richiesta per avere accesso ad una risorsa. L'RM coinvolge l'ACS che otterrà l'identità di un Handle Service (HS) da contattare per ogni richiesta successiva dell'utente; questo processo mediante il servizio WAYF. L'HS risponde attraverso una asserzione SAML, contenente un ID unico, che viene passato dall'ACS all'AR del SP. L'AR sfrutta sia questo ID che l'indirizzo dell'Attribute Authority associato per chiedere tutti gli attributi che può conoscere. Questi dati sono analizzati e verificati dall'AR secondo opportune policy di ammissibilità degli attributi (AAP).
I contenuti degli attributi risultanti saranno forniti all'RM, che si occupa di utilizzarlo per garantire l'accesso alla risorsa.
In sintesi, quando un utente vuole accedere a servizi protetti, il SP lo redirige all'IdP di appartenenza, che mostra all'utente una pagina di login per autenticarsi, oppure, in caso di sessione già attiva, ritrasmette all'SP le informazioni di autenticazione già effettuata.

3.2.3 Where Are You From

Il servizio Where Are You From (WAYF) o Discovery Service (DS) consente di scegliere la propria organizzazione di appartenenza tra le tante afferenti alla Federazione ed è gestito e mantenuto proprio dalla Federazione.
Il servizio si può trovare all'indirizzo https://wayf.idem.garr.it e contiene la lista di tutti gli IdP e le coordinate dei relativi siti di autenticazione delle proprie organizzazioni di appartenenza. Attraverso il protocollo https si garantisce una comunicazione sicura con il server WAYF. La scelta della home organization può essere memorizzata in modo permanente. Se si sceglie di impostare una Home Organization predefinita, la scelta verrà ricordata e non bisognerà più reinserirla quando si accederà le volte successive a risorse AAI con un determinato web browser.

3.3 Comunicazione tra IdP, SP e WAYF. Fasi del processo

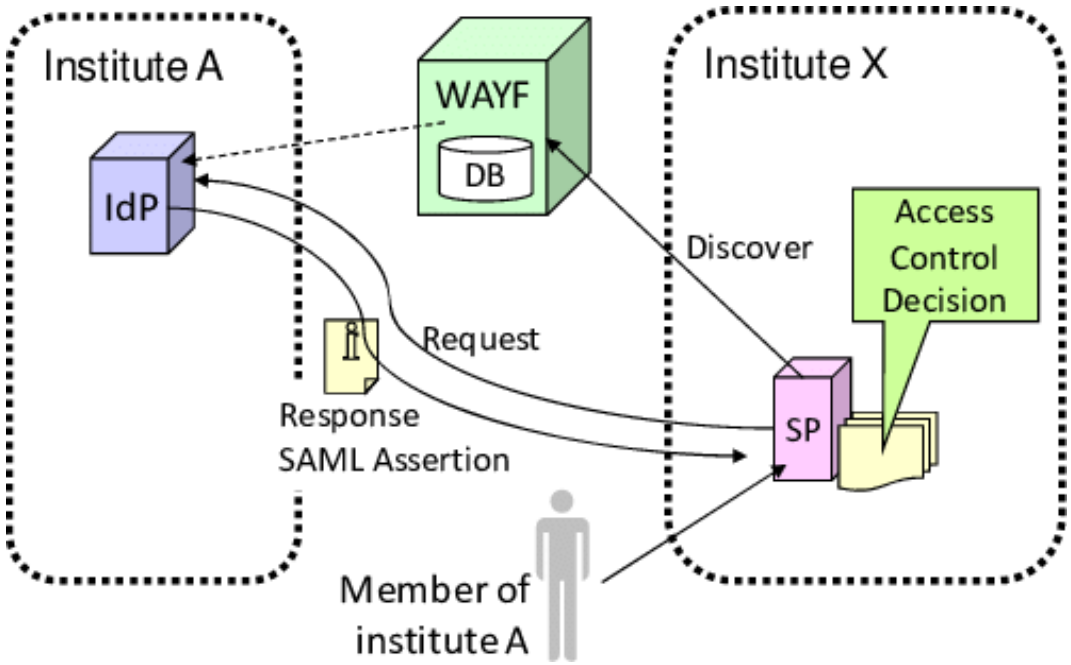


Figura 3.3 [17]

Il processo di autenticazione avviene in questo modo:

- il client chiede la connessione ad una risorsa protetta, in modo che il SP intercetti la richiesta (la risorsa da proteggere è definita nei files di configurazione del web server che la ospita).
  Per compiere tale richiesta occorre che l'utente acceda alla pagina iniziale, inserendo l'indirizzo della risorsa;

- il SP determina a quale IdP far riferimento e quale protocollo utilizzare mediante il servizio WAYF. La richiesta di autenticazione passa così al WAYF che a sua volta la reindirizza all'IdP selezionato dall'utente;

- a questo punto l'IdP decide se l'utente può o meno autenticarsi e quali attributi inviare al SP, una scelta fatta in base alle caratteristiche del SP stesso;

- l'utente visualizza un form dove poter inserire le sue credenziali di accesso, da notare l'avvenuta redirezione all'indirizzo della pagina di login propria dell'organizzazione.

- l'IdP invia i dati come asserzione SAML al SP che li interpreta e li decodifica eseguendo una serie di controlli di sicurezza per decidere se colui che sta effettuando l'operazione di autenticazione abbia o meno diritto di accesso alla risorsa desiderata;

- se l'esito del risultato è negativo, ovvero se le credenziali inserite non sono corrette, l'utente non avrà accesso alle risorse;

- l'utente visualizzerà un messaggio di errore.

- infine, se il processo di verifica è andato a buon fine, l'utente viene rediretto alla risorsa desiderata.

Come si può notare, l'utente si autentica presso la propria organizzazione, utilizzando un solo username ed una sola password per più servizi evitando di dover reinserire nuovamente le credenziali per tutti gli altri gestori di servizi.
Tutto ciò può avvenire solo se i personaggi coinvolti nelle operazioni di autenticazione appartengono alle Federazioni, istituzioni collaborative di fornitori ed utilizzatori di servizi.
Un fornitore può allo stesso tempo essere anche un utilizzatore del servizio: un'università, per esempio, potrebbe avere utenti che vogliono accedere a risorse bibliografiche esterne, e contemporaneamente potrebbe consentire l'accesso al suo WiFi a utenti di altri enti, purché federati.

3.4 Un esempio di funzionamento concreto di SHIBBOLETH

Supponiamo che un client voglia autenticarsi ad un determinato servizio per cui possiede i diritti di accesso, ad esempio supponiamo che cerchi di accedere alle riviste pubblicate da ACS Publications.

Il server ACS, che rappresenta il Service Provider (SP), non accetta la richiesta e la inoltra al Where Are You From (WAYF), che ha il compito di decifrare chi è l'utente in questione. A questo punto, dietro richiesta da parte del WAYF, l'utente fornisce allo stesso WAYF le informazioni che lo identificano e questo ultimo chiede all'Handle Service del Identity Provider (IdP), ossia l'organizzazione a cui l'utente ha dichiarato di appartenere, una conferma.

L'Handle Service è uno dei componenti dell'Identity Provider, che rappresenta appunto l'istituzione.

Questo stesso richiede all'utente di non accedere direttamente sul sito remoto dell'editore ACS, ma di utilizzare il web login, ossia di accedere tramite Shibboleth, al fine di essere riconosciuto e conseguentemente di accedere in maniera automatica a qualsiasi risorsa a cui ha diritto.

L'utente viene riconosciuto grazie al confronto dei dati personali contenuti nel database degli utenti (User DB).

Tramite l'Handle di Shibboleth, le credenziali dell'utente vengono passate al Service Provider, ossia ad ACS, che valida l'utente e l'asserzione.

Ma al Service Provider mancano ancora gli attributi dell'utente, ossia essi non sono stati ancora registrati nell'Attribute Resource (AR).

Quindi si rende necessaria una nuova richiesta verso l'IdP, al fine di recuperare i dati relativi agli attributi dell'utente attingendo all'Attribute Authority (AA). L'IdP riconosce il Service Provider che ha inoltrato la richiesta, lo valida e stabilisce quali attributi sia necessario trasmettergli.

Questi vengono inviati al fine di ultimare la fase di autorizzazione e permettere così all'utente di accedere alla risorsa da lui richiesta.

Inoltre, in questo modo l'utente ora è stato riconosciuto, i suoi dati memorizzati e, quindi, può accedere a qualsiasi altra risorsa o servizio di cui possiede i diritti di accesso.

Il fatto innovativo è che non ci sono nuove username o password da ricordare o distribuire con il timore di perderle.
Per poter accedere a ciò a cui si ha diritto è sufficiente autenticarsi tramite il web login, che permette all'utente di essere riconosciuto da qualsiasi posto cerchi di connettersi, superando in questo modo i limiti legati al riconoscimento degli IP, che spesso inibisce gli utilizzatori che in quel particolare istante non sono presenti all'interno della rete dell'ente di appartenenza.
È a disposizione degli utilizzatori un help online, che facilita l'uso dello strumento in questione, di cui non è necessario assolutamente conoscere i particolari dell'architettura per poterlo correttamente utilizzare.
Affinché tutto questo sia veramente applicabile e dia i risultati voluti, è però necessario che le organizzazioni stesse creino delle superstrutture di condivisione dei dati di autenticazione dei loro utenti, le cosiddette Federazioni.

3.4.1 I metadati della federazione

I metadati sono delle informazioni che, associate ad una pagina web o ad una porzione di essa, ne descrivono il contenuto specificandone il contesto di riferimento.
La loro caratteristica consiste nella possibilità di classificare i dati pubblicati sul web in maniera strutturata, in modo tale che la ricerca delle informazioni da parte degli utenti sia più efficace.
I metadati della Federazione contengono, all'interno di un file basato su SAML 2.0, le informazioni relative a tutti i Service Provider ed agli Identity Provider partecipanti e rappresentano lo strumento con il quale si condivide la fiducia all'interno della Federazione; vengono inoltre utilizzati per distribuire informazioni relative alle CA.
Tramite questo file la Federazione pubblica i dati descrittivi dei partecipanti e gli stessi partecipanti utilizzano proprio i metadati per verificare l'identità del partner durante le comunicazioni, costruendo delle relazioni di fiducia; per verificare l’identità della controparte e comunicare, infatti, si utilizza il relativo certificato contenuto nei metadati.
È necessario quindi prestare la massima attenzione a questo file perché include tutte le informazioni necessarie per il riconoscimento reciproco dei partecipanti.

3.5 Modifiche tra i partecipanti alla Federazione

Quando un nuovo IdP o un SP modifica la propria configurazione già presente oppure entra a far parte della Federazione IDEM, deve comunicare tempestivamente questa variazione a tutti i partecipanti della Federazione.
In particolare, colui che partecipa alla modifica invia al servizio IDEM la nuova configurazione (frammento file Metadata); il servizio IDEM integra la nuova configurazione del partecipante nella configurazione complessiva della Federazione; la nuova configurazione sarà recapitata in maniera automatica agli altri partecipanti della Federazione sul proprio IdP o SP, in modo tale da non costringere tutti i membri a mettersi in contatto tra di loro affinché la modifica venga recapitata.
In casi particolari in cui alcuni SP non hanno procedure automatiche per ricevere gli aggiornamenti sulle nuove configurazioni, il servizio IDEM si metterà in contatto con ciascun SP per comunicare le modifiche alla configurazione dell'IdP cambiato. Il servizio IDEM effettua specifici test per accertarsi che la variazione sia stata recepita e si pone come intermediario tra l'IdP modificato e i SP che devono ricevere le notifiche di cambiamento.

3.6 Modalità di gestione dei metadati

Tutto ciò che è stato detto porta una notevole cura da parte dei partecipanti nel trattare i metadati, in particolare:

- nell'inserimento di un IdP/SP nei metadati, perché il frammento relativo al nuovo servizio dovrà contenere esplicitamente il certificato e dovrà essere trasmesso alla Federazione con modalità sicure;
- nella variazione dei metadati, perché i partecipanti dovranno comunicare tempestivamente la variazione dei dati nel caso in cui vengano revocati o variati i certificati;
- nello scarico dei metadati aggiornati, perché i partecipanti dovranno prelevare ogni giorno i metadati dalla Federazione; tali metadati andranno ricavati tramite il protocollo HTTPS ponendo attenzione alla verifica della firma;

- nella memorizzazione dei file dei metadati, in quanto il file scaricato deve restare sul server e non deve essere in alcun modo modificato.

3.7 Lo standard SAML

L'architettura Shibboleth usa il protocollo SAML (Security Assertion Markup Language), un framework basato su XML (Extensible Markup Language) per lo scambio di informazioni di autenticazione e di autorizzazione tra domini differenti, in particolare tra identity provider e service provider, quindi lavora su utenti, dispositivi o qualsiasi entità identificabile.
Come suggerisce il nome, SAML permette ad entità aziendali di fare asserzioni riguardanti l'identità, gli attributi e i diritti di un soggetto (un ente che è spesso un utente umano) verso altre entità, come ad esempio un'azienda partner o un'altra applicazione d'impresa. Tale soggetto è un'entità (una persona o un computer) che ha un'identità in un dominio di sicurezza.
SAML inoltre prevede opportuni meccanismi di estendibilità e definisce il formato dei metadati, utilizzati da Shibboleth per descrivere informazioni di vario tipo che caratterizzano entità SAML, come ruoli o certificati dei membri di una federazione.
Fornisce funzionalità di Single Sing-On federato e un framework per lo scambio di attributi; fornisce funzionalità estese relative alla privacy e riesce a comunicare informazioni di autenticazione e autorizzazione tra domini federati attraverso determinati messaggi che vengono chiamati “assertion” (affermazioni).

3.7.1 Assertion e Statement SAML

Le asserzioni e gli statement costituiscono la base dello standard SAML.
SAML definisce tre tipi diversi di statement che possono essere contenuti in un'assertion:

- Authentication Statement (statement di autenticazione), specifica che un client è stato autenticato precedentemente attraverso uno degli svariati metodi (come password, chiave pubblica X.509);

- Authorization Statement (statement di autorizzazione), specifica se un soggetto può avere o meno accesso a determinate risorse;
- Attribution Statement (statement di attributo), specifica che quell'utente è associato a determinate caratteristiche individuali (gli attributi) espresse generalmente da una coppia nome-valore.

