MÒDUL D'AUTENTICACIÓ SAML2 PER A DOKUWIKI

Màster Universitari de Programari Lliure

Autor: Fernando Gil Gil

Consultor: Cándido Rodríguez Montes

Juny de 2013

Resum del projecte

En el projecte s'elabora un mòdul que permet l'autenticació federada de wikis amb un proveïdor d'identitat SAML 2.0

L'aplicació utilitzada per la gestió de les wikis és Dokuwiki i la llibreria utilitzada per aconseguir wikis federades en el protocol SAML 2.0 és simpleSAMLphp. El mòdul permet integrar Dokuwiki i simpleSAMLphp de manera que els usuaris no s'autentiquen en Dokuwiki sinò en el proveïdor d'identitat (IdP). El protocol SAML2 és un mètode d'autenticació Single Sign-On en què Dokuwiki demana autenticació al proveïdor d'identitat (IdP) mitjançant un proveïdor de servei (SP), que també està integrat en simpleSAMLphp.

El mòdul es prova en tres situacions:

I) El proveïdor d'identitat és extern, Feide OpenIdP
II) El proveïdor d'identitat és local i la font d'autenticació és estàtica
III) El proveïdor d'identitat és local i la font d'autenticació és un servidor OpenLDAP

Es defineixen els grups amb permisos ACL a Dokuwiki a partir dels atributs que té l'usuari en el proveïdor de servei (SP). S'han utilitzat els filtres Athentication Processing Filters per a definir grups personalitzats tals com el grup d'administradors de Dokuwiki, "admin".

En la situació III) es donen les indicacions per a construir un servidor OpenLDAP en què l'esquema de la seva base de dades inclogui l'objetClass eduPerson. A més , s'han utilitzat els filtres ldap:AttributeFromLDAP i ldap:AttributeAddUsersGroups per passar els grups jerarquitzats de l'usuari autenticat en el servidor LDAP al proveïdor de servei (SP) i, indirectament , a través del mòdul, a Dokuwiki.

També, es fa la prova del nou template inclòs a l'última versió estable de Dokuwiki, "Adora Belle", en dispositius mòbils.

Fernando Gil Gil

Mòdul d'Autenticació SAML2 per a Dokuwiki
Màster de programari lliure

Índex de continguts

1. Introducció

Dokuwiki és un programari per la gestió de webs col·laboratives de tipus wiki, escrit en llenguatge PHP i distribuït sota llicència GPL. Està orientat per a ser utilitzat per grups de desenvolupament, grups de treball i petites empreses. Entre les seves avantatges cal destacar el fet d'emmagatzemar la informació en fitxers de text pla, no requereix la utilització de bases de dades. El seu procediment de registre d'usuaris és obert , cosa que dóna lloc a l'enregistrament anònim i a la possible corrupció de la wiki. Això planteja la utilització de wikis Federades, que tenen les avantatges següents:

- No requereixen enregistraments
- Treballen amb Single Sing-On. Procediment d'autenticació que permet als usuaris accedir a diversos sistemes amb una única instància d'autenticació.
- L'autenticació del usuaris pot ser anònimament rastrejada per l'administrador de la wiki.
- Poden utilitzar atributs confiables per realitzar el control d'accés.

La llibreria que s'utilitzarà per aconseguir wikis Federades és SimpleSAMLphp. L'objectiu principal del projecte és la realització d'un mòdul escrit en PHP que permeti integrar Dokuwiki amb SimpleSAMLphp perquè els usuaris no s'autentiquen en Dokuwiki sinó en el Proveïdor d'identitat SAML 2 de la seva organització, indicant qui és l'usuari i quins són els seus atributs.

2. Objectius del projecte

Per poder assolir l'objectiu abans esment s'han d'haver assumit prèviament els següents objectius:

- Conèixer el disseny de l'arquitectura de Dokuwiki
- Conèixer l'estàndard SAML 2
- Conèixer el disseny de l'arquitectura de SimpleSAMLphp

3. Estudi de la viabilitat

3.1 Establiment de l'abast del sistema

Com s'ha enunciat prèviament l'objectiu estratègic del projecte és la implementació d'un mòdul SAML 2 en PHP per a Dokuwiki. A més, un cop el mòdul sigui desenvolupat es publicarà sota una llicència lliure compatible amb la llicència GPL, utilitzada a Dokuwiki i la llicencia LGPL, utilitzada a SimpleSAMLphp. Aquest fet té la implicació que l'abast del projecte estarà definit per les condicions de la llicència. En cas, que el mòdul es publiqués amb llicència GPL qualsevol usuari podria utilitzar-lo sense restriccions.

