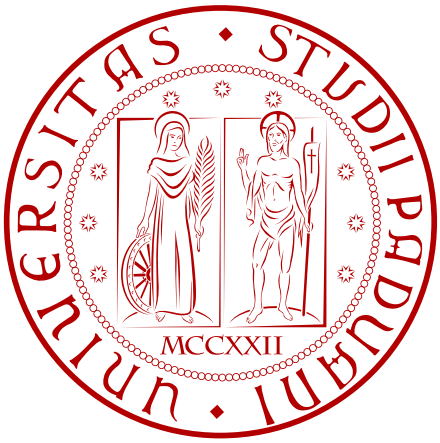
SINGLE SIGN-ON PER MOODLE

MICHELE MAROSTICA



Laurea in Ingegneria Informatica
Relazione di Tirocinio

Febbraio 2011

Dedico questo lavoro ai miei genitori.

SOMMARIO

In questa relazione di tirocinio verrà descritto come è stato aggiunto il metodo di Single Sign-On alla piattaforma LMS Moodle dell'Università degli Studi di Padova.

RINGRAZIAMENTI

Ringrazio i miei genitori che mi hanno permesso di raggiungere questo importante obbiettivo, la mia famiglia, Silvia e i miei amici.

Il periodo che ho trascorso presso il centro di calcolo si è rivelato un'importante esperienza lavorativa, soprattutto come voce per il curriculum vitae. Spero con ciò che ho prodotto di aver apportato un buon contribuito prima di tutto ai miei colleghi studenti dell'ateneo di Padova, alla comunità di Moodle e a tutte le persone che prima o poi accederanno a tale piattaforma tramite il mio modulo per il Single Sign-On.

INDICE

ELENCO DELLE FIGURE

ELENCO DEI CODICI

ACRONYMS

SSO Single Sign-On

SAML Security Assertion Markup Language

CCA Centro di Calcolo di Ateneo

SSD Servizio e Supporto alla Didattica

LMS Learning Management System

IDP Identity Provider

SP Service Provider

GPL General Purpose Lincense

FOSS Free and Open Source Software

1 INTRODUZIONE

L'attività svolta durante il periodo di tirocinio, presso l'ufficio Servizio e Supporto alla Didattica del Centro di Calcolo di Ateneo, oggetto di questa relazione, consiste nel definire e realizzare un metodo di Single Sign-On per la piattaforma di Learning Management System (LMS) adottata dall'ateneo di Padova: Moodle.

1.1 MOODLE

Moodle è un Learning Management System (LMS) open source a licenza General Purpose Lincense (GPL) [11] molto diffuso in ambiente universitario e con un'ampia comunità di supporto alle spalle `http://www.moodle.org` [6]. Deve la sua diffusione alla estrema semplicità di utilizzo. L'architettura di tipo modulare, la possibilità di aggiungere nuove funzionalità e di personalizzare la piattaforma rendono questo strumento estremamente adattabile a molteplici esigenze. E' la scelta ideale per coloro che cercano un gran numero di funzionalità e che prevedono di investire molte risorse, a livello organizzativo, nel programma di formazione. E' una piattaforma web-based open source: è un progetto, nato negli anni '90, che continua il suo sviluppo con l'obiettivo di creare un ambiente di supporto alla didattica basato sul costruttivismo sociale, percio' integra al suo interno diversi strumenti per il lavoro collaborativo (forum, instant messaging, sistema integrato di e-mail, gestione gruppi di lavoro, agenda condivisa, blog, wiki). Moodle puo' essere installato su un qualsiasi piattaforma che supporti PHP, Apache e MySQL, ed è tradotto in più di 80 lingue. Altro aspetto che fa ulteriormente apprezzare Moodle è la facilità dal punto di vista dell'amministrazione di personalizzare l'interfaccia utente con la possibilità di spostare, cancellare o aggiungere moduli. Il sistema usa fogli di stile/CSS e pagine web PHP alle quali è relativamente semplice apportare modifiche.

1.2 SERVIZIO E SUPPORTO ALLA DIDATTICA DEL CENTRO DI CALCOLO DI ATENEO (SSD)

Il personale del Servizio e Supporto alla Didattica (SSD) del Centro di Calcolo di Ateneo (CCA) svolge un compito di supporto alla didattica fornendo agli utenti tre tipologie di strumenti:

1.2.1 *Moodle*

In Ateneo sono 11 le Facoltà che utilizzano piattaforme Moodle gestite dal SSD. Le Facoltà che utilizzano il servizio sono: Facoltà di Agraria, Facoltà di Economia, Facoltà di Farmacia, Facoltà di Giurisprudenza, Facoltà di Ingegneria, Facoltà di Lettere e Filosofia, Facoltà di Medicina e Chirurgia, Facoltà di Medicina e Veterinaria, Facoltà di Scienze Politiche, Facoltà di Statistica. Il SSD gestisce attualmente 10 esemplari di Moodle, con circa 22.000 utenti/studenti e 700 utenti/docenti (nella categoria docenti sono comprese anche le figure di tutor). In Ateneo 3 servizi dell'Amministrazione centrale utilizzano Moodle, con piattaforme dedicate, come applicativo gestionale: Servizio Civile, Servizio Relazioni Internazionali, Servizio Orientamento, oltre al Centro Diritti Umani, che ha le proprie attività sul Moodle di Ateneo.