3.7.2 La specifica SAML

La specifica SAML si basa su alcuni componenti fondamentali:

- asserzioni: sono dichiarazioni relative all'autenticazione e all'autorizzazione di un utente, sia esso una persona o un sistema hardware/software.
  Le asserzioni sono di tre tipi diversi.
  Le prime, quelle di autenticazione, stabiliscono che un client ha verificato la propria identità ad un determinato asserting party (emesso da una SAML authority).
  Le seconde, quelle di attributo, indicano alcuni dati di un utente come, ad esempio, il ruolo che quest'ultimo ha all'interno di un'organizzazione.
  Le ultime asserzioni, i permessi (AuthorizationDecision), stabiliscono le operazioni precise che un utente può effettuare;

- protocolli: le asserzioni devono avere la possibilità di scambiarsi opportunamente tra le entità che interagiscono contattando l'asserting party. Per questo motivo sono stati definiti opportuni protocolli che consentono lo scambio di asserzioni attraverso un meccanismo propriamente detto di “domanda e risposta”: nello specifico sono messaggi “SAML request” e “SAML response”, codificati sempre in XML;

- binding: sono utilizzati per indicare come avviene lo scambio di informazioni di sicurezza in SAML attraverso appropriati protocolli di trasporto (HTTP o SOAP). Questo perché i protocolli non stabiliscono le modalità di trasporto ma solo la struttura delle informazioni che possono essere scambiate;

- profili: rappresentano un insieme di asserzioni, protocolli e binding SAML, organizzati in diversi casi d'uso, che specificano come questi elementi vengono combinati per raggiungere lo scopo del caso d'uso in questione.

Un esempio può essere la realizzazione del Single Sign-On tra svariati servizi.
Il livello di fiducia che si trova all'interno di un'assertion non è specificato da SAML; questo compito è affidato ai sistemi locali i quali decidono se le politiche di sicurezza di una determinata applicazione siano sufficienti a proteggere un'azienda nel caso in cui sorgano dei problemi circa una decisione di autorizzazione basata su un'assertion errata.
Questa caratteristica di SAML fa si che le attività basate sul web, prima di accettare un'asserzione, debbano aderire ad un livello base di verifica.
SAML può fondersi con diversi protocolli di comunicazione e trasporto. Ad esempio, può essere legato a SOAP (Simple Object Access Protocol) su HTTP (HyperText Transfer Protocol).

3.7.3 Funzionamento SAML

Il funzionamento di SAML è il seguente:
l'utente viene registrato presso un IdP che provvede ad autenticarlo; il SP deve ovviamente identificare l'utente che chiede l'autenticazione, quindi, riceve dall'IdP un'asserzione SAML sulla base della quale il SP decide se concedere o vietare l'accesso dell'utente ai propri servizi.
Ad esempio, supponiamo che un utente di un'organizzazione X viene autenticato dal sistema di identificazione di X e può accedere ai servizi di Y, questo perché l'organizzazione di Y verifica che sia valido il token di autenticazione rilasciato da X

e non chiede un ulteriore processo di verifica da parte del token rilasciato da Y. I token del mittente e del ricevente sono infatti equivalenti.
Affinché il token SAML sia valido bisogna redirigere la richiesta del client al server di autenticazione, questo nel caso in cui venisse meno il token relativo all'identità dell'utente e al ruolo che gli è stato associato. In questo caso, l'applicazione dovrà contattare il server di autenticazione dove ci saranno le credenziali dell'utente ed interrogare il servizio di autenticazione del dominio in cui l'utente è registrato. Se l'esito sarà positivo, sarà restituita un’assertion con i dati dell'utente.

4 Accesso Wi-Fi con Autenticazione Federata.

In questa tesi viene descritta l'attività di realizzazione di un sistema Captive Portal WiFi per l'accesso a internet con Autenticazione Federata. Il progetto ha per obiettivo quello di consentire agli ospiti del Dipartimento di Economia dell'Università degli Studi di Perugia, 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. [18]

4.1 Introduzione

Presso il Dipartimento di Economia è presente una infrastruttura Wireless a 2.4Ghz/5Ghz composta attualmente da sei Access Points distribuiti presso i tre piani del Dipartimento, due ogni piano, uno al lato est ed uno al lato ovest.
La configurazione dei singoli Access Point è gestita in maniera centralizzata da una piattaforma Captive Portal per l'autenticazione e registrazione di utenti per il libero accesso alla navigazione Internet.
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.
In questa tesi, oltre alle ormai 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. [19]
Per ottenere questo scopo è stato necessario istituire un Service Provider e registrarlo presso la Federazione IDEM del GARR. [20]
È stato deciso di utilizzare la distribuzione Linux Open Source "Zeroshell" per la flessibilità e robustezza delle sue funzionalità di Access Control. Grazie al supporto di SAML (Security Assertion Markup Language) è stato possibile modificare le

dinamiche di autenticazione per demandarle all'IdP di appartenenza dell'utente anziché al RADIUS [21] di Zeroshell.

4.2 Definizione di Captive Portal

- E' un gateway di livello 2 o 3 che unisce due segmenti di rete
    - I client che si associano al primo segmento ottengono subito connettività IP, ma non possono comunicare con il secondo segmento se non si autenticano
    - Le richieste http/https dei client non autenticati vengono redirette verso un portale di autenticazione in cui l'utente deve dimostrare la propria identità

4.3 Cosa è Zeroshell

- E' una distribuzione Linux che fornisce i principali servizi di rete
- Configurabile via web
    - Il nome Zero-Shell (Senza-Shell) significa che la configurazione dovrebbe avvenire esclusivamente via Web. L'accesso alla shell è comunque possibile

4.3.1 I principali servizi offerti da Zeroshell

- Routing e Bridging con supporto delle VLAN 802.1q
- Firewall con supporto per i filtri Layer 7
- Traffic Shaping e QoS assegnando banda massima, banda garantita e priorità in base alla tipologia di traffico
- Load Balancing e Failover dei collegamenti WAN
- VPN site-to-site con OpenVPN (TAP)
- VPN gateway per accessi Host-to-LAN (OpenVPN e IPSec/L2TP)
- Captive Portal con backend di autenticazione Kerberos 5, RADIUS, certificati X.509 e SAML v2 mediante Shibboleth
- Proxy HTTP trasparente con scansione antivirus delle pagine web

- Server LDAP, Kerberos 5, RADIUS con accounting, DNS e DHCP
- Access Point Wi-Fi con supporto per Multiple SSID [22]

4.4 Sviluppo del progetto

Le diversi fasi sviluppate, che verranno poi descritte nel dettaglio, per la configurazione dell'accesso alla Wi-Fi dipartimentale con autenticazione Federata sono:

- Scelta della distribuzione Linux Open Source "Zeroshell" per la realizzazione del Captive Portal;
- Installazione;
- Configurazione Network;
- Registrazione del Service Provider presso la Federazione IDEM.

4.4.1 Download

Come detto, è stato scelto di utilizzare la distribuzione "Zeroshell" che è uno dei pochi Captive Portal (opensource) che supporta l'integrazione nativa con SAML. Il captive portal può così diventare un SP che può interagire con gli altri sistemi della federazione.

Il download della distribuzione può essere effettuato al link:

- https://www.zeroshell.org/download/

L'immagine generica da installare su HD o Flash USB è:

- ZeroShell-3.9.5-X86.iso

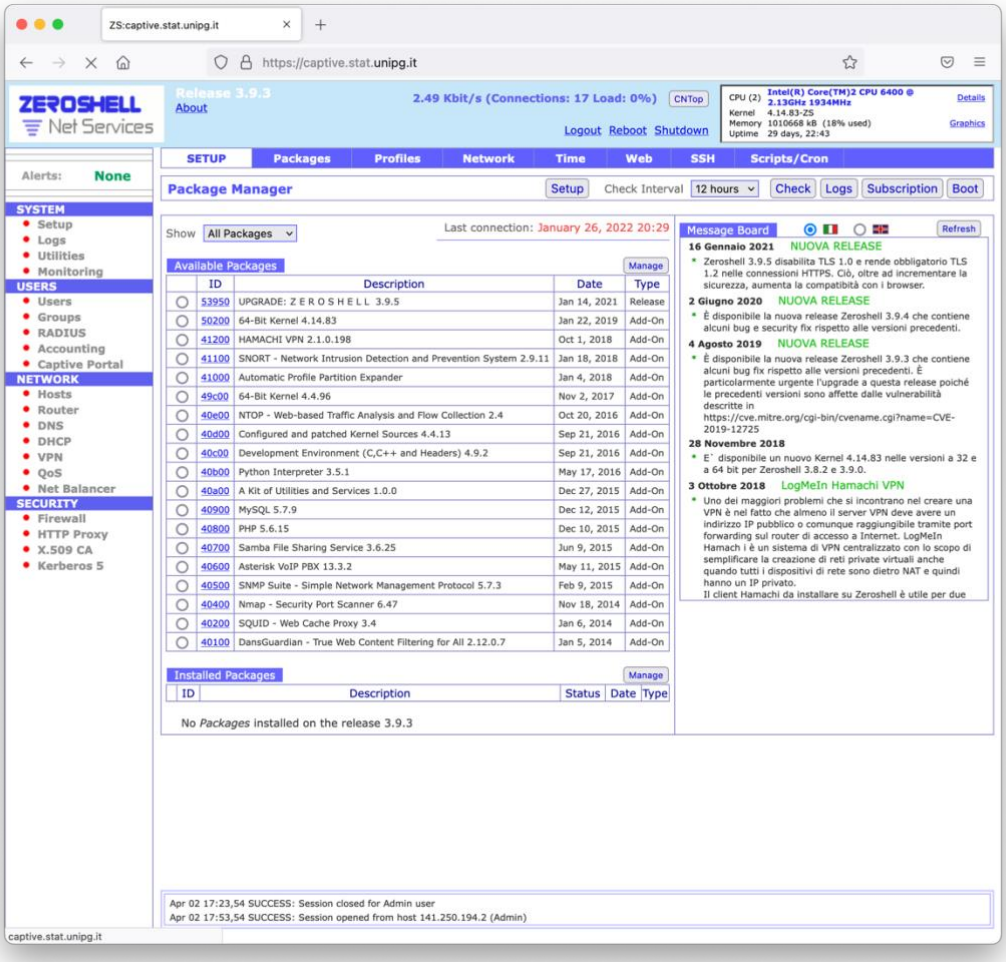


Figura 4.1: Interfaccia web Zeroshell

4.4.2 Installazione

L'installazione della distribuzione "Zeroshell" è stata effettuata su un PC con limitate risorse hardware:

CPU (2):	Intel™ Core™2 CPU 6400 @ 2.13GHz
Ram:	1 GB DDR2
Hard disk:	250GB SATA
Network Card (3):	Gigabit Ethernet, 10/100/1000Mbps

Installazione su Hard Disk

La partizione contenente Zeroshell è Read-Only per una maggiore sicurezza.

/boot (Kernel + initrd)	Partizione 1
Zeroshell Live CD	Partizione 2
Profili di Configurazione	Partizione 3

Accesso all'interfaccia web

Una volta installata la distribuzione, la prima configurazione, in particolare l'IP per l'interfaccia web ed altri parametri di base, può essere eseguita usando l'interfaccia a carattere disponibile localmente all'avvio di Zeroshell:

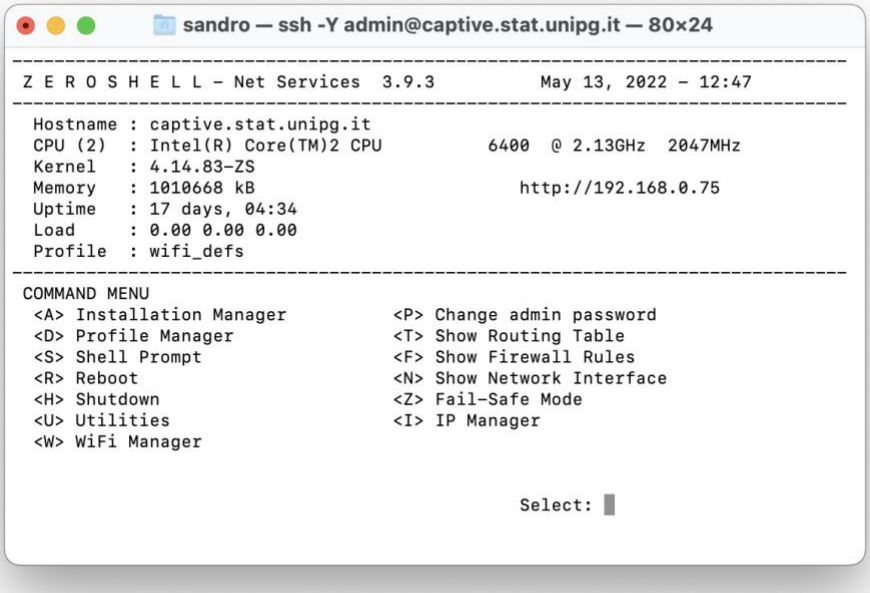


Figura 4.2: Interfaccia a carattere Zeroshell

L’interfaccia a carattere, in seguito, può essere raggiunta anche in SSH, dopo averla abilitata, a seconda delle proprie necessità per un unico IP address, per una subnet o per una specifica interfaccia di rete.
L’interfaccia di Zeroshell è settata di default con IP 192.168.0.75, che è stato cambiato in 141.250.6.25, IP della rete del Dipartimento di Economia.