3.2 Estudi de la situació actual

Actualment existeix una component que integra Dokuwiki amb SimpleSAMLphp desenvolupada per Andreas Åkre Solberg, que permet autenticació federada amb SAML 2.0 o Shibboleth 1.3 IdP. Es tracta d'un plugin d'autenticació per a Dokuwiki que utilitza una instal·lació de simpleSAMLphp en el mateix servidor. El mòdul ha estat provat amb DokuWiki 20080505 i SimpleSAMLphp 1.6.2.

3.3 Definició de requeriments del sistema

Tant Dokuwiki com SimpleSAMLphp s'instal·laran en un ordinador amb el sistema operatiu GNU/Linux. Les distribucions utilitzades podran ser Ubuntu 12.04 o Debian Squeeze. Es requereix, també, el servidor Apache 2.0 i PHP 5. La IDE utilitzada per fer el desenvolupament serà Eclipse Indigo. S'utilitzarà com a eina de depuració l'extensió de Firefox, Firebug.

En relació als requeriments que ha de complir el mòdul cal destacar el següent:
L'autenticació d'usuaris a Dokuwiki ha de ser completament substituïda per l'autenticació en el Proveïdor d'identitat, utilitzant el format de dades SAML2.
També, es requereix que el mòdul sigui provat i estigui operatiu amb les últimes versions de Dokuwiki i SimpleSAMLphp.

3.4 Estudi de les alternatives de solució

SimpleSAMLphp és una biblioteca desenvolupada en PHP basada en el codi de Sun OpenSSO Extensions (també conegut como Lightbulb) que permet integrar fàcilment un servei en aquest llenguatge amb una estructura de gestió d'identitat que utilitzi SAML 2. El Proveïdor de Servei SAML 2 , que és comunica amb el User Agent (Dokuwiki) i el IdP (Proveïdor d'Identitat digital) per donar autenticació, està integrat en la llibreria SimpleSAMLphp. La figura 1 mostra l'esquema d'una infraestructura SAML 2.