1.2.2 *QuestionMark Perception*

QuestionMark Perception [7] è il software per l'erogazione di esami è utilizzato in 5 Facoltà: Facoltà di Economia, Facoltà di Giurisprudenza, Facoltà di Ingegneria, Facoltà di Lettere e Filosofia, Facoltà di Psicologia, Facoltà di Scienze MM.FF.NN.. Sono circa 50 i docenti che lo utilizzano; sono 60 le materie i cui esami sono fatti attraverso questo software. Vengono erogati circa 15.000 esami/anno. Oltre allo svolgimento di prove di valutazione Perception viene utilizzato per consentire agli studenti di fare simulazioni d'esame, circa 110.000 simulazioni/anno. Il software viene utilizzato anche per la costruzione di questionari e survey per la raccolta di dati per attività di ricerca (circa 60.000 compilazioni/anno). Il software è utilizzato da 4 servizi dell'Amministrazione centrale: Ufficio Stage e mondo del lavoro, Ufficio Relazioni Internazionali, Servizio Orientamento, Servizio Civile. Sono circa 60 gli strumenti attivi fra questionari, survey e sondaggi, vengono raccolti circa 150.000 record/anno

1.2.3 *Dynamic 08*

Con il software Dynamic 08 [3] viene erogato un servizio di lettura ottica per la correzione di esami di profitto e la gestione delle prove in itinere. Il SSD implementa su richiesta dei docenti la scheda per la lettura ottica, il programma di acquisizione dati, il programma di correzione e il file di output. Attualmente il lettore ottico è utilizzato da 2 facoltà (Facoltà di Scienze Politiche e Facoltà di Medicina e Chirurgia) per lo svolgimento di 3 esami da parte di 2 docenti e per la gestione delle prove in itinere. Attualmente il lettore ottico è utilizzato da Segreterie studenti e Servizio Organizzazione; le attività svolte dal SSD sono: proget-

tazione foglio per la lettura e implementazione programma di lettura, stampa schede, lettura ottica e preparazione output.

1.2.4 *Attività svolte*

Nel contesto dell'ufficio SSD sono state svolte 4 attività, 2 su richiesta dei docendi del Diparitmento di Ingegneria dell'Informazione (DEI), una richiesta dalla facoltà di Psicologia e la quarta è quella prevista per l'attività di tirocinio e oggetto di questa relazione.

1.2.4.1 *Foglio di calcolo*

Il primo lavoro che è stato svolto durante il periodo del tirocinio, è stato richiesto da un docende del DEI, aggiungere la possibilità di scaricare un foglio di calcolo (spreadsheet) contenente una tabella degli studenti aderenti ad un corso dalla pagina Partecipanti accessibile dai singoli corsi, mantenendo la possibilità presente in tale pagina di utilizzare dei fltri di selezione. Si è reso necessario un gran lavoro di reverse engineering e di studio su come creare con la libreria di PHP un foglio di calcolo. E' stata usata da esempio una funzionalità simile presente in un'altra sezione di Moodle. Lla modifica da effettuare consiste nell'aggiunta di una decina di righe di codice PHP in due pagine di Moodle e nell'inclusione di un file contenente la funzione per generare il foglio di calcolo nella cartella /user sempre di Moodle.

1.2.4.2 *Invio mail*

La seconda funzionalità sviluppata, richiesta da un amministratore di un esemplare di Moodle del DEI, è stata quella di aggiungere la capacità al modulo Reservation, il modulo per la prenotazione degli esami, di inviare una mail agli utenti che hanno effettuato l'iscrizione ad un esame. La diffcoltà più grande in questo caso è stata la totale assenza di commenti al codice e di documentazione e l'indisponibilità dello sviluppatore di tale modulo (utente del forum) a collaborare. Si è resa necessaria una settimana di reverse engineering del codice solo per capire dove mettere le mani e in che modo; poi è stato abbastanza semplice terminare il lavoro essendo tale funzione è già presente in un altra parte di Moodle, e da questa, avendo una documentazione decente, è stato indolore prendere spunto (copiarla e personalizzarla) per completare il modulo di prenotazione.

1.2.4.3 *Limesurvey*

Dalla facoltà di Psicologia è giunta la richiesta per l'integrazione di Limesurvey [4] in Moodle, Limesurvey è un sistema Free and Open Source Software (FOSS) per generare e gestire sondaggi.

Il problema da risolvere è stato quello di dare la possibilità ai docenti di selezionare gli studenti e le persone, utenti di Moodle, a cui fare un sondaggio in base ad un contesto; cioè ad esempio a tutti gli studenti di un corso, a tutti gli studenti di Moodle, a tutti i docenti, ecc.. Sul forum di moodle.org era già presente un Blocco che notifica all'utente collegato il fatto che ha un sondaggio attivo in LimeSurvey che deve ancora compilare, ma questo non da la possibilità di selezionare gli utenti a cui fare il sondaggio. Quindi è stata creata una pagina apposita con l'ausilio di una multiselect, elemento html personalizzato da ryancramerdesign (sotto licenza MIT-license [5]) *jquery-asmselect* reperibile su `code.google.com`.

Limesurvey non ha al suo interno un database che gestisce le persone a cui fare i sondaggi, ma gestisce solo gli utenti che possono creare o modificare un sondaggio; quindi si è dovuto mettere a punto un meccanismo che dall'esterno (Moodle) potesse aggiungere partecipanti. E' stato sfruttato il fatto che Limesurvey da la possibilità di assegnare dei Token, gettoni, a chi deve compilare un sondaggio, associandoli all'indirizzo e-mail che è un dato univoco. Infatti nella pagina creata per selezionare gli utenti in Moodle è stato fatto proprio questo, viene fornito un menù a tendina da cui scegliere il sondaggio attivo a cui aggiungere partecipanti e poi vengono aggiunti automaticamente nella tabella dei token del sondaggio scelto nel database di Limesurvey una tupla per ogni utente contentente il numero di token (incrementale rispetto al massimo già presente) e l'indirizzo email. In questo caso il lavoro da eseguire consiste nella sola installazione del blocco Limesurvey in Moodle, e di Limesurvey ovviamente. Bisogna assicurarsi poi che alla creazione di un sondaggio si attivi la gestione dei token per esso.