Creazione della profile

Una volta in condizione di accedere all’interfaccia web la prima cosa fatta è stata la creazione della profile, che consente il salvataggio della configurazione. Nella scheda Profiles abbiamo la possibilità di gestirne più di una, ed in particolare per ogni profile: backup, creazione, cancellazione, attivazione, disattivazione e ripristino

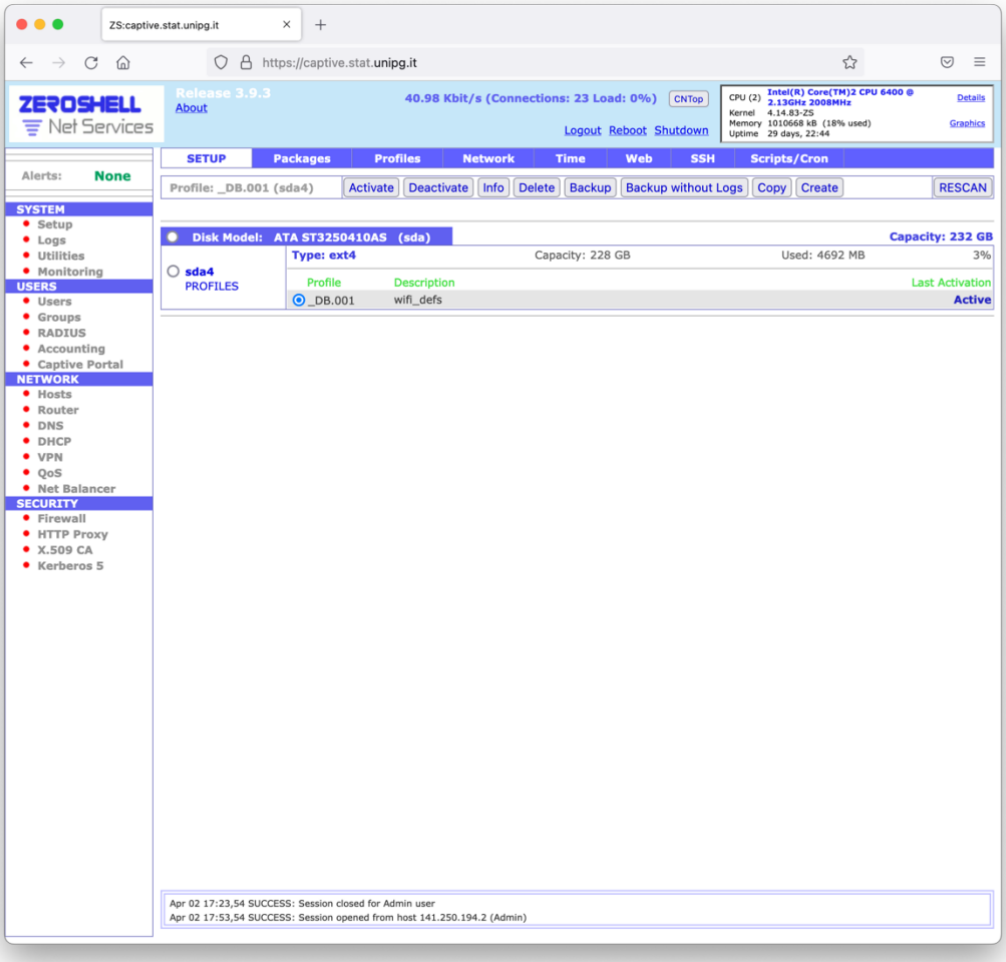


Figura 4.3: Profile Zeroshell

4.4.3 Configurazione della rete

La configurazione della rete è possibile dalla scheda Setup>Network
Le interfacce di rete disponibili sono tre, due per la rete interna (ETH00 ed ETH01) ed un'altra per Internet (ETH02). Sulle due interfacce ETH00 ed ETH01 è stato creato un BRIDGE (BRIDGE00). Su BRIDGE00, è stato impostato il nostro IP, 192.168.0.75 e su ETH02 è stato usato 141.250.6.15 per accedere ad internet. È stato anche abilitato un DHCP sull'interfaccia BRIDGE00 per fornire un indirizzo IP dinamico agli utenti ospiti.

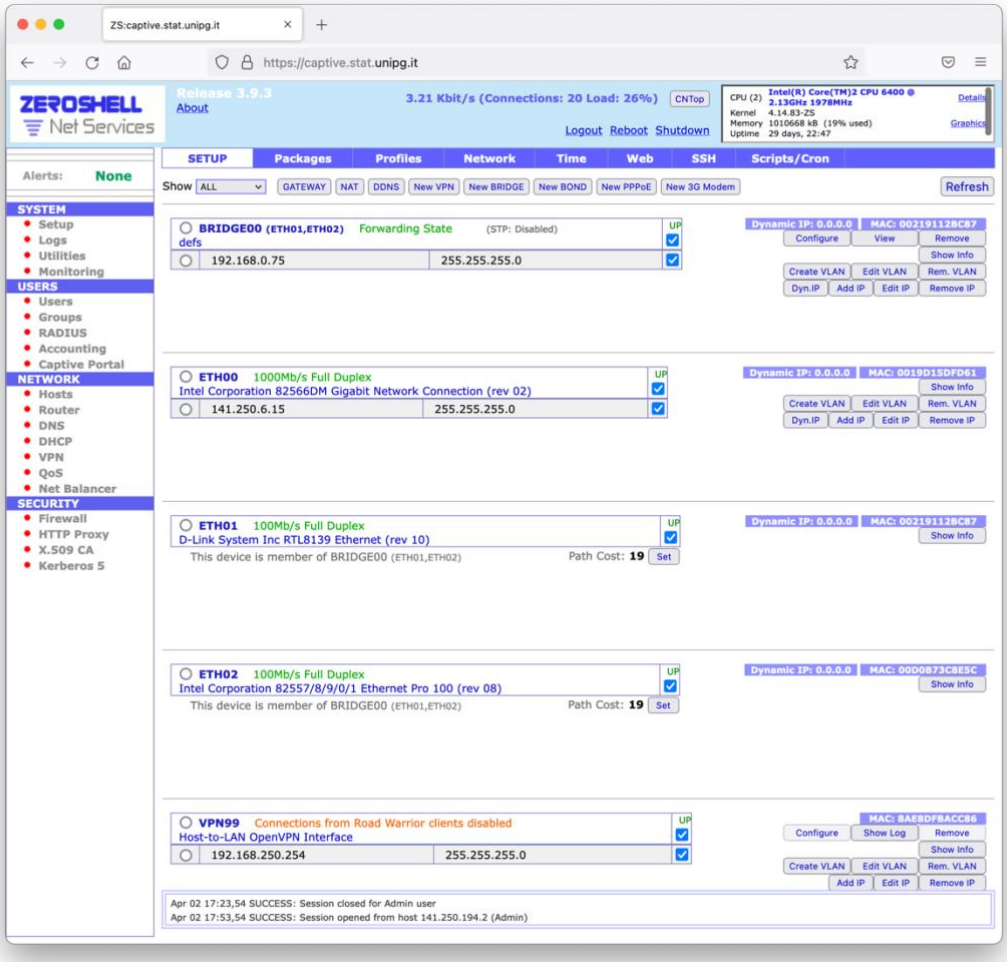


Figura 4.4: Configurazione rete Zeroshell

4.4.4 Captive Portal

Zeroshell permette di creare un Captive Portal tramite l'utilizzo del gateway predefinito che cattura la richiesta dagli utenti ospiti. Come detto è stata configurata un'interfaccia (BRIDGE00) sulla rete interna su cui si voleva abilitare il Captive Portal. Quindi dalla scheda Captive Portal è stata selezionata l'interfaccia BRIDGE00 dal menu a discesa e quindi selezionata la casella di controllo “GW" per abilitare il Captive Portal. In questo modo il Captive Portal funziona su BRIDGE00 e permette di autenticarsi usando username/password.

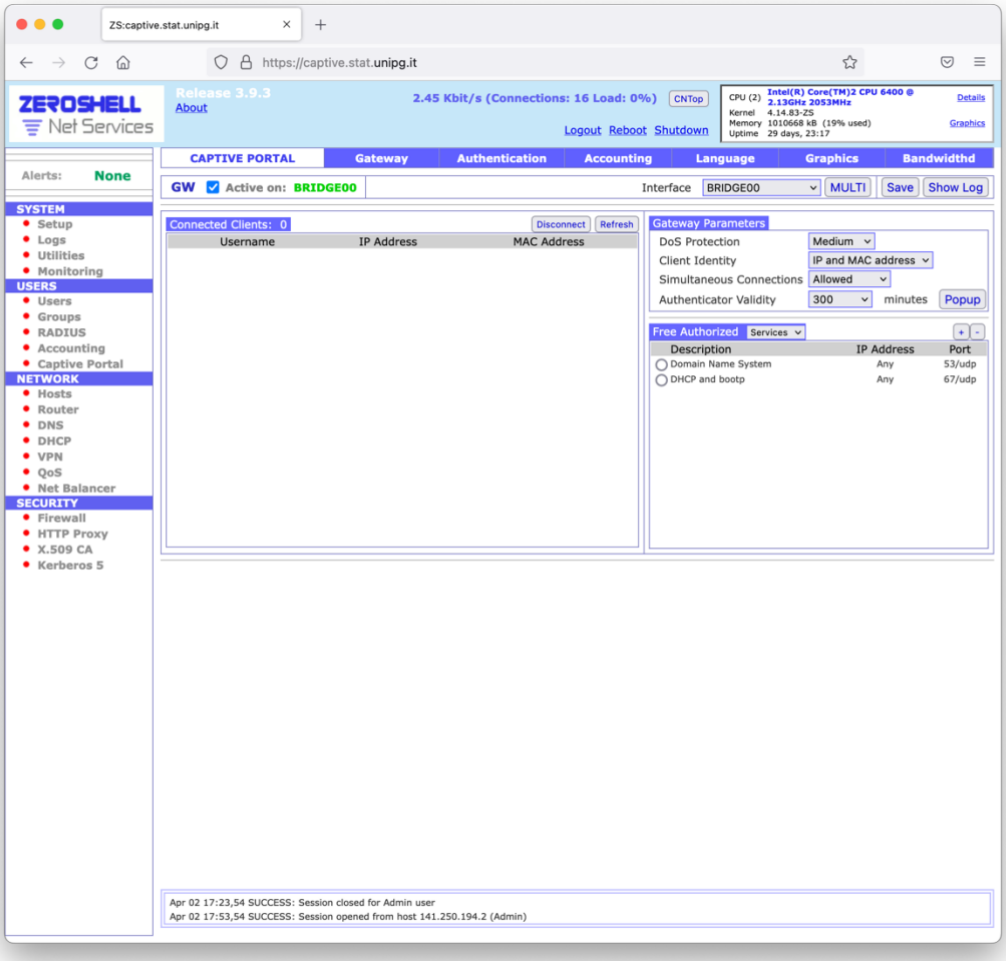


Figura 4.5: Abilitazione Captive Portal Zeroshell

4.4.5 Configurazione Access Point

Nel caso di accesso mediante Captive Portal, gli Access Point vengono programmati in modalità aperta, cioè senza alcuna autenticazione e cifratura. Il client si può associare liberamente e riceve immediatamente un indirizzo IP dal server DHCP. Tuttavia, il Gateway di accesso a internet blocca la comunicazione con l'esterno e redirige qualsiasi richiesta web (http e https) verso un portale di autenticazione.
Gli Access Point devono essere autorizzati dal server Radius interno a Zeroshell condividendo lo *Shared Secret*, questa operazione è possibile da:

Users > Authorized Clients
specificando nome dell'Access Point (Client Name), IP e Shared Secret.

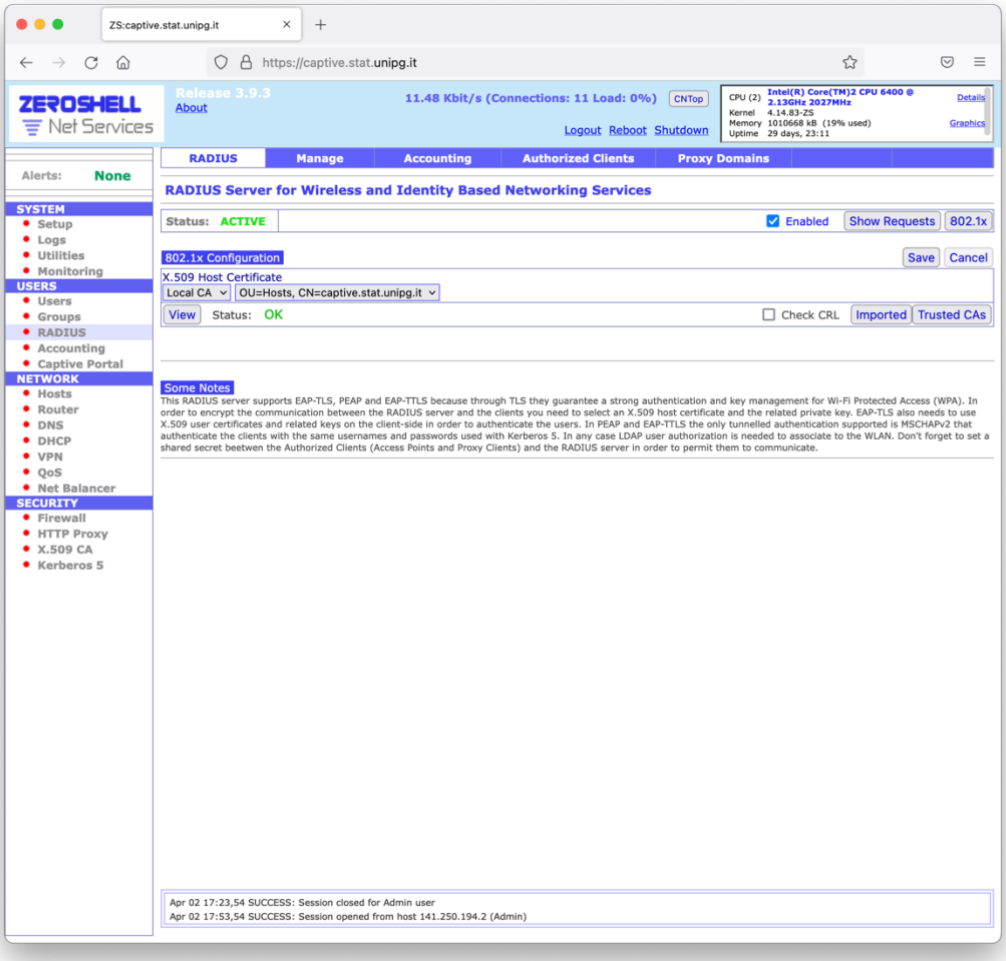


Figura 4.6: Abilitazione server Radius Zeroshell

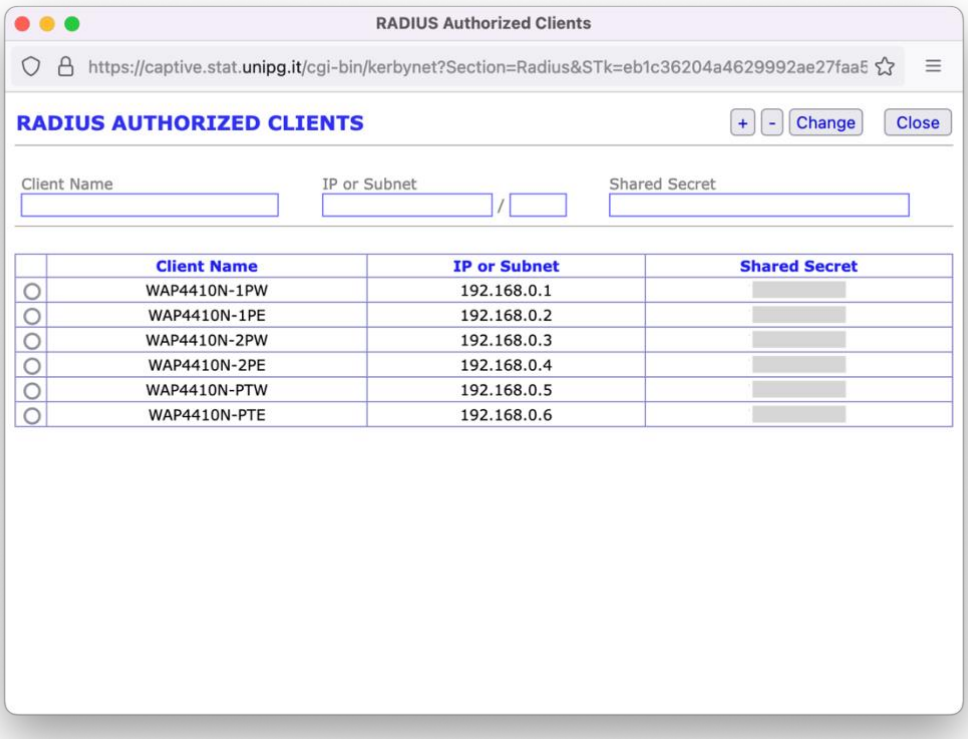


Figura 4.7: Autorizzazione Access Point Zeroshell

Gli Access Point installati nel Dipartimento di Economia sono sei:

WAP4410N-1PW	192.168.0.1	Primo Piano Lato Ovest
WAP4410N-1PE	192.168.0.2	Primo Piano Lato Est
WAP4410N-2PW	192.168.0.3	Secondo Piano Lato Ovest
WAP4410N-2PE	192.168.0.4	Secondo Piano Lato Est
WAP4410N-TPW	192.168.0.5	Piano Terra Lato Ovest
WAP4410N-TPE	192.168.0.6	Piano Terra Lato Est

Gli Access Point del lato Est sono collegati fisicamente tramite l'infrastruttura di rete esistente all'interfaccia ETH01, gli altri del lato Ovest all'interfaccia ETH02.
Gli Access Point installati sono CISCO WAP4410N, per ognuno oltre all'IP, è stato impostato il SSID (service set identifier) e le informazioni di sicurezza per essere autorizzati dal server Radius di Zeroshell.

Come SSID è stato scelto *defs* acronimo di Dipartimento di Economia, Finanza e Statistica, tre delle aree del Dipartimento di Economia.
L'indirizzo del server Radius di Zeroshell è 192.168.0.75, la porta è la 1812, il metodo di protezione è WPA2 Enterprise e naturalmente lo Shared Secret deve essere lo stesso condiviso dal server Radius Zeroshell.

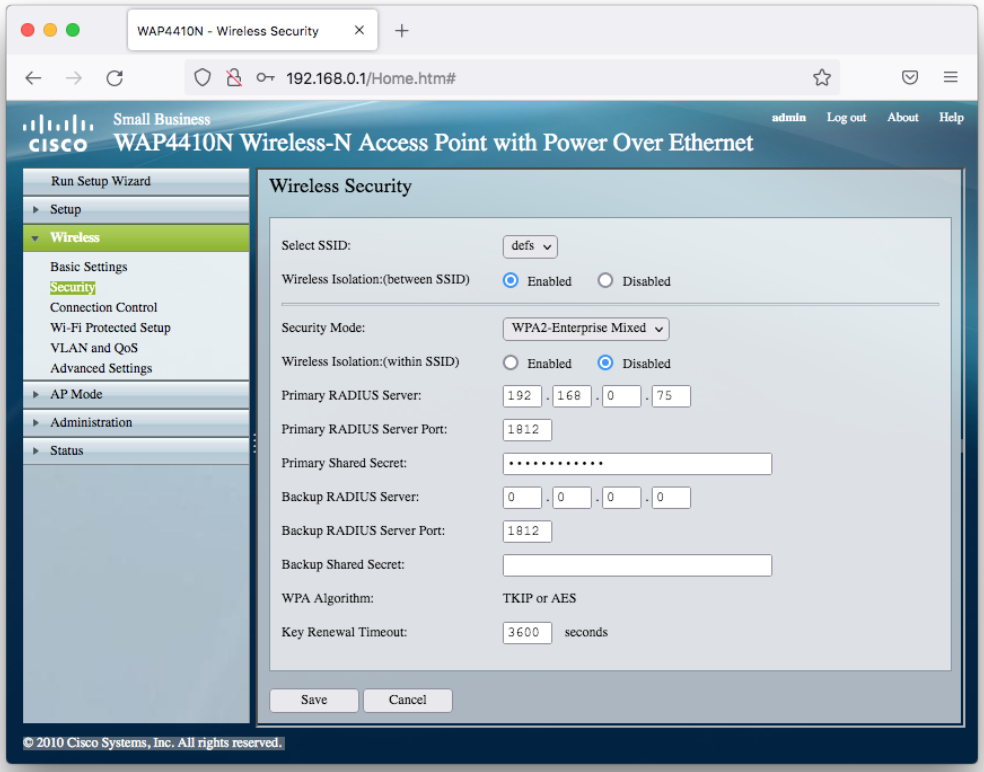


Figura 4.8: Configurazione Access Point CISCO WAP4410N

4.5 Autenticazione Shibboleth

Zeroshell integra la possibilità di utilizzare l'autenticazione shibboleth per Captive Portal.
L'abilitazione dell'autenticazione shibboleth può essere eseguita da:

Captive Portal > Autentication > Shibboleth Autentication

Abilitata consente di autenticarsi utilizzando sia nome utente/password che Shibboleth SAML 2.0.

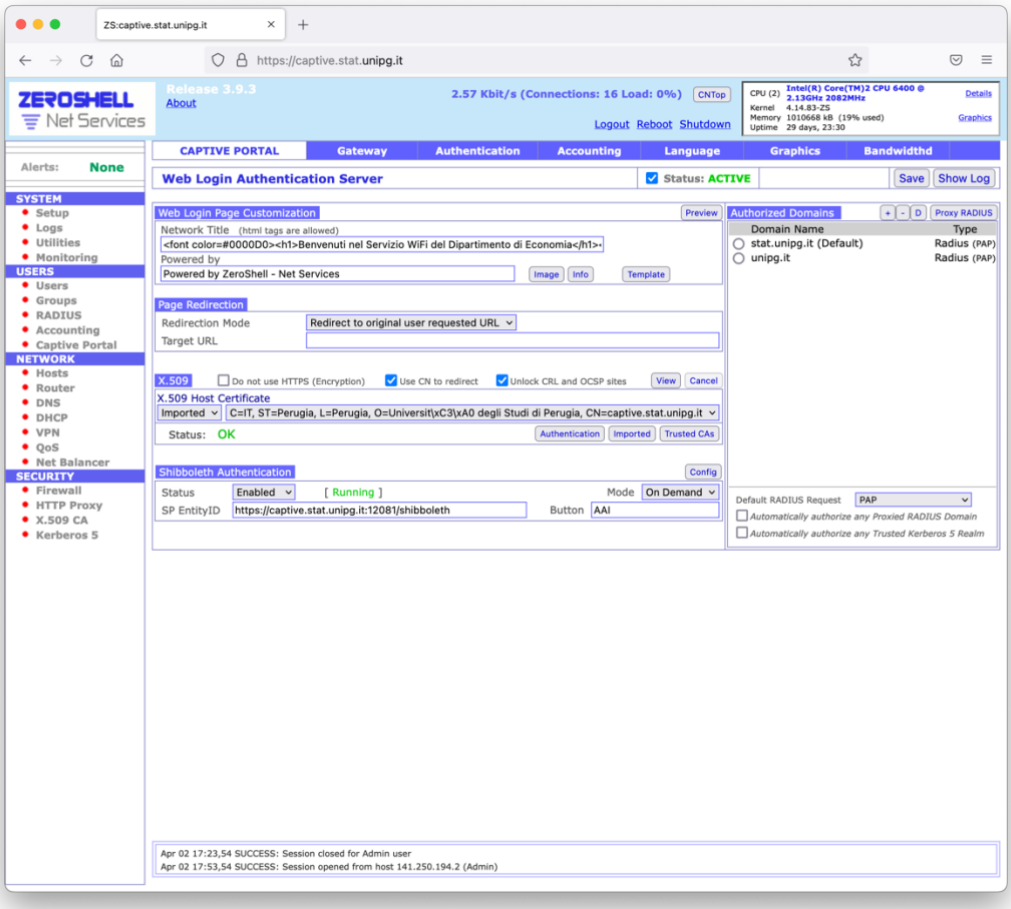


Figura 4.9: Abilitazione Captive Portal Shibboleth Zeroshell

4.5.1 Files di configurazione Shibboleth

Zeroshell fornisce un'elementare file editor per la configurazione di Shibboleth e per la relativa verifica di correttezza. È accessibile dalla scheda:

Captive Portal > Authentication > Shibboleth Authentication > Config

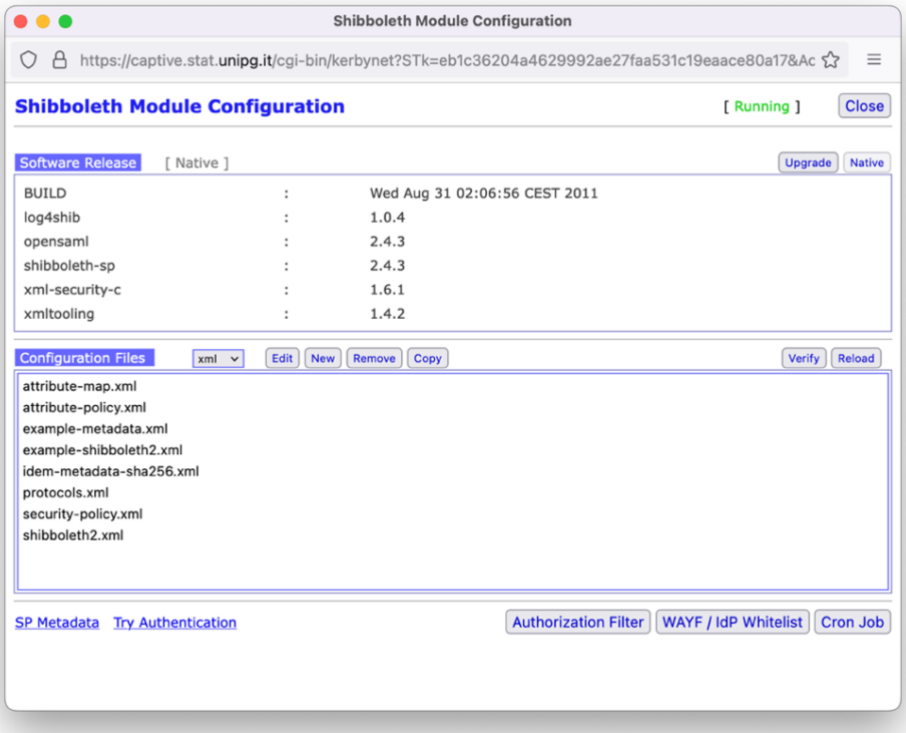


Figura 4.10: Configurazione files Shibboleth Zeroshell

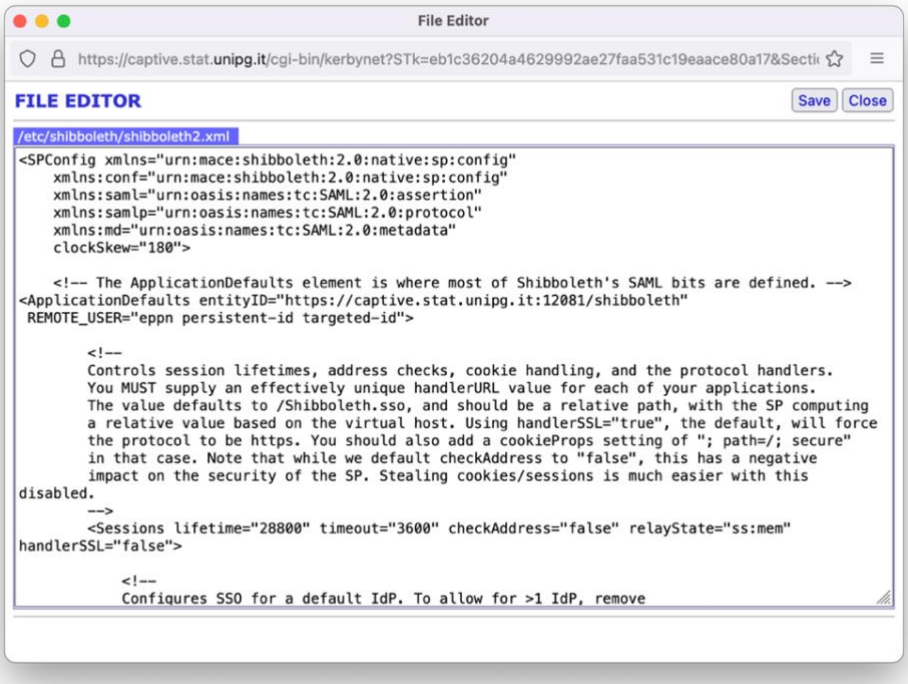


Figura 4.11: Configurazione file shibboleth2.xml Zeroshell

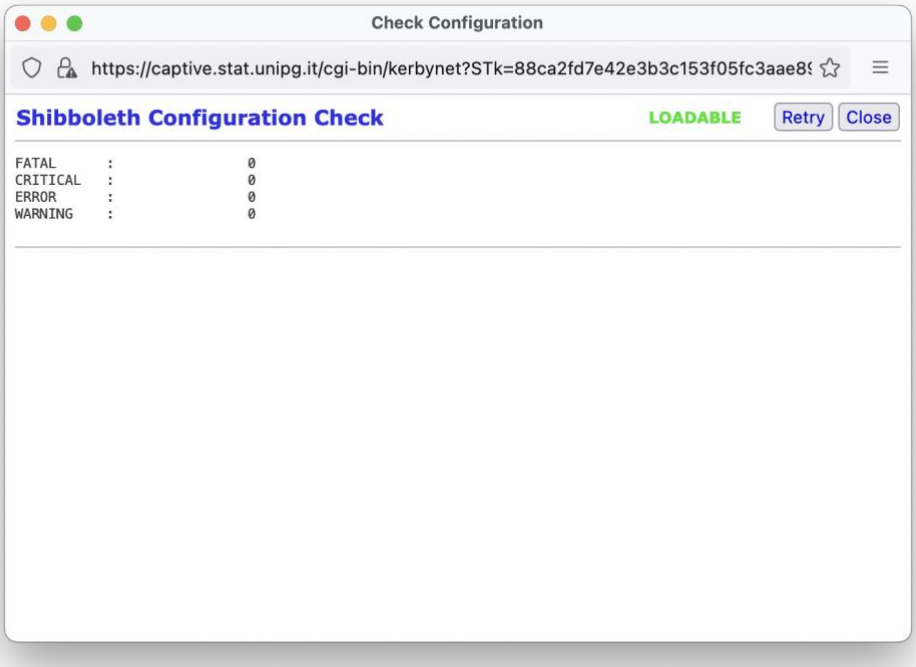


Figura 4.12: Verifica correttezza configurazione Shibboleth Zeroshell

4.5.2 Configurazione del Service Provider Shibboleth

La configurazione del Service Provider si è sviluppata nelle fasi seguenti.