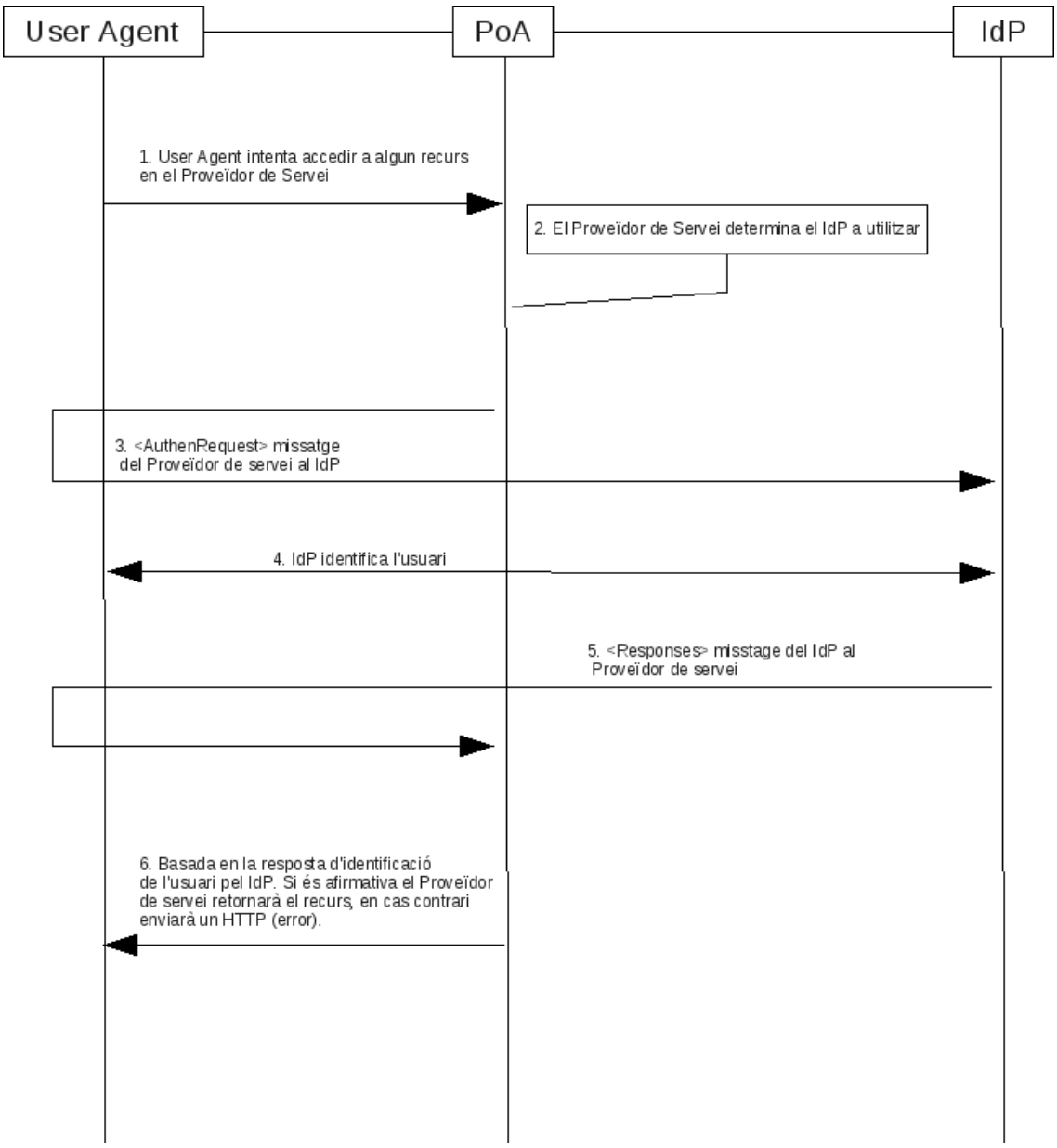

Figura 1

- User Agent: Aplicació que accedeix al sistema
- PoA: Punt d'Accés (Proveïdor de servei)
- IdP: Proveïdor d'Identitat

Una altra opció per aconseguir wikis federades amb Dokuwiki, consisteix en crear un mòdul d'autenticació per a Dokuwiki utilitzant la tecnologia PAPI, que també és un mètode d'autenticació Single Sing-On. L'arquitectura d'una infraestructura PAPI és més complexa que la d'una infraestructura SAML 2. La figura 2 mostra l'esquema:

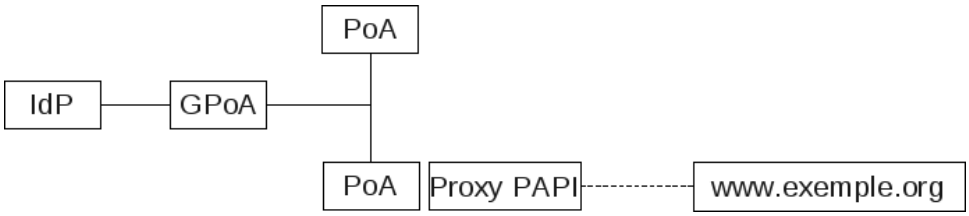

Figura 2

- IdD: Proveïdor d'Identitat. Autentica l'usuari en la seva organització i l'associa un conjunt d'atributs associats al resultat de l'autenticació.
- GpoA: Grup de Punts d'Accés. Component opcional de PAPI que permet agrupar diversos punts d'accés en un únic punt.
- PoA: Punt d'Accés (Proveïdor de servei), realitza l'autorització del servei protegit.
- Proxy PAPI: Funcionalitat opcional d'un PoA. Permet accedir remotament a un recurs web extern reescrivint les URLs de la pàgina original amb les pròpies del domini on s'ha desplegat. Això permet oferir als usuaris un accés distribuït i remot a recursos en què la autenticació es realitza per direcció IP.

Valoració de costos i anàlisi dels riscos

Donat que el requisit mínim de maquinari que es necessita és d'un ordinador amb connexió a Internet i que el programari que s'utilitza és lliure, el cost total del projecte estarà determinat pel nombre d'hores invertides. Segons el conveni signat amb l'empresa col·laboradora aquest nombre ha de ser de 185 hores. Per tant, si es fa l'estimació de 30€ / hora de treball, el cost total serà de 5550€.

El risc més significatiu per al projecte és la discontinuïtat d'algun dels projectes, simpleSAMLphp o Dokuwiki. També, cal mencionar que el desenvolupament del mòdul és fonamenta en la possibilitat que té Dokuwiki de poder escriure un “backend” per autenticar i, es suposa que en les properes versions es seguirà oferint-la.

Valoració de les alternatives

Des del punt de vista econòmic el projecte té el mateix cost tant si s'utilitza el protocol SAML2 com el protocol PAPI, però des del punt de vista dels riscos, cal tenir en consideració un altre rics tècnic en el cas del protocol PAPI: Les llibreries utilitzades per implementar aquest protocol estan incompletes. Per exemple, la llibreria phpPoA de RedIris que implementa PAPI no disposa actualment de servei de logout.