1.2.4.4 *Single Sign-On (SSO)*

La quarta attività che si è svolta, che è l'oggetto di questa relazione, è stata quella di dare la capacità a Moodle di utilizzare il server Shibboleth [8] per il Single Sign-On (SSO) [13] già adottato dalla piattaforma per la gestione degli studenti di ateneo (UNIWEB [9]) e quindi di eliminare quella sorta di discontinuità che separava questi servizi forniti dall'ateneo agli studenti.

2 SINGLE SIGN-ON (SSO)

Si parla di sistema basato su Single Sign-On (SSO) [13] quando le richieste di autenticazione non vengono direttamente gestite dal sistema stesso ma vengono ridirette verso un altro sistema di autenticazione che ha precedentemente certificato le credenziali dell'utente connesso, senza quindi avere la necessità di richiedere nuovamente le credenziali per l'accesso. L'obiettivo principe del SSO è quello di rendere la sicurezza trasparente all'utente finale, facilmente mantenibile e gestibile per gli amministratori; l'utente deve rendersi conto di lavorare in un sistema sicuro, ma non deve assolutamente vivere la sicurezza come un onere aggiuntivo. Una premessa doverosa da fare è la seguente: a qualcuno dobbiamo necessariamente porre la nostra fiducia, che questo qualcuno sia l'utente finale che digita la combinazione di username e password o sia il server di un servizio che ha in precedenza autenticato l'utente connesso fa poca differenza, dobbiamo solamente scegliere di chi fidarci. La scelta è ricaduta sul server piuttosto che chiedere nuovamente le credenziali all'utente; tutto ciò per i motivi che abbiamo appena elencato (trasparenza, sicurezza e semplicità).

2.1 SECURITY ASSERTION MARKUP LANGUAGE (SAML)

Security Assertion Markup Language (SAML) [12] è un linguaggio standard per lo scambio di dati di autenticazione e di autorizzazione tra domini di sicurezza distinti, in genere un Identity Provider ed un Service Provider. SAML definisce l'utente Principal il quale deve necessariamente essere registrato in almeno un Identity Provider, ad esso spetta il compito dell'autenticazione. Su richiesta del principal l'Identity Provider passa una asserzione SAML al Service Provider sulla base della quale quest'ultimo decide se permettere o negare l'accesso ai propri servizi da parte del principal.

2.2 SHIBBOLETH

Shibboleth [8] è un pacchetto open source per ottenere la funzionalità di Single Sign-On sul web all'interno o attraverso i confini di un organizzazione. Sempre più università, organizzazioni e uffici della pubblica amministrazione offrono servizi online, gli utenti generalmente accedono a risorse web che risiedono sia internamente che esternamente alla loro organizzazione per fare il loro lavoro. Ad esempio gli studenti dell'università di Pado-

va possono utilizzare l'LMS Moodle, la web mail di ateneo e il nuovo sistema informativo Uniweb i quali sono ospitati in parte al Centro di Calcolo di Ateneo e in parte in Cineca. In passato ognuno di questi servizi necessitava di un suo specifico ID e di una sua specifica password per ogni utente registrato a tale servizio. Ciò rende complicata la gestione dei servizi e può generare delle falle di sicurezza. Con Shibboleth si è riusciti a risolvere questo problema, ogni utente utilizza il suo ID di ateneo con la rispettiva password per accedere a tutti i servizi offerti dall'università fornendo la funzionalità di Single Sign-On. Dal punto di vista del Service Providers Shibboleth sostanzialmente riduce i rischi e il tempo impiegato nell'offrire un servizio. In passato venivano passati ai Service Providers grossi file di dati di identità per aggiornare e creare gli account, ora i providers ricevono le informazioni aggiornate ogni volta che l'utente accede a tale risorsa, quindi non c'è più il bisogno di mantenere aggiornati i dati relativi ai vari profili. Anche dal punto di vista della sicurezza questo porta al vantaggio di eliminare il rischio di potenziali accessi dannosi causati da un mancato aggiornamento.

Il sistema Shibboleth comprende due componenti software principali: l'Identity Provider (IdP) e il Service Provider (SP). Sono due componenti separate ma che lavorano in simbiosi per assicurare l'accesso alle risorse web. Questa è la descizione del processo passo-passo di come funziona Shibboleth:

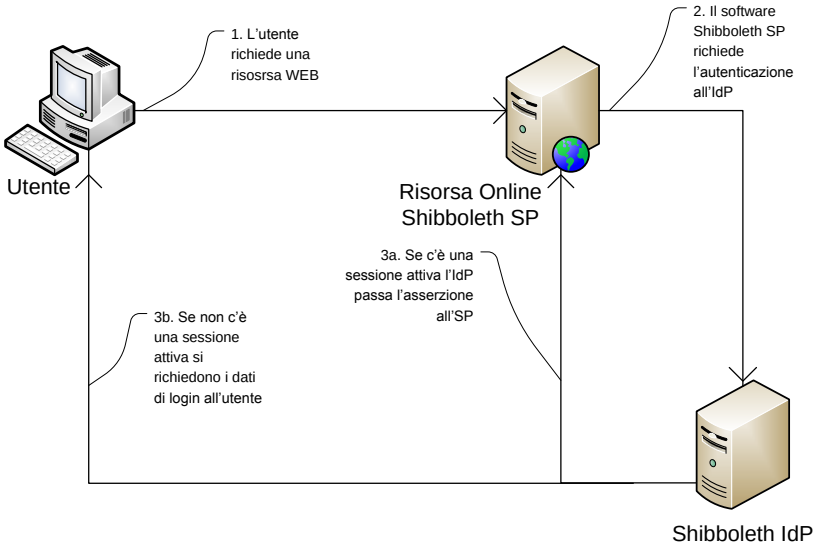


Figura 1: Funzionamento di Shibboleth

1. L'utente giunge alla risorsa web tramite il suo browser. La risorsa è protetta, quindi richiede informazioni sull'utente per decidere se permettere o meno l'accesso.