Richiesta ed installazione del certificato per il SP

In linea con le specifiche tecniche della Federazione IDEM è stato necessario richiedere ed installare sulla porta 443 un certificato rilasciato da una CA riconosciuta.

Impostazione nome host

È stato aggiunto il nome host captive.stat.unipg.it della macchina scelta per ospitare il Service Provider di Shibboleth.

da: Network > Hosts

oppure dalla shell modificando il file */etc/hosts*

Shibboleth Service Provider

- È stato scaricato l'*idem-signer-20241118.pem* per la verifica del file metadati da:

  https://md.idem.garr.it/certs/idem-signer-20241118.pem

  e copiato in */etc/shibboleth*, (una delle poche operazioni come altre che seguono, fatte con l'utilizzo della shell e non dall'interfaccia web).

- Sono stati installati i certificati per la firma e la cifratura delle asserzioni:
  /etc/shibboleth/captive_stat_unipg_it.crt
  /etc/shibboleth/captive.stat.unipg.it.key

- E' stato editato il file *shibboleth2.xml* per apportare le seguenti modifiche:

  entityID

  <ApplicationDefaults
  entityID="https://captive.stat.unipg.it:12081/shibboleth"
  REMOTE_USER="eppn persistent-id targeted-id">

  SSO

  <SSO discoveryProtocol="SAMLDS"
  discoveryURL="https://wayf.idem.garr.it/WAYF">
  SAML2 SAML1
  </SSO>

  MetadataProvider

  <MetadataProvider type="XML"
  uri="http://md.idem.garr.it/metadata/idem-metadata-sha256.xml"
  backingFilePath="idem-metadata-sha256.xml">

<MetadataFilter type="Signature" certificate="/etc/shibboleth/idem-signer-20241118.pem"/>
</MetadataProvider>

- Sono stati registrati i Metadati del SP, ottenibili all'URL:

  http://captive.stat.unipg.it/Shibboleth.sso/Metadata

  o dall'interfaccia Zeroshell su:

  Captive Portal > Authentication > Shibboleth Authentication > Config > SP Metadata

  sull'IDEM Entity Registry: https://registry.idem.garr.it

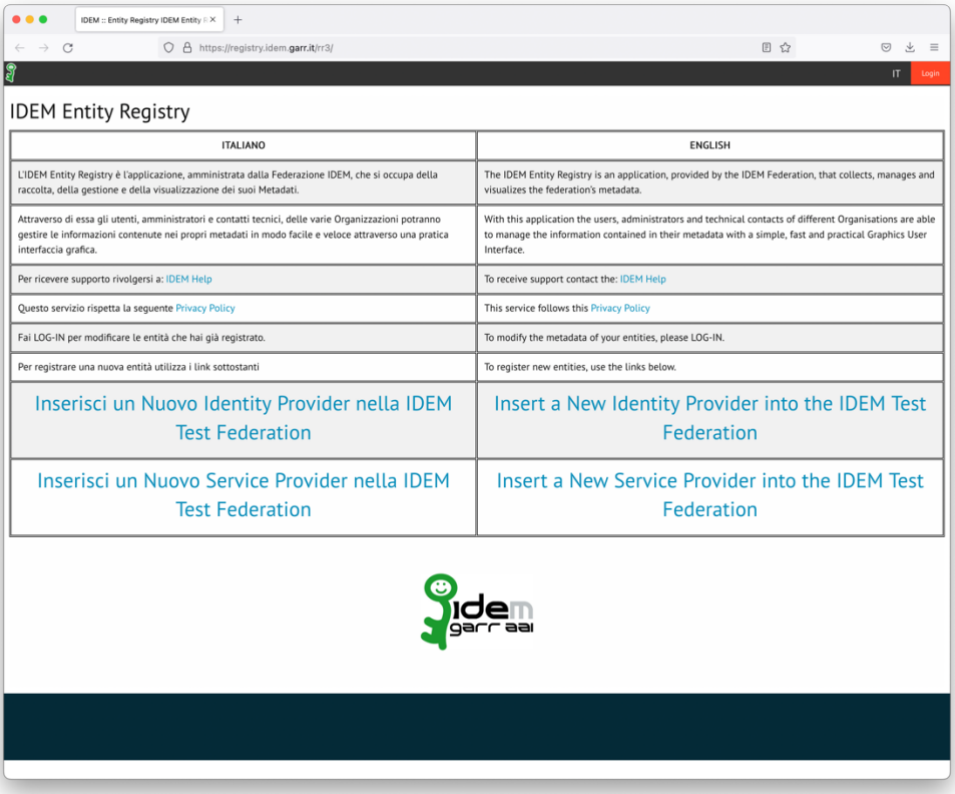


Figura 4.13: https://registry.idem.garr.it

4.5.3 Registrazione del Service Provider presso la Federazione 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 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.
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. In particolare, nella tesi:

Nome del servizio:
WiFi Dipartimento di Economia - Università degli Studi di Perugia

Attributi:
Attributo: *mail*

- Indirizzo email
- Requisito IDEM: Raccomandato
- Es.: MARIO.ROSSI@unipg.it

Attributo: *eduPersonScopedAffiliation (ePSA)*

- Indica l'affiliazione dell'utente presso l'organizzazione di appartenenza
- Requisito IDEM: Obbligatorio
- Calcolato in base al ruolo coperto nell'Ateneo
- Es.: staff@unipg.it;member@unipg.it;student@unipg.it

Attributo: *eduPersonTargetedID (ePTID)*

- Identificativo anonimo, persistente, non riassegnabile
- Requisito IDEM: Obbligatorio
- Calcolato nella forma: [organizzazione]![servizio]![stringa opaca]

- Es.: https://idp.unipg.it/idp/shibboleth!https://sp-test.garr.it/sp!53694456-da65-4bcd-b280-e98a0a5ce786

Una volta conclusa la fase di test il nostro SP è entrato a far parte della lista dei Service Provider autorizzati dalla Federazione, abilitato così allo scambio di asserzioni SAML, con gli IdP già registrati in IDEM, volte all'Identificazione e Autenticazione degli utenti.

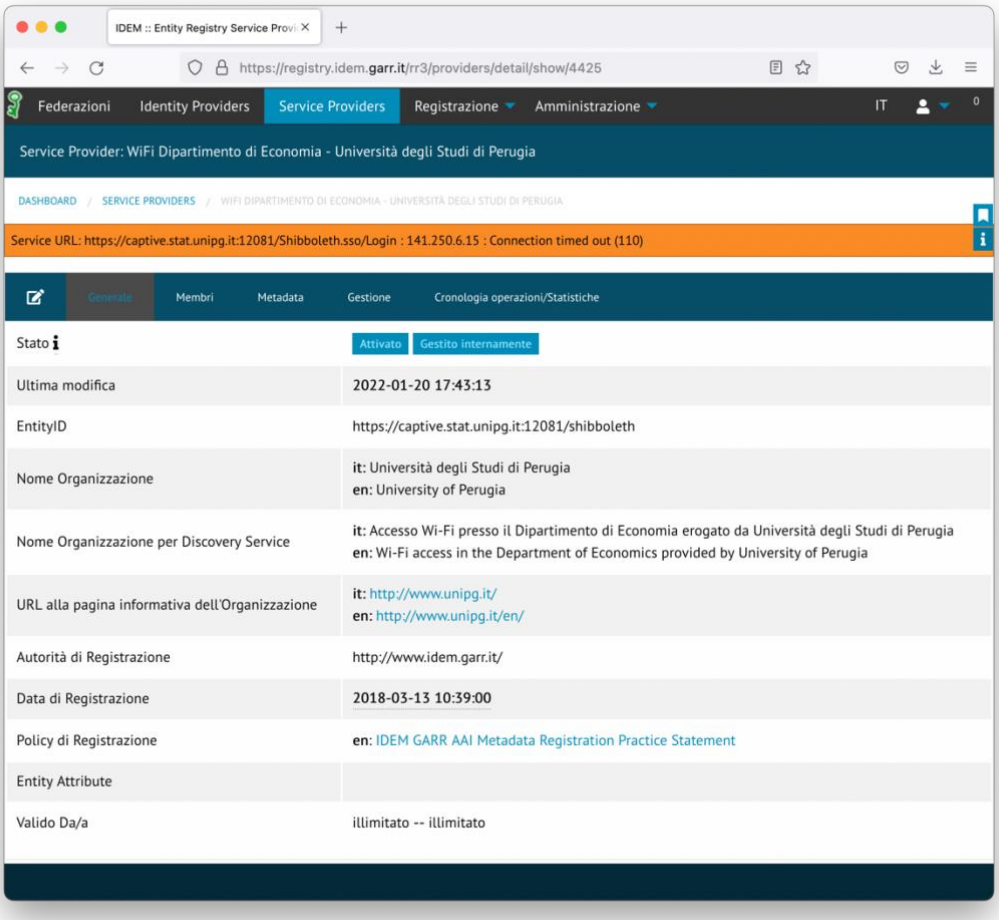


Figura 4.14: Service Provider: WiFi Dipartimento di Economia - Università degli Studi di Perugia

5 Testing e sperimentazione

In conclusione, vengono riportate le schermate che mostrano il funzionamento del Captive Portal realizzato, in particolare:

- Connessione verso l'Identity Provider appartenenti alla Federazione per l'ottenimento dell'Autenticazione;
- Log del Captive Portal;
- Log degli accessi;
- Statistiche del Captive Portal.

5.1 Ciclo di autenticazione

Il funzionamento del Captive Portal con autenticazione federata IDEM può essere testato con un effettivo accesso alla rete Wi-Fi *defs* da un dispositivo mobile o dall'interfaccia di Zeroshell da:

Captive Portal > Authentication > Shibboleth Authentication > Config > Try Authentication