3.5 Selecció de la solució

S'ha escollit l'autenticació SAML2 perquè és una tecnologia què permet iniciar-se en els conceptes de Proveïdor d'Identitat digital, Infraestructures Federades i Autenticació Single Sing-On. Altres tecnologies d'autenticació com a PAPI tenen un nivell de complexitat més alt i requerixen estar familiaritzat amb els conceptes abans esmentats per dur a terme el desenvolupament d'un mòdul.

4. Anàlisi del sistema

4.1 Definició del sistema

Requisits exactes del mòdul

El mòdul d'autenticació SAML 2.0 per a Dokuwiki haurà de complir els següents requisits:

- Els usuaris seran autenticats mitjançant l'IdP (proveïdor d'identitat) utilitzant el format de dades SAML 2.0.
- El sistema SSO (Single Sing-On) d'autenticació d'usuaris SAML2 reemplaçarà al sistema d'autenticació de Dokuwiki.
- L'autenticació SSO mitjançant el protocol SAML 2.0 s'iniciarà des de l'SP (proveïdor de servei).
- Únicament les persones autoritzades podran accedir a la wiki amb permisos d'administració, edició o lectura segons els assignats als grups que pertanyen. Aquesta autorització consistirà en el fet que cadascuna d'aquestes persones tindrà un nom d'usuari i una contrasenya que la identificaran unívocament en l'IdP, el qual l'assignarà uns atributs.
- El mòdul permetrà la generació de grups d'usuaris construïts mitjançant els atributs dels usuaris.
- El mòdul permetrà la creació de grups personalitzats, entre els quals s'inclourà el grup 'admin' d'administradors de Dokuwiki
- Els permisos d'accés ACL dels grups d'usuaris de Dokuwiki seran establerts per un usuari del grup 'admin'.
- El mòdul haurà de ser funcional tant si l'IdP és remot com si s'allotja junt amb l'SP (proveïdor de servei) en el mateix servidor.
- El mòdul haurà de ser operatiu amb les darreres versions de simpleSAMLphp i Dokuwiki.
- L'edició de wikis mitjançant Dokuwiki i l'autenticació d'usuaris s'haurà de poder realitzar mitjançant les versions dels navegadors Microsoft Internet Explorer (versió 7.0 o posterior), Mozilla Firefox (versió 1.0 o posterior) i Google Crome (versió 23.0.1271.95 m o posterior).
- La llicència d'ús del mòdul haurà de ser tan poc restrictiva com sigui possible: en concret serà la GNU General Public License que s'utilitza en Dokuwiki i és compatible amb la llicència LGPL utilitzada a SimpleSAMLphp.

- La llicència d'ús del sistema operatiu del servidor web serà la corresponent a GNU/Linux; és a dir, GNU General Public License.

Entorn tecnològic del sistema

L'entorn tecnològic del sistema web serà el següent:

- Sistema operatiu: GNU/Linux (distribució Ubuntu 12.04)
- Servidor web Apache (versió 2.2.22)
- Llenguatge de programació per al desenvolupament web PHP (versió 5.3.10-1ubuntu3.4)
- Dokuwiki (versió 2012-10-13)
- Proveïdor de servei (SP): simpleSAMLphp (versió 1.10.0)
- Proveïdor remot d'identitat SAML 2.0 (IdP): Feide OpenIdP
- Proveïdor local d'identitat (IdP) construït amb simpleSAMLphp
- S'utilitzarà l'estàndard definit per OASIS per a l'intercanvi de dades d'autenticació i autorització entre dominis SAML 2.0 (Security Assertion Markup Language 2.0)

Normes que es poden seguir en el sistema

- El mòdul es dissenyarà prenent com a punt de partida la documentació inclosa a Dokuwiki sobre autenticació "backend" i les normes fixades a l'estàndard SAML 2.0, entorn basat en XML per a serveis Web que permet l'intercanvi d'informació d'autorització i autenticació entre diferents llocs Web.

Identificació d'usuaris

- Els usuaris potencials del mòdul són les persones u organitzacions que estiguin interessats en utilitzar Dokuwiki com a eina per a editar wikis de forma segura.

4.2 Establiment de requeriments

Cal destacar els següents requeriments funcionals que fan referència a l'autenticació dels usuaris:

- Els usuaris autenticats per l'IdP obriran sessió a Dokuwiki i tindran accés als recursos en funció dels permisos ACL assignats als grups que pertanyin.

- Cap usuari no autenticat per l'IdP podrà obrir sessió a Dokuwiki
- Els usuaris tancaran sessió de forma correcta, de manera que un cop un usuari hagi realitzat el procediment “log off” no es podrà accedir als recursos de Dokuwiki sense autenticació.