2. L'utente esegue il login dalla risorsa, passando per una pagina che nel caso del nostro ateneo è uguale per tutte le tre risorse e invia i dati all'Identity Provider.

3. L'IdP produce come risultato un insieme di informazioni di sicurezza chiamato asserzione che prova l'effettiva avvenuta autenticazione dell'utente.

4. Il software SP di Shibboleth convalida l'asserzione e passa le informazioni al provider web della risorsa. Quest'ultimo, infine, decide in base ai dati contenuti nell'asserzione e alla sua politica di sicurezza se permettere o meno l'accesso all'utente.

Spesso taluni passaggi possono essere saltati, ad esempio se l'utente ha già una sessione aperta in un altro SP dotato della funzionalità di single sing-on allora la pagina comune di login non verrà visualizzata ma verrà automaticamente dato l'accesso alla risorsa richiesta (sempre rispettando le politiche locali di sicurezza). Un aspetto chiave che ha fortemente influenzato la realizzazione di Shibboleth è stato quello di garantire una protezione alla privacy degli utenti. I provider delle risorse ricevono al più le informazioni che necessitano per permettere il controllo dell'accesso. Il software Shibboleth IdP ha un sottosistema per gestire le politiche di diffusione degli attributi, permettendo un'efficace filtraggio dinamico delle informazioni in uscita.

3 REQUISITI

I requisiti principali da rispettare per la progettazione del metodo di SSO per la piattaforma Moodle dell'ateneo di Padova sono la maggior trasparenza possibile nel passaggio da Moodle stesso alla pagina di login del sistema di SSO comune per tutti i servizi dell'ateneo e la migrazione delle vecchie utenze Moodle che non rispettano la definizione delle nuove (es. diversità di definizione dei campi, primo su tutti l'username). Questa migrazione deve avvenire senza perdita di dati e deve gestire l'eterogeneità degli stessi precedentemente contenuti nella base di dati.

3.1 SICUREZZA

La procedura di Single Sign-On è intrinsecamente sicura dato che:

- Utilizza il protocollo https per la comunicazione criptata della password;
- Separa la fase di autenticazione da quella di autorizzazione, ciò significa che tutte le credenziali (username e password) per l'accesso vengono gestite da un solo server, quello del SSO, mentre i server che gestiscono i servizi (ad es. moodle) vengono sgravati dall'onere della sicurezza degli accessi perché non vengono nemmeno a conoscenza di tali informazioni;
- Inoltre il server che gestisce il Single Sign-On è ospitato in un data center sicuro sia dal punto di fista fisico-ambientale che dal punto di vista software (è un server dedicato solo a questa funzione).

Dato che un'unica password proteggerà più servizi è necessario:

- Rendere sicura la password collegata alla posta elettronica, questo significa inserire nella password: lettere, numeri, simboli di interpunzione. La password dovrà essere formata da 8 caratteri;
- Non cedere a nessuno la propria password, dato che quando la cediamo non cediamo solo la possibilità ad una terza persona di entrare in moodle ma anche di vedere la nostra posta e le nostre pagine per i servizi che affluiranno al SSO;

- Chiudere il browser per uscire definitivamente da tutti i servizi acceduti sotto SSO.

3.2 TRASPARENZA

Per limitare l'effetto dell'impatto con il nuovo sistema di SSO agli utenti, il blocco di login in Moodle sarà nella stessa posizione del precedente e molto visibile, e una volta giunti alla pagina di login in essa l'utente troverà tutte le informazioni di cui ha bisogno per poter sfruttare il nuovo metodo di accesso. Il tutto tenendo presente che ci sarà già una certa familiarità al metodo, essendo esso utilizzato anche per il nuovo sistema informativo UNIWEB [9].

3.3 MIGRAZIONE

Il problema di fondo della migrazione dei vecchi utenti sta nei diversi domini utilizzati per i campi del database di Moodle e di quelli definiti per i valori che Shibboleth passa a Moodle nell'asserzione SAML; e di quali campi vengono utilizzati come chiave primaria nei due schemi.

4 SVILUPPO

L'autenticazione SSO si basa sul modulo già presente in Moodle chiamato: Shibboleth. A questo il resto dei componenti che sono stati sviluppati si agganciano con particolari campi riportati più avanti. Il modulo Shibboleth di Moodle viene esteso realizzando un filtro sulle utenze basato sul campo email e sul campo codice di corso di laurea. A tal fine per la configurazione viene reso disponibile il blocco per Moodle *shib_emercency*. Esso gestisce le password, i corsi abilitati all'entrata, gli help che carpiscono i dati degli utenti sia in caso di autenticazione riuscita che non. Viene reso disponibile un ulteriore blocco per Moodle *shib_login* che gestisce l'autenticazione.