Figura 5.1: Autenticazione Captive Portal Zeroshell - Passo 1

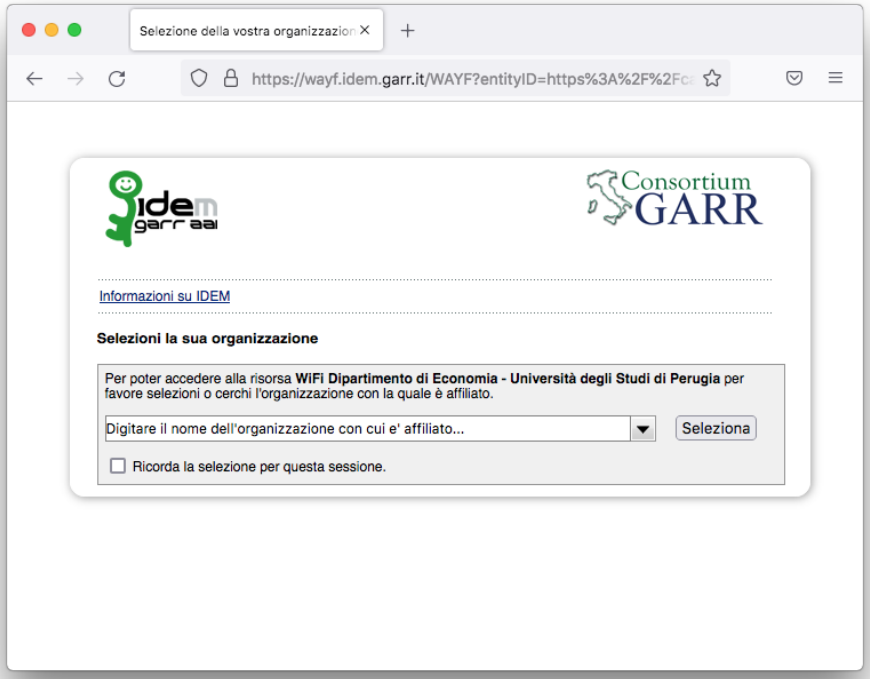


Figura 5.2: Autenticazione Captive Portal Zeroshell - Passo 2

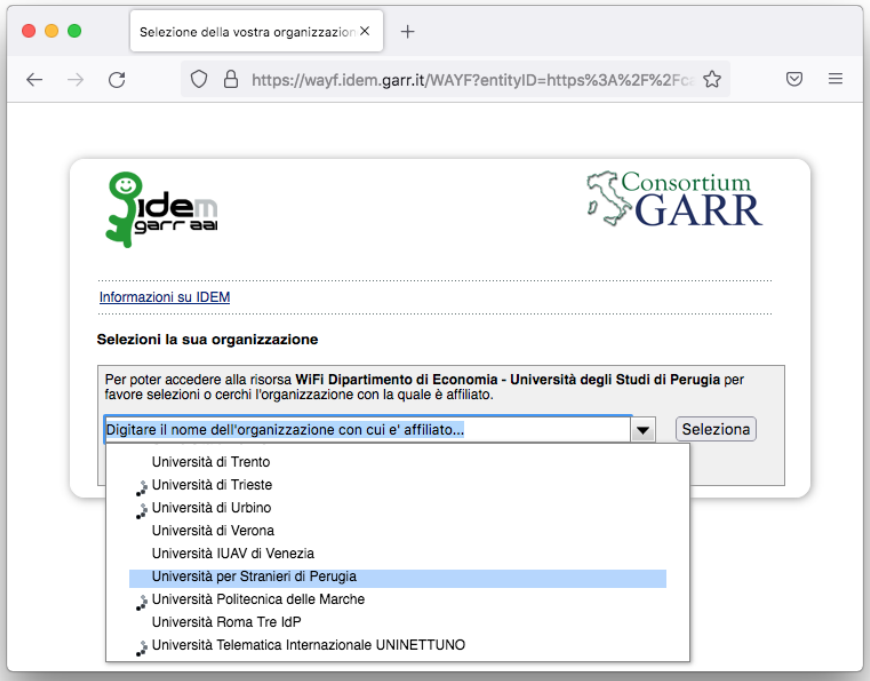


Figura 5.3: Autenticazione Captive Portal Zeroshell - Passo 3

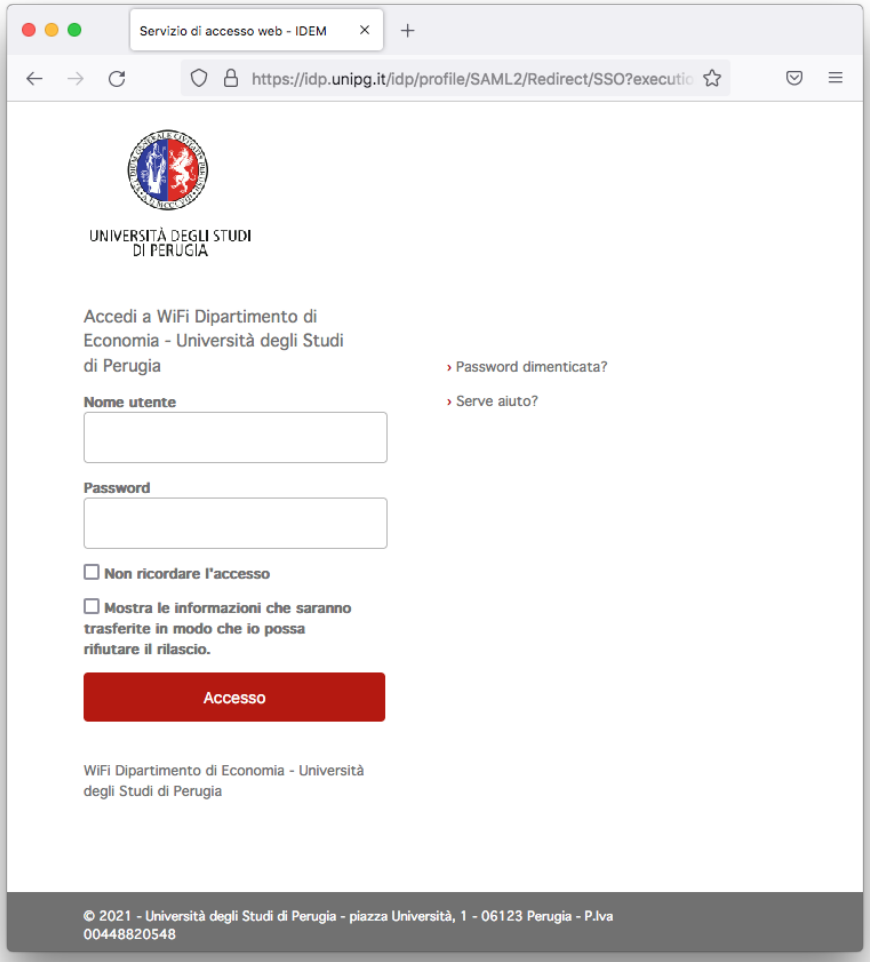


Figura 5.4: Autenticazione Captive Portal Zeroshell - Passo 4

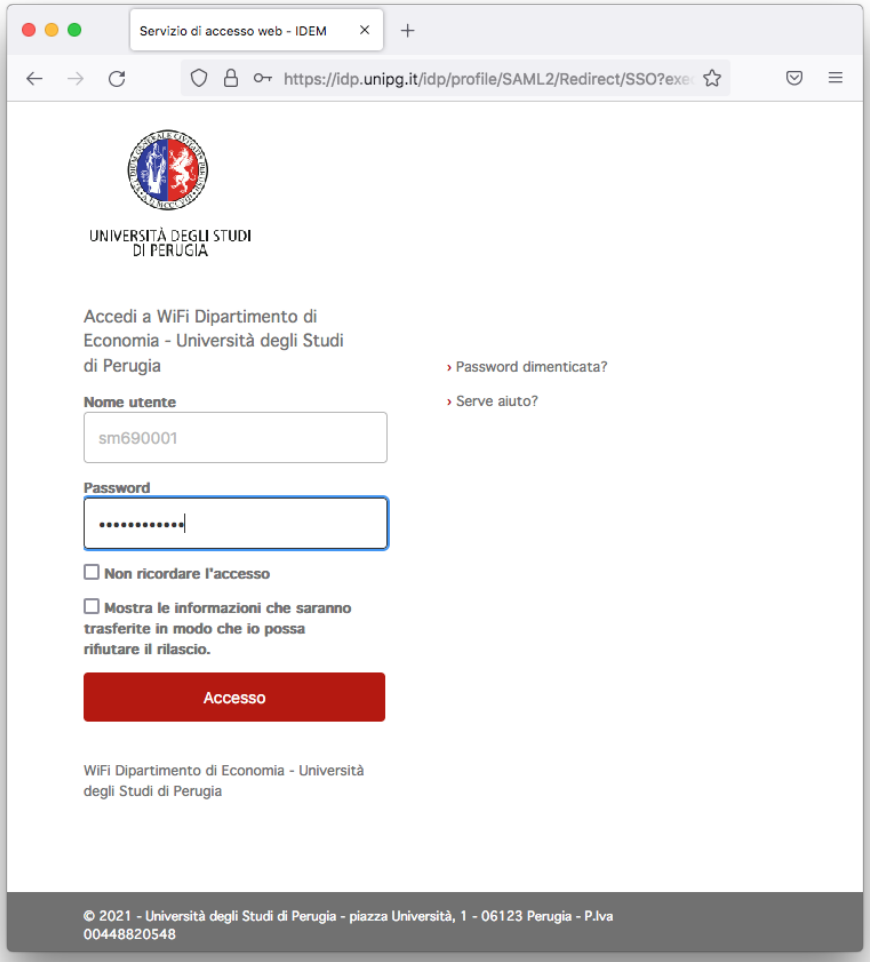


Figura 5.5: Autenticazione Captive Portal Zeroshell - Passo 5

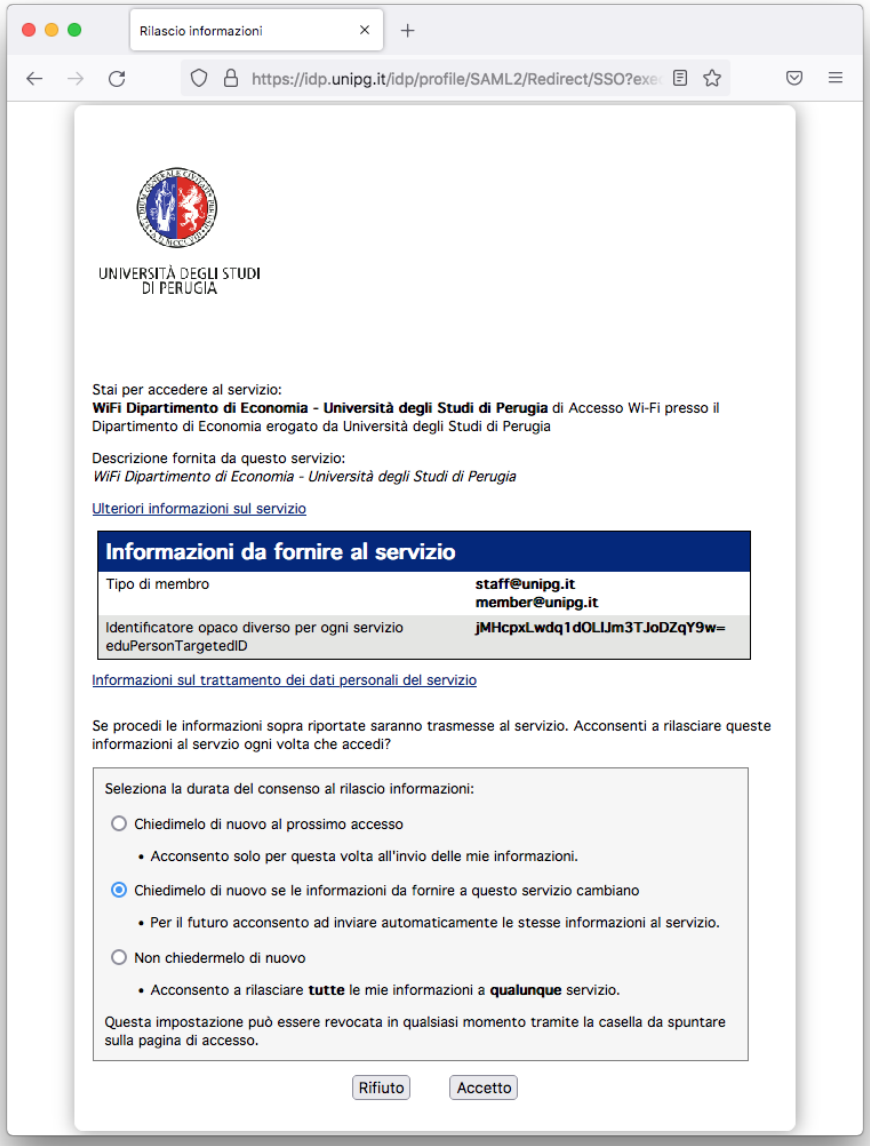


Figura 5.6: Autenticazione Captive Portal Zeroshell - Passo 6

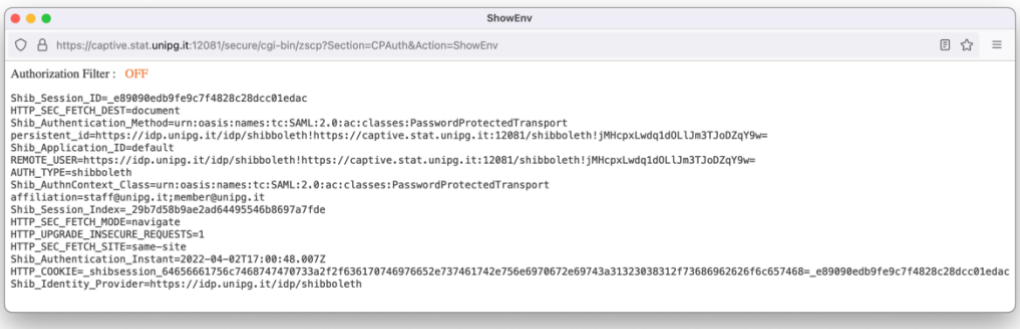


Figura 5.7: Try Authentication Captive Portal Zeroshell – Esito prova

5.2 Log del Captive Portal

L'interfaccia web di Zeroshell fornisce, tra un'ampia possibilità di log, quello relativo al Captive Portal, accessibile da:

Setup > Logs > Section > CaptivePortal

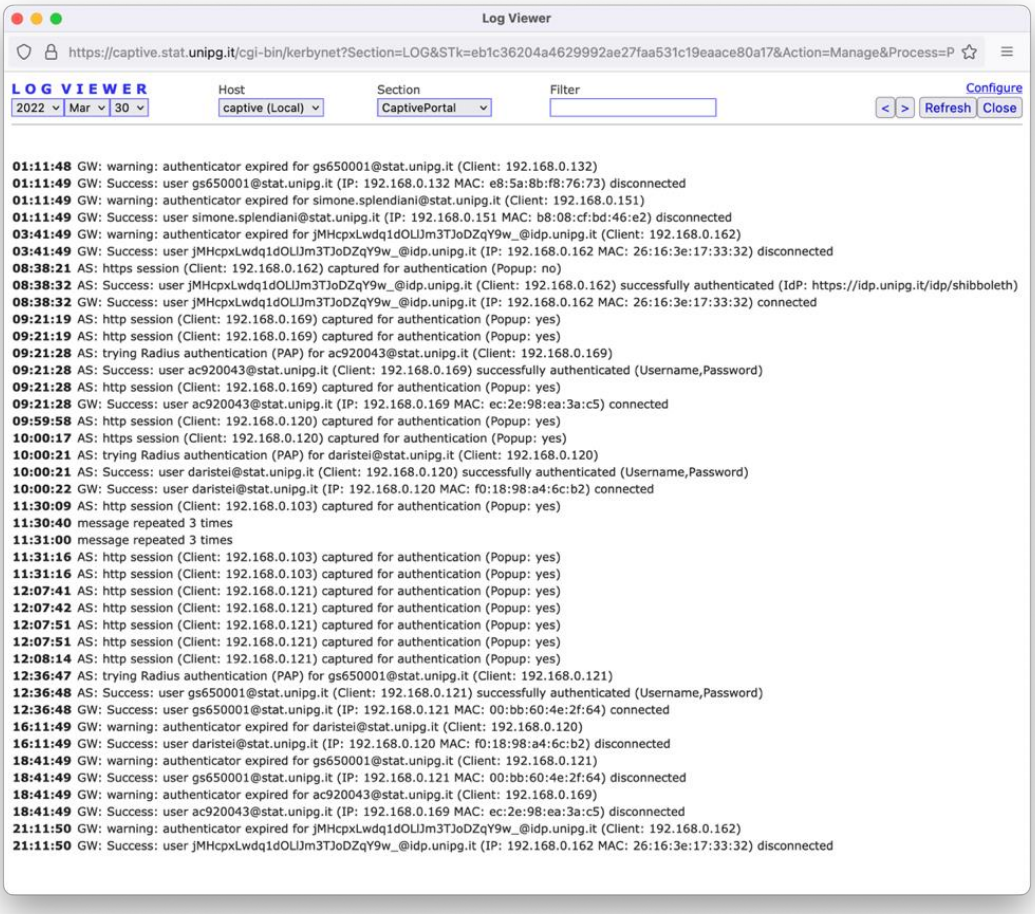


Figura 5.8: Log Captive Portal Zeroshell

Molti altri log possono essere richiesti effettuando la scelta da:

Setup > Logs > Section (es. 802.1X, ConnTrack, dhcpd, radiusd, ecc.)