Es distingeix el següent requeriment de rendiment:

- És minimitzarà el nombre de grups personalitzats. La majoria dels grups estaran definits a partir dels atributs dels usuaris assignats per l'IdP.

També cal mencionar els següents requeriments de seguretat:

- Cal prioritzar la utilització del protocol HTTPS amb el servidor Web.
- La instal·lació i configuració de Dokuwiki i simpleSAMLphp, així com la configuració de l'SP i la integració de Dokuwiki amb simpleSAMLphp la portarà a terme l'administrador del sistema, que serà membre del grup 'admin'.

Entre els requeriments d'implantació es distingeix el següent:

- Dokuwiki i simpleSAMLphp estaran instal·lats a l'ordinador on s'allotgi el servidor Web.

4.3 Definició d'interfícies d'usuari

Es distingeixen els usuaris que pertanyen al grup 'admin', els quals tenen privilegis per assignar permisos ACL als grups i als altres usuaris de la Wiki.

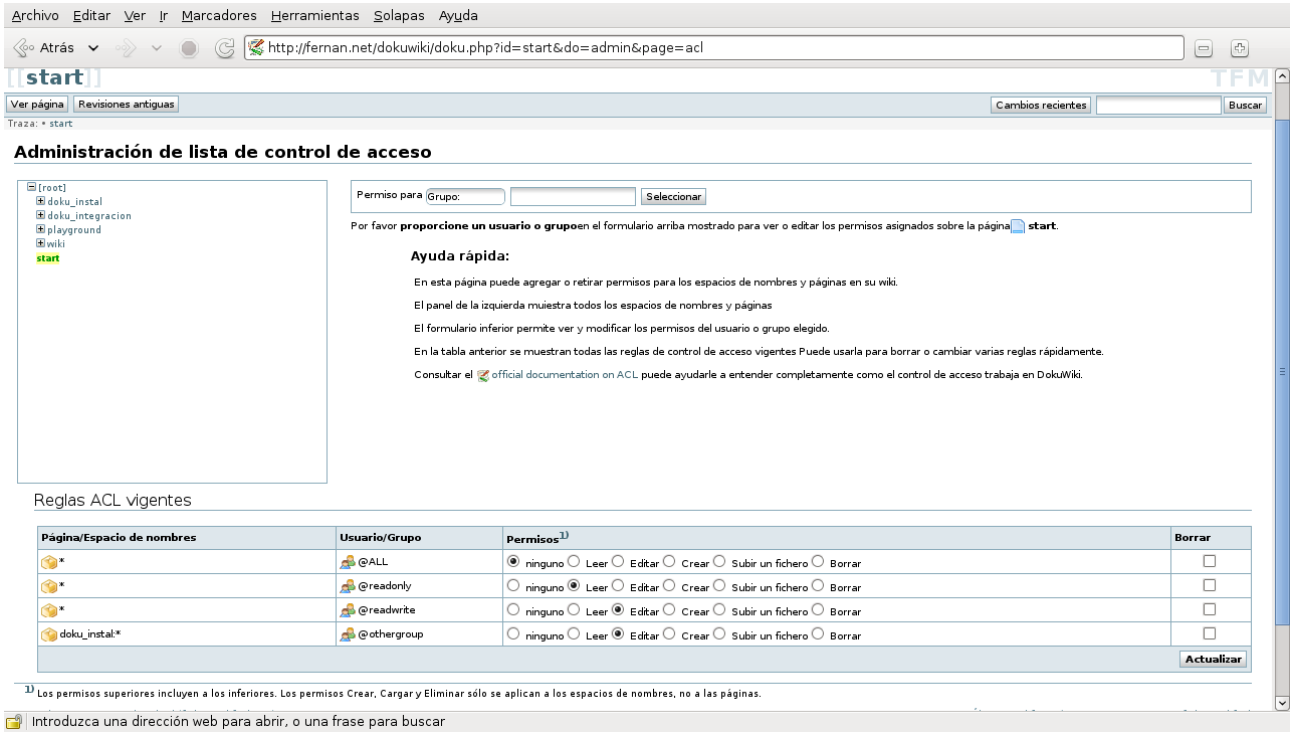

Figura 3

Tal com es mostra a la "*Figura 3*" els permisos ACL poden ser: "Esborrar fitxers", "Afegir fitxers", "Crear", "Editar", "Llegir" i "Cap". Aquests permisos estan jerarquitzats segons l'ordre anterior, de manera que un usuari que té el permís "Crear" també té