4.1 STRUMENTI DI SVILUPPO

Gli strumenti di sviluppo adottati sono 3 personal computer, uno per la realizzazione dei componenti e 2 configurati a server di test. Uno con Apache HTTPD 2.3 per la gestione dei contenuti web sul quale è possibile caricare i file tramite il software WebDav [10], e l'altro con un'installazione di MySQL 5.1.41 alla quale è possibile accedere tramite phpMyAdmin per le funzioni di creazione e gestione dei vari database di test.

Tutte le postazioni, i server di prova e le stampanti dell'ufficio sono collegate in una rete Ethernet a 100Mbps con gli indirizzi IP preassegnati dai sistemisti.

L'accesso ai server di produzione situati al piano terra del centro di calcolo o al CINECA [1] è precluso per motivi di sicurezza. I file prodotti e testati in ufficio devono essere spediti via mail al membro del personale addetto alla gestione di tali server, che li caricherà nella destinazione desiderata da riportare nella mail.

Gli strumenti software adottati per supportare lo sviluppo dei componenti richiesti sono:

ECLIPSE FOR PHP DEVELOPERS: IDE specializzato per applicazioni web based in php;

NOTEPAD++: editor di testo avanzato per veloci modifiche al codice;

WEBDAV: strumento per il trasferimento dei file prodotti sul web server di prova; [10]

PHPMYADMIN: interfaccia in PHP per la gestione del database mySQL;

GOOGLE CHROME, MOZILLA FIREFOX E INTERNET EXPLORER: principali browser di test.

I linguaggi di programmazione utilizzati per questo progetto sono stati: php per la creazione delle pagine web dinamiche, HTML per le pagine web statiche, javascript per definire alcune funzioni di utilità lato client in certe pagine web. Per la manipolazione del database di Moodle si è utilizzato SQL nella versione per il RDBMS mySQL.

4.2 COMPONENTI DA SVILUPPARE

PAGINA DI LOGIN MODIFICATA: pagina HTML adattata al nuovo sistema di autenticazione.

BLOCCO *shib_emergency*: blocco per la gestione da parte dello staff SSD del metodo di autenticazione tramite Shibboleth.

BLOCCO *shib_login*: blocco che permette l'autenticazione tramite il metodo di SSO.

PAGINA *./auth/shiboleth/index.php*: modifica al codice di questo file per incrociare i dati tra Moodle e la SAML.

4.2.1 *Pagina di login*

Figura 2: Pagina di login

É stata creata questa nuova pagina di login in HTML con degli script in JavaScript pensata con l'obbiettivo di fare da riferimento per le istruzioni su come procedere col nuovo sistema e su come risolvere gli evenutali problemi che si verranno a creare.

Figura 3: Blocco *shib_emergency*

4.2.2 *Blocco shib_emergency*

Il blocco *shib_emergency* è stato ideato con l'obbiettivo di fornire agli amministratori della piattaforma Moodle su cui si vuole aggiungere il metodo di autenticazione SSO degli strumenti che consentono agilmente tramite dei file *.csv* di configurare il filtro di accesso e di abilitare degli utenti esterni.

4.2.3 *Blocco shib_login*

Figura 4: Blocco *shib_login*

Il nuovo blocco di login che va a sostituire quello presente in Moodle è *shib_login*. Si è cercato di renderlo molto visibile per attirare l'attenzione sul nuovo sistema SSO. Esso ha 2 collegamenti, uno ad una pagina di documentazione contenente delle informazioni utili agli utenti e l'altro collegamento rimanda alla pagina di login del SSO.

4.2.4 *Pagina ./auth/shiboleth/index.php*

É stata effettuata una modifica alla pagina del *index.php*, modulo di moodle *Auth/Shibboleth*, che intercettando i dati provenienti dalla SAML li incrocia con i dati presenti nel database di Moodle. In questo modo si è risolto il problema di far combaciare i vecchi utenti con campi e domini degli identificatori differenti da quegli scelti per la SAML. Il pezzo di codice che segue infatti per prima cosa controlla se esiste nel database un utente con la matricola ricevuta dalla SAML, se si ne aggiorna i campi perché si ritiengono sempre più attuali i dati che provengono da Shibboleth. Altrimenti viene creato un nuovo utente sempre utilizzando i dati della SAML.

Codice 1: Modifica alla pagina *./auth/shiboleth/index.php*

```
/**************************************/
/*Modifica Michele Marostica 13.04.2010*/
/**************************************/

//Controllo incrociato dei dati provenienti dalla SAML
//con quelli presenti nel database di Moodle.
//Se e' presente gli aggiorno i dati, visto che sono da
    ritenere
//piu' aggiornati quelli della SAML.
$email  = $_SERVER['HTTP_SHIB_INETORGPERSON_MAIL'];
if(strlen($email)==0)
        $email = $_SERVER['SHIB_INETORGPERSON_MAIL'];
$matricola = $_SERVER['HTTP_SHIB_CAREER_IDNUMBER'];
if(strlen($matricola)==0)
        $matricola = $_SERVER['SHIB_CAREER_IDNUMBER'];

//Controllo se l'utente e' gia' presente nel database con il
    campo matricola
//Che in moodle e' utilizzato come identificatore.

if (count_records('user','idnumber',$matricola)>0){
        //se e' gia' stato sistemato non faccio nulla!
        if (get_field('user','auth','idnumber',$matricola) !=
             'shibboleth'){
                //ottengo l'id dell'utente
                $userid = get_field('user','id','idnumber',
                    $matricola);
                //aggiorno i campi: mail (cosi poi non crea
                    piu' il nuovo utente), auth in shibboleth
                set_field('user','email',$email,'id',$userid)
                    ;
                set_field('user','auth','shibboleth','id',
                    $userid);
                //cambio anche l'username perche' non so dove
                     poi mi controlla questo :(
                $predominio = explode("@",$email);
```

```
        $dominio = $predominio[1];
        $predominio =  $predominio[0];
        $username = $predominio;
        if ($dominio === "studenti.unipd.it"){
                $username .= "_studenti@unipd.it";
        }else{
                $username .= "@".$dominio;
        }
                set_field('user','username',$username,'id',
                    $userid);
        }
}
/*************************************/
/*Fine Modifica Michele Marostica      */
/*************************************/
```