5.3 Log degli accessi

Il log degli accessi di tutti gli utenti può essere visualizzato da:

Captive Portal > Accounting

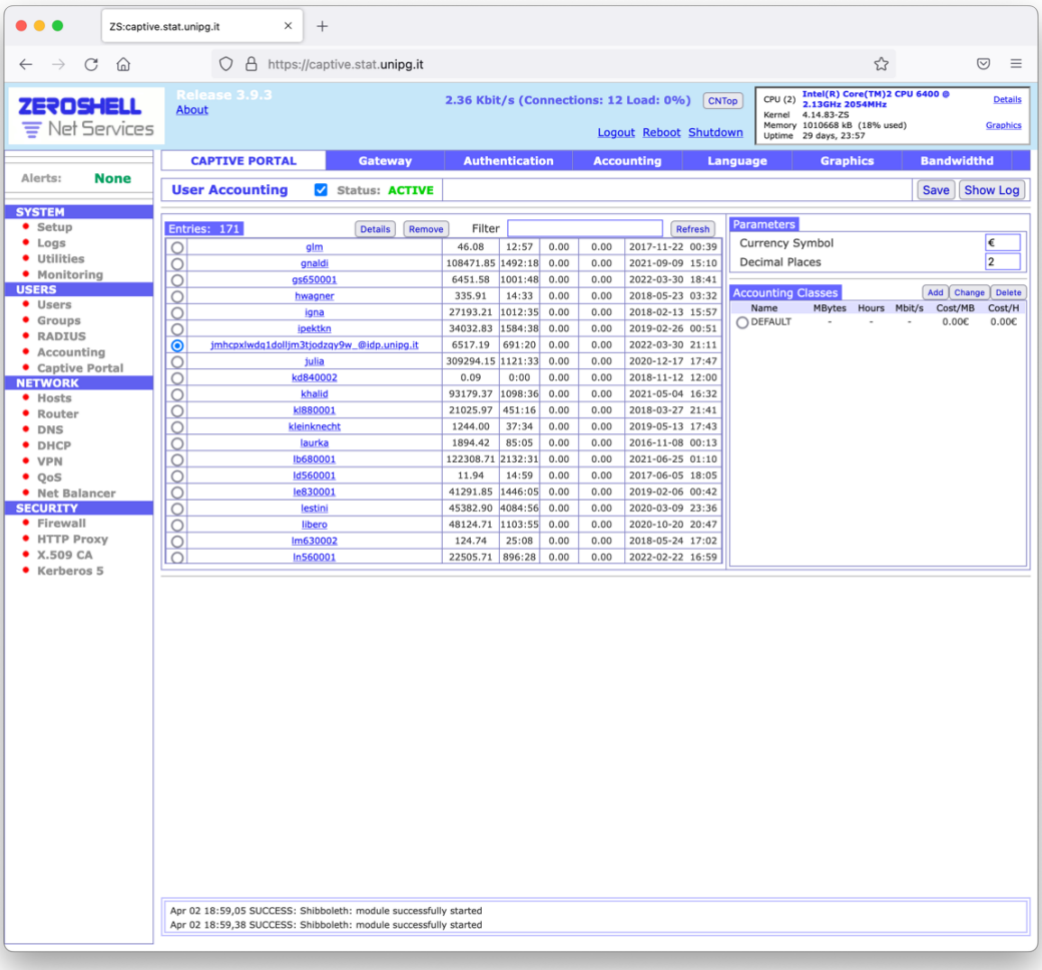
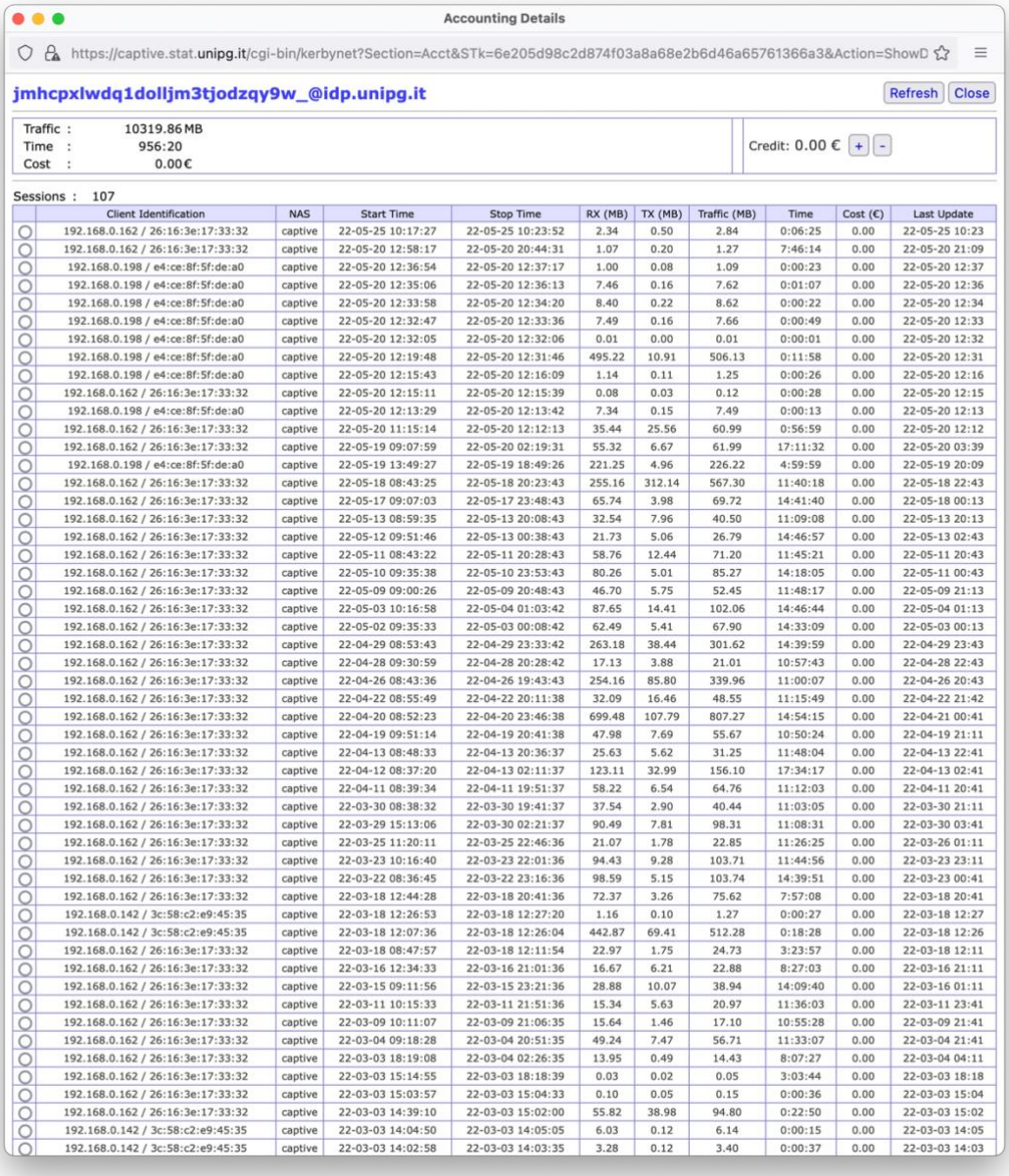


Figura 5.9: Accessi utenti Captive Portal Zeroshell

Il dettaglio degli accessi di un singolo utente può essere visualizzato selezionando lo specifico username da:

Captive Portal > Accounting



	Client Identification	NAS	Start Time	Stop Time	RX (MB)	TX (MB)	Traffic (MB)	Time	Cost (€)	Last Update
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-25 10:17:27	22-05-25 10:23:52	2.34	0.50	2.84	0:06:25	0.00	22-05-25 10:23
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-20 12:58:17	22-05-20 20:44:31	1.07	0.20	1.27	7:46:14	0.00	22-05-20 21:09
○	192.168.0.198 / e4:ce:8f:5f:de:a0	captive	22-05-20 12:36:54	22-05-20 12:37:17	1.00	0.08	1.09	0:00:23	0.00	22-05-20 12:37
○	192.168.0.198 / e4:ce:8f:5f:de:a0	captive	22-05-20 12:35:06	22-05-20 12:36:13	7.46	0.16	7.62	0:01:07	0.00	22-05-20 12:36
○	192.168.0.198 / e4:ce:8f:5f:de:a0	captive	22-05-20 12:33:58	22-05-20 12:34:20	8.40	0.22	8.62	0:00:22	0.00	22-05-20 12:34
○	192.168.0.198 / e4:ce:8f:5f:de:a0	captive	22-05-20 12:32:47	22-05-20 12:33:36	7.49	0.16	7.66	0:00:49	0.00	22-05-20 12:33
○	192.168.0.198 / e4:ce:8f:5f:de:a0	captive	22-05-20 12:32:05	22-05-20 12:32:06	0.01	0.00	0.01	0:00:01	0.00	22-05-20 12:32
○	192.168.0.198 / e4:ce:8f:5f:de:a0	captive	22-05-20 12:19:48	22-05-20 12:31:46	495.22	10.91	506.13	0:11:58	0.00	22-05-20 12:31
○	192.168.0.198 / e4:ce:8f:5f:de:a0	captive	22-05-20 12:15:43	22-05-20 12:16:09	1.14	0.11	1.25	0:00:26	0.00	22-05-20 12:16
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-20 12:15:11	22-05-20 12:15:39	0.08	0.03	0.12	0:00:28	0.00	22-05-20 12:15
○	192.168.0.198 / e4:ce:8f:5f:de:a0	captive	22-05-20 12:13:29	22-05-20 12:13:42	7.34	0.15	7.49	0:00:13	0.00	22-05-20 12:13
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-20 11:15:14	22-05-20 12:12:13	35.44	25.56	60.99	0:56:59	0.00	22-05-20 12:12
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-19 09:07:59	22-05-20 02:19:31	55.32	6.67	61.99	17:11:32	0.00	22-05-20 03:39
○	192.168.0.198 / e4:ce:8f:5f:de:a0	captive	22-05-19 13:49:27	22-05-19 18:49:26	221.25	4.96	226.22	4:59:59	0.00	22-05-19 20:09
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-18 08:43:25	22-05-18 20:23:43	255.16	312.14	567.30	11:40:18	0.00	22-05-18 22:43
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-17 09:07:03	22-05-17 23:48:43	65.74	3.98	69.72	14:41:40	0.00	22-05-18 00:13
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-13 08:59:35	22-05-13 20:08:43	32.54	7.96	40.50	11:09:08	0.00	22-05-13 20:13
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-12 09:51:46	22-05-13 00:38:43	21.73	5.06	26.79	14:46:57	0.00	22-05-13 02:43
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-11 08:43:22	22-05-11 20:28:43	58.76	12.44	71.20	11:45:21	0.00	22-05-11 20:43
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-10 09:35:38	22-05-10 23:53:43	80.26	5.01	85.27	14:18:05	0.00	22-05-11 00:43
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-09 09:00:26	22-05-09 20:48:43	46.70	5.75	52.45	11:48:17	0.00	22-05-09 21:13
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-03 10:16:58	22-05-04 01:03:42	87.65	14.41	102.06	14:46:44	0.00	22-05-04 01:13
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-05-02 09:35:33	22-05-03 00:08:42	62.49	5.41	67.90	14:33:09	0.00	22-05-03 00:13
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-04-29 08:53:43	22-04-29 23:33:42	263.18	38.44	301.62	14:39:59	0.00	22-04-29 23:43
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-04-28 09:30:59	22-04-28 20:28:42	17.13	3.88	21.01	10:57:43	0.00	22-04-28 22:43
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-04-26 08:43:36	22-04-26 19:43:43	254.16	85.80	339.96	11:00:07	0.00	22-04-26 20:43
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-04-22 08:55:49	22-04-22 20:11:38	32.09	16.46	48.55	11:15:49	0.00	22-04-22 21:42
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-04-20 08:52:23	22-04-20 23:46:38	699.48	107.79	807.27	14:54:15	0.00	22-04-21 00:41
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-04-19 09:51:14	22-04-19 20:41:38	47.98	7.69	55.67	10:50:24	0.00	22-04-19 21:11
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-04-13 08:48:33	22-04-13 20:36:37	25.63	5.62	31.25	11:48:04	0.00	22-04-13 22:41
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-04-12 08:37:20	22-04-13 02:11:37	123.11	32.99	156.10	17:34:17	0.00	22-04-13 02:41
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-04-11 08:39:34	22-04-11 19:51:37	58.22	6.54	64.76	11:12:03	0.00	22-04-11 20:41
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-30 08:38:32	22-03-30 19:41:37	37.54	2.90	40.44	11:03:05	0.00	22-03-30 21:11
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-29 15:13:06	22-03-30 02:21:37	90.49	7.81	98.31	11:08:31	0.00	22-03-30 03:41
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-25 11:20:11	22-03-25 22:46:36	21.07	1.78	22.85	11:26:25	0.00	22-03-26 01:11
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-23 10:16:40	22-03-23 22:01:36	94.43	9.28	103.71	11:44:56	0.00	22-03-23 23:11
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-22 08:36:45	22-03-22 23:16:36	98.59	5.15	103.74	14:39:51	0.00	22-03-23 00:41
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-18 12:44:28	22-03-18 20:41:36	72.37	3.26	75.62	7:57:08	0.00	22-03-18 20:41
○	192.168.0.142 / 3c:58:c2:e9:45:35	captive	22-03-18 12:26:53	22-03-18 12:27:20	1.16	0.10	1.27	0:00:27	0.00	22-03-18 12:27
○	192.168.0.142 / 3c:58:c2:e9:45:35	captive	22-03-18 12:07:36	22-03-18 12:26:04	442.87	69.41	512.28	0:18:28	0.00	22-03-18 12:26
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-18 08:47:57	22-03-18 12:11:54	22.97	1.75	24.73	3:23:57	0.00	22-03-18 12:11
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-16 12:34:33	22-03-16 21:01:36	16.67	6.21	22.88	8:27:03	0.00	22-03-16 21:11
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-15 09:11:56	22-03-15 23:21:36	28.88	10.07	38.94	14:09:40	0.00	22-03-16 01:11
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-11 10:15:33	22-03-11 21:51:36	15.34	5.63	20.97	11:36:03	0.00	22-03-11 23:41
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-09 10:11:07	22-03-09 21:06:35	15.64	1.46	17.10	10:55:28	0.00	22-03-09 21:41
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-04 09:18:28	22-03-04 20:51:35	49.24	7.47	56.71	11:33:07	0.00	22-03-04 21:41
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-03 18:19:08	22-03-04 02:26:35	13.95	0.49	14.43	8:07:27	0.00	22-03-04 04:11
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-03 15:14:55	22-03-03 18:18:39	0.03	0.02	0.05	3:03:44	0.00	22-03-03 18:18
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-03 15:03:57	22-03-03 15:04:33	0.10	0.05	0.15	0:00:36	0.00	22-03-03 15:04
○	192.168.0.162 / 26:16:3e:17:33:32	captive	22-03-03 14:39:10	22-03-03 15:02:00	55.82	38.98	94.80	0:22:50	0.00	22-03-03 15:02
○	192.168.0.142 / 3c:58:c2:e9:45:35	captive	22-03-03 14:04:50	22-03-03 14:05:05	6.03	0.12	6.14	0:00:15	0.00	22-03-03 14:05
○	192.168.0.142 / 3c:58:c2:e9:45:35	captive	22-03-03 14:02:58	22-03-03 14:03:35	3.28	0.12	3.40	0:00:37	0.00	22-03-03 14:03