5 INSTALLAZIONE DEL MODULO DI SSO

In questa sezione vengono descritti dettagliatamente i passaggi da eseguire per dare a Moodle il metodo di SSO (I file necessari sono contenuti in un file compresso).

1. Blocco *shib_emergency*
2. Blocco *shib_login*
3. Pagina di login modificata
4. Pagina di autenticazione modifcata
5. Modifica messaggi d'errore
6. Insieme di parametri da impostare manualmente
7. Configurazione del metodo di autenticazione
8. Caricamento del filtro tramite CSV

5.1 ALBERO DEL PACCHETTO DI INSTALLAZIONE

Questo è l'albero delle cartelle e dei file contenuti nel file compresso che è stato creato per l'installazione del SSO in Moodle.
./Blocchi/shib_emergency
./Blocchi/shib_login
./Pagina di login/index_form.html
./Pagina autenticazione/index.php
./Messaggi d'errore/messaggi.txt

5.2 INSTALLAZIONE BLOCCHI

Per prima cosa vanno aggiunti a Moodle i due blocchi che si trovano all'interno della cartella *./Blocchi/* del file compresso copiandoli all'interno della cartella *./Blocks/* di Moodle. Per installarli basterà accedere a Moodle come amministratore e aprire la pagina delle notifiche.

5.3 SOSTITUZIONE PAGINA DI LOGIN

Va sostituita la pagina originale di login con quella modificata che è nella cartella *./pagina login/* del file compresso e va messa nella cartella *./Login/* di Moodle assicurandosi di sostituire quella

presente, rinomimandola quindi in *index_form.html*, è cosa utile rinominare la pagina vecchia *index_form.html.bak* per tenerla come eventuale backup in caso di problemi.

5.4 SOSTITUZIONE PAGINA DI AUTENTICAZIONE

Va sostituita la pagina index.php originale del metodo di autenticazione Shibboleth con quella modifcata che è presente nella cartella *./pagina autenticazione/* del file compresso e va messa nella cartella *./Auth/shibboleth* di Moodle assicurandosi di sostituire quella originale, va scelto a seconda del caso se utilizzare la pagina che controlla gli utenti in base alla matricola o in base all'indirizzo email; se viene effettuata la scelta sbagliata verrà creato un nuovo utente al primo accesso.

5.5 MODIFICA AI MESSAGGI D'ERRORE

Va editato il file *./Lang/it_utf8/auth.php* di Moodle si devono sostituire i 2 messaggi di errore *shib_no_attributes_error* e *shib_not_all_attributes_error* con i seguenti:

Codice 2: Modifiche ai messaggi d'errore

```
$string['shib_no_attributes_error'] = 'Gentili utenti,<br/>A
    causa di un problema tecnico, attualmente la piattaforma
    Moodle non &egrave; accedibile tramite il <b>Single Sign
    On</b>. In particolare siete state riconosciuti dal
    sistema, ma non pervengono a Moodle informazioni
    sufficienti per autenticarvi correttamente. Si prega di
    contattare il gestore della piattaforma tramite il modulo
     di aiuto, e segnalare quest&rsquo;errore. <br/><br/>In
    questo momento &egrave; possibile accedere alla
    piattaforma utilizzando il sistema <u>alternativo</u> di
    login, qualora si sia gi&agrave; acceduti in precedenza
    con il SSO. Ritornare alla pagina di Login della
    piattaforma e NON cliccare sul logo SSO. Cliccare invece
    sul pulsante &quot;Pagina di Login Senza Single Sign On&
    quot;, in basso a destra. Il logo SSO scompare e al suo
    posto appare un Form di Login. Nei campi Username e
    Password inserire i dati Single Sign On completi come:<br
    /><center>marco.bianchi.17@studenti.unipd.it<br/></center
    > e la password SSO. Verrete autenticati tramite un
    sistema di backup del SSO.<br/>Cordiali saluti,<br/>
    StaffSSD<br/><br/>Informazioni sull&rsquo;errore: non
    vengono inviati gli attributi $a';

$string['shib_not_all_attributes_error'] = 'Gentili utenti,<
    br/>A causa di un problema tecnico, attualmente la
    piattaforma Moodle non &egrave; accedibile tramite il <b>
    Single Sign On</b>. In particolare siete state
    riconosciuti dal sistema, ma non pervengono a Moodle
```

```
tutte le informazioni disponibili su di voi per
autenticarvi correttamente. Si prega di contattare il
gestore della piattaforma tramite il modulo di aiuto, e
segnalare quest&rsquo;errore. <br/><br/>In questo momento
 &egrave; possibile accedere alla piattaforma utilizzando
 il sistema <u>alternativo</u> di login, qualora si sia
gi&agrave; acceduti in precedenza con il SSO. Ritornare
alla pagina di Login della piattaforma e NON cliccare sul
 logo SSO. Cliccare invece sul pulsante &quot;Pagina di
Login Senza Single Sign On&quot;, in basso a destra. Il
logo SSO scompare e al suo posto appare un Form di Login.
 Nei campi Username e Password inserire i dati Single
Sign On completi come:<br/><center>marco.bianchi.17
@studenti.unipd.it<br/></center> e la password SSO.
Verrete autenticati tramite un sistema di backup del SSO
.<br/>Cordiali saluti,<br/>StaffSSD<br/><br/>Informazioni
 sull&rsquo;errore: Attributi Mancanti  $a';
```