Figura 5.10: Dettaglio accessi utente Captive Portal Zeroshell

5.4 Statistiche del Captive Portal

Le statistiche giornaliere, settimanali, mensili ed annuali delle connessioni al Captive Portal sono accessibili da:

Captive Portal > Graphics > Captive Portal

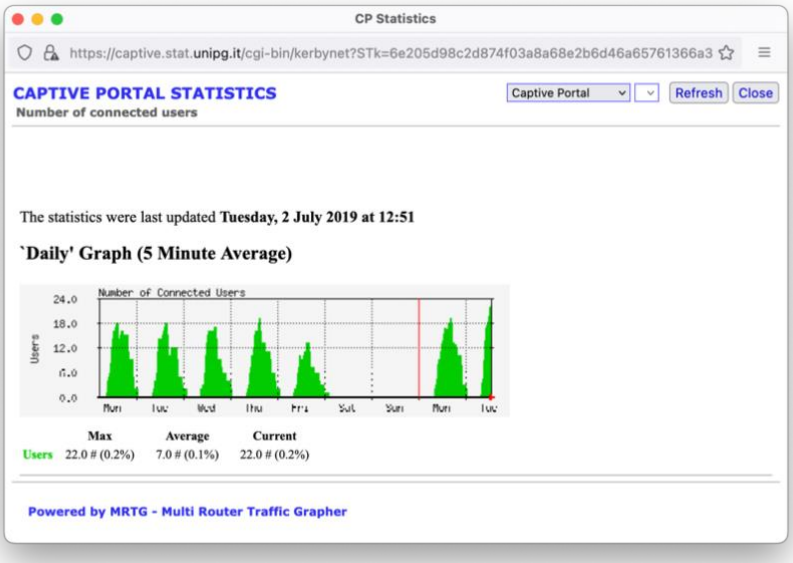


Figura 5.11: Statistiche accessi giornalieri utenti Captive Portal Zeroshell

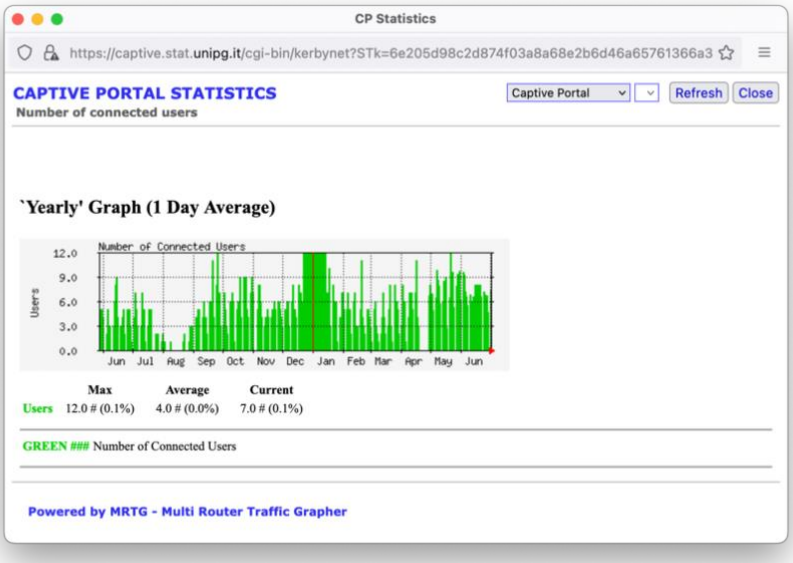


Figura 5.12: Statistiche accessi annuali utenti Captive Portal Zeroshell

Sempre da: Captive Portal > Graphics è possibile visualizzare altre statistiche, tra le quali il traffico relativo alle interfacce di rete.

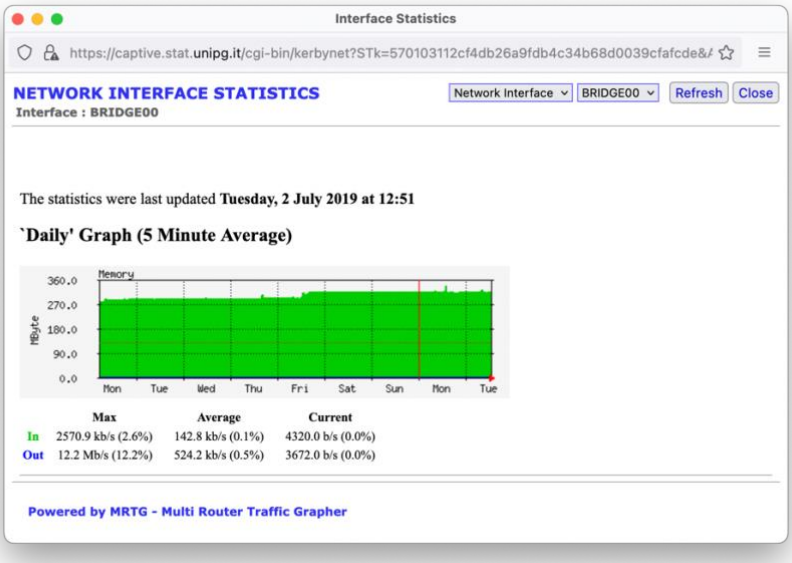


Figura 5.13: Statistiche traffico giornaliero interfaccia BRIDGE00 Captive Portal Zeroshell

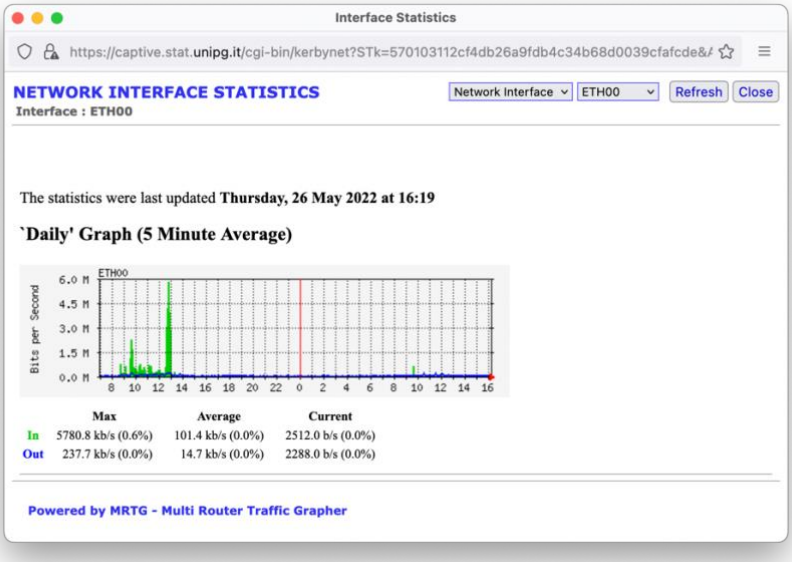


Figura 5.14: Statistiche traffico giornaliero interfaccia ETH00 Captive Portal Zeroshell

Conclusioni

In questa tesi si è scelto di integrare il servizio WiFi del Dipartimento di Economia dell'Università di Perugia in IDEM, poiché la Federazione di identità italiana della rete della ricerca e dell'educazione, è una realtà consolidata ed esistente da diversi anni nelle università e negli enti di ricerca in Italia e nel mondo. Tramite IDEM gli utenti possono accedere a numerosi servizi e risorse, come biblioteche digitali, riviste, pubblicazioni scientifiche, reti WiFi, piattaforme di e-learning, registro elettronico. Inoltre, all'Università degli Studi di Perugia è già esistente un servizio di Shibboleth IdP, gestito dall'Ufficio Reti.

La scelta di Zeroshell è stata determinata dal fatto che la distribuzione già veniva utilizzato come Captive Portal con autenticazione locale usando username/password ed è tra i pochi Captive Portal (open source) a supportare l'integrazione nativa con SAML. Importante è stato anche il fatto che Zeroshell non richieda risorse hardware elevate.

La possibilità di utilizzare più profile è molto utile per testare nuove configurazioni, di contro essendo Zeroshell Read-Only, per questioni di sicurezza, a volte si sono incontrati problemi in particolari configurazioni, es. le modifiche al file *ssl.conf* che ad ogni riavvio vengono perse.

Questo lavoro, si conclude con una sorpresa inaspettata, a fine 2021 Fulvio Ricciardi, INFN Lecce, sviluppatore del progetto Zeroshell ne ha annunciato la dismissione con la versione 3.9.5. Pertanto, sviluppi futuri saranno possibili scegliendo un Captive Portal di analoghe caratteristiche come, ad esempio, CoovaChilli [23] oppure realizzandolo a partire da una distribuzione Linux come Ubuntu [24] o Debian [25].

Bibliografia e Sitografia

[1] IDEM GARR AAI, [Online]. Available: https://www.idem.garr.it/.

[2] Captive portal, [Online]. Available: https://it.wikipedia.org/wiki/Captive_portal.

[3] Zeroshell – Net Services, [Online]. Available: https://www.zeroshell.org/it/.

[4] GARR, [Online]. Available: https://www.garr.it/it/.

[5] Shibboleth Consortium, [Online]. Available: https://www.shibboleth.net/.

[6] Single Sign-On (SSO): Cos'è, Come Funziona e Alcuni Esempi, [Online]. Available: https://itmanager.space/sso-single-sign-on/.

[7] M. Malavolti, «Studio comparativo dei sistemi di getione dei metadati per le federazioni di identità,» 2012. [Online]. Available: https://amslaurea.unibo.it/4460/1/malavolti_marco_tesi.pdf.

[8] SAML Specifications | SAML XML.org, [Online]. Available: http://saml.xml.org/saml-specifications/.

[9] Extensible Markup Language (XML), [Online]. Available: https://www.w3.org/XML/.

[10] REFEDS, [Online]. Available: https://discovery.refeds.org/.

[11] I Certificati Digitali - Cosa sono e come funzionano i certificati digitali, [Online]. Available: https://httplab.it/DigitalCert.

[12] «cifratura_messaggio.png,» [Online]. Available: https://blog.bit4id.com/wp-content/uploads/2017/05/cifratura_messaggio.png.

[13] «processo_certificazione_digitale.png,» [Online]. Available: https://blog.bit4id.com/wp-content/uploads/2014/07/processo_certificazione_digitale.png.

[14] «Struttura_certificato_x509.PNG,» [Online]. Available: https://it.wikipedia.org/wiki/X.509#/media/File:Struttura_certificato_x509.PNG.

[15] «wayf.png,» [Online]. Available: https://people.unica.it/idem/files/2008/11/wayf.png.

[16] «Giudici.png,» [Online]. Available: https://people.unica.it/idem/files/2011/12/Giudici.png.

[17] «The-service-model-of-Shibboleth-Shibboleth-proposed-WAYF-Where-Are-You-From-mechanism.png,» [Online]. Available: https://www.researchgate.net/figure/The-service-model-of-Shibboleth-Shibboleth-proposed-WAYF-Where-Are-You-From-mechanism_fig5_40723539.

[18] L. Ianniello e A. Pifferi, «Accesso Wi-Fi con Autenticazione Federata.,» *Smart eLab,* vol. 8, 2016.

[19] A. Pifferi, L. Ianniello, C. Ricci, L. Rossi e M. Simonetti, «Un Captive Portal per l'utenticazione su Reti Wifi Dedicate agli Internet Access Point Liberi.,» *Smart eLab,* vol. 2, 2013.

[20] IDEM :: Entity Registry IDEM Entity Registry, [Online]. Available: https://registry.idem.garr.it/rr3/.

[21] FreeRADIUS, [Online]. Available: https://freeradius.org/.

[22] F. Ricciardi, «Zeroshell come Captive Portal per l'accesso ad IDEM - IDEM DAY Bologna,» 10 Novembre 2011. [Online]. Available: https://www.idem.garr.it/federazione-idem/convegni-incontri-corsi/terzo-idem-day-10-11-2011-cnr-bologna/570-ricciardi-presentazione-1/file.

[23] Open-source captive portal and RADIUS solutions, [Online]. Available: https://coova.github.io/.

[24] Ubuntu Italia, [Online]. Available: https://www.ubuntu-it.org/.

[25] Debian -- Il Sistema Operativo Universale, [Online]. Available: https://www.debian.org/index.it.html.

Ringraziamenti

Ringrazio il Prof. Fausto Marcantoni, che mi ha seguito con grande competenza e disponibilità in questo lungo percorso.

Ringrazio Tiziana Jajani, che in tutti questi anni mi ha incoraggiato a raggiungere questo traguardo ed è diventata un'amica.

Ringrazio la mia famiglia, mia moglie Anna Maria ed i miei tre splendidi figli Sofia, Filippo e Federico che mi hanno spinto a dare il massimo.

Ringrazio il mio amico Prof. Walter Betori, senza il suo aiuto l'esame di Fisica non lo avrei mai superato. Lo ringrazio anche per avermi spronato costantemente a non lasciare quando mancava soltanto la tesi.

E "last but not least", ringrazio il "Grifo", compagno di una vita.

Voglio dedicare questa tesi di laurea a mia nonna Felicetta scomparsa diversi anni fa. Sono convinto che avrebbe detto: "Questa tesi è mondiale!".

Sandro Massini 23/05/2022