5.6 INSERIMENTO PARAMETRI MANUALI

Figura 5: Campi personalizzati

Per aggiungere i parametri andare da utente amministratore nel pannello a sinistra su *Utenti->Profili->Campi personalizzati* e aggiungere i seguenti campi:

1. Corso di Laurea
    - Tipo: riga di testo
    - Nome breve: cdl
    - Nome: Corso di Laurea
    - Campo bloccato: SI
    - Numero caratteri visualizzati: 60
    - Numero massimo caratteri: 255
2. Matricola
    - Tipo: riga di testo

- Nome breve: matricola
- Nome: Matricola
- Campo bloccato: SI
- Numero caratteri visualizzati: 10
- Numero massimo caratteri: 10

3. Facoltà
   - Tipo: riga di testo
   - Nome breve: facolta
   - Nome: Facoltà
   - Campo bloccato: SI
   - Numero caratteri visualizzati: 60
   - Numero massimo caratteri: 255
4. Anno Accademico Pagamento Tasse
   - Tipo: riga di testo
   - Nome breve: tax
   - Nome: Anno Accademico Pagamento Tasse
   - Campo bloccato: SI
   - Numero caratteri visualizzati: 10
   - Numero massimo caratteri: 10
5. Codice Del Corso di Laurea
   - Tipo: riga di testo
   - Nome breve: codcorso
   - Nome: Codice Del Corso di Laurea
   - Campo bloccato: SI
   - Numero caratteri visualizzati: 10
   - Numero massimo caratteri: 10

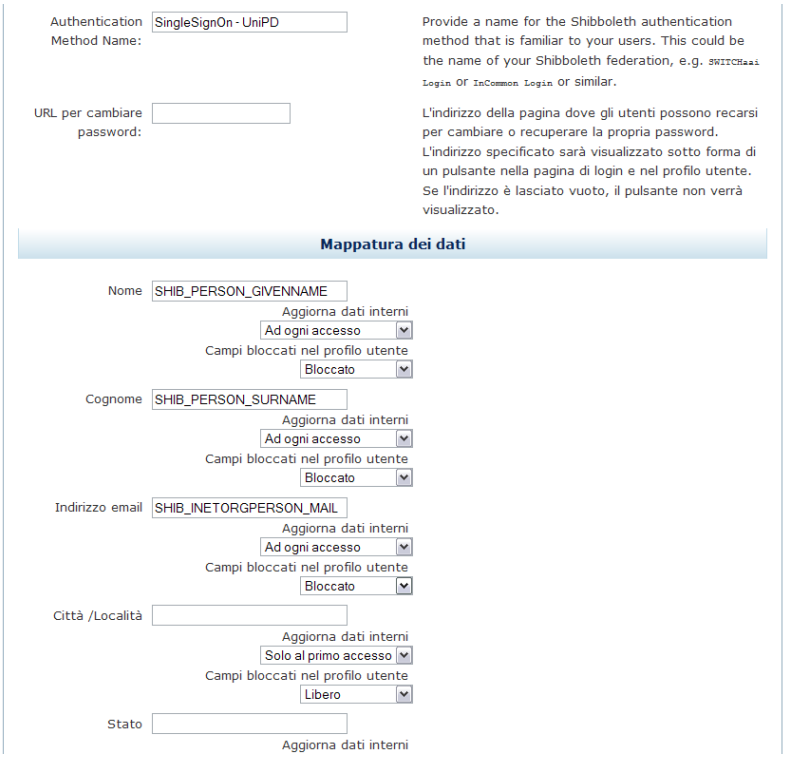
5.7 CONFIGURAZIONE DEL METODO DI AUTENTICAZIONE SHIBBOLETH

Qui viene spiegato come configurare Moodle in modo che riconosca l'asserzione SAML che gli invia Shibboleth, sempre dal pannello di amministrazione a sinistra bisogna configurare il metodo di autenticazione, seguono i parametri da configurare:

1. User id: SHIB_INETORGPERSON_USERID
2. API per la modifica: percorso tipo `/free/elearning/moodlewww/TUO_MOODLE/blocks/shib_emergency/elaborate_sso_parameters.php`

3. Authentication Method Name: SingleSignOn - UniPD
4. Nome: SHIB_PERSON_GIVENNAME -> ad ogni accesso, bloccato
5. Cognome: SHIB_PERSON_SURNAME -> ad ogni accesso, bloccato
6. Email: SHIB_INETORGPERSON_MAIL -> ad ogni accesso, bloccato
7. Matricola o IDNumber: SHIB_CAREER_IDNUMBER -> ad ogni accesso, bloccato
8. Corso di Laurea o Istitution: SHIB_CAREER_COURSE -> ad ogni accesso, bloccato

Figura 6: Configurazione SSO



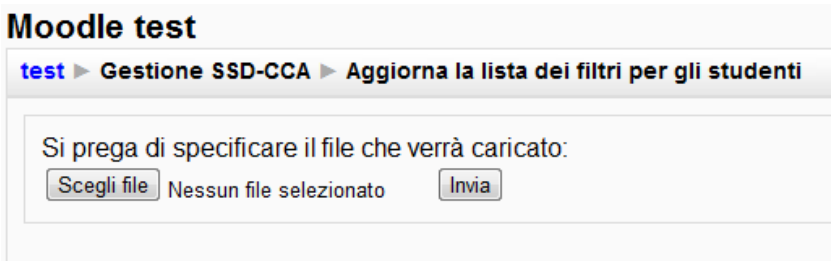
5.8 CARICAMENTO DEL FILTRO TRAMITE CSV

Scrivere metodo di caricamento dei dati del filtro Dal blocco *shib_emergency* si devono caricare i dati che andranno a configurare il filtro di selezione degli utenti che richiedono l'autorizzazione per accedere alle risorse di Moodle. In particolare vanno selezionati gli utenti in base al loro corso di laurea.

Figura 7: Blocco *shib_emegency*

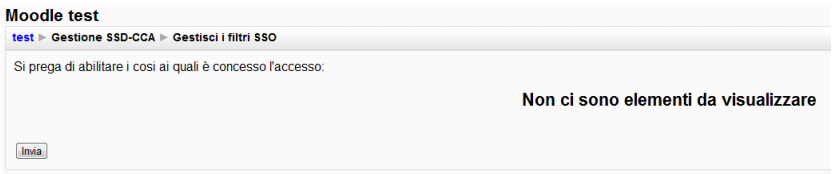
Cliccando sul collegamento *Aggiorna la lista dei filtri per gli studenti* si apre questa pagina: Va caricato il file *.csv* contenente i dati

Figura 8: Carica filtro SSO



dei corsi di laurea. Poi si deve tornare al blocco *shib_emergency* e cliccare sul collegamento *Gestisci i filtri SSO*.

Figura 9: Gestione filtri SSO



Qui se è stato caricato in precedenza un file *.csv* con i dati viene visualizzata una lista di corsi di laurea con un pulsantino per abilitarli o disabilitarli.
Dal blocco *shib_emergency* è possibile anche abilitare un singolo utente che non appartiene ad uno dei corsi di laurea consentiti tramite il collegamento *Abilitazione utenti esterni*

Figura 10: Abilitazione utenti esterni

6 SEQUENZA DI ACCESSO

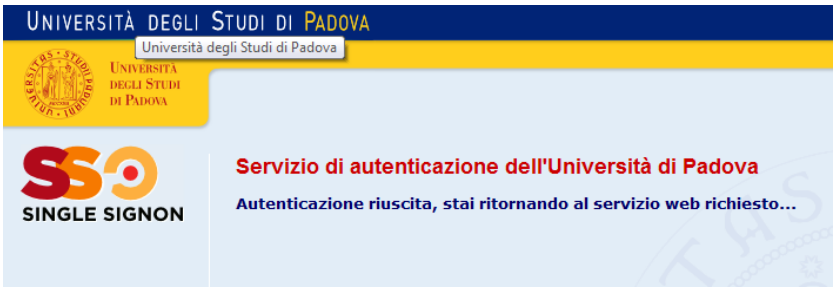
La sequenza di accesso decisa prevede un blocco come quello in figura che tramite la pressione del pulsante *Login* venga aperta la pagina informativa sul nuovo servizio.

Figura 11: Blocco *shib_login*

Figura 12: Pagina di login

Questa pagina contiene tutte le informazioni necessarie agli utenti per poter accedere al servizio e il pulsante che una volta premuto attiva la richiesta al Service Provider di Shibboleth di verificare se è già presente una sessione aperta da parte del browser del cliente, se esiste viene da parte sua inviata l'asserzione SAML con le credenziali dell'utente.

Figura 13: Pagina di reindirizzamendo



Nel caso in cui non fosse attiva una sessione, si viene reindirizzati alla pagina di accesso comune a tutti i servizi dell'ateneo dotati di SSO, la quale autentica l'utente creando una sessione nel server Shibboleth.

Figura 14: Pagina di login a Shibboleth

Per terminare la sessione, o in altri termini scollegarsi, è necessario chiudere il browser web con il quale ci si è collegati.

7 CONCLUSIONE

Il progetto è stato portato a termine rispettando tutti i requisiti (sicurezza, trasparenza e migrazione dei dati) e completando tutti gli obbiettivi. Sono state effettuate molte ore di test che hanno permesso di risolvere qualche piccolo bug e di ottenere un pacchetto completo e pronto all'uso. Tale pacchetto infatti è già stato adottato con successo dalla piattaforma moodle del Dipartimento di Costruzione e Trasporti (DCT) di Ingegneria Civile [2]

BIBLIOGRAFIA

[1] Cineca. www.cineca.it.

[2] Moodle dipartimento costruzione e trasporti. elearning.unipd.it/moodle/dct.

[3] Dynamico8. http://gqs-online.it/download/PresentazioneDynamic08.pdf.

[4] Limesurvey. http://docs.limesurvey.org/English+Instructions+for+LimeSurvey.

[5] Mit-license. http://www.opensource.org/licenses/mit-license.

[6] Moodle. www.moodle.org.

[7] Questionmarkperception. http://www.questionmark.com/us/perception/.

[8] Shibboleth. http://shibboleth.internet2.edu/about.html.

[9] Uniweb, sistema informativo di ateneo. http://www.uniweb.unipd.it.

[10] Webdav. http://www.webdav.org/.

[11] General Purpose License. Gpl. http://www.gnu.org/copyleft/gpl.html.

[12] Security Assertion Markup Language. Saml. http://saml.xml.org/about-saml.

[13] Single Sign-On. Sso. http://www.opengroup.org/security/sso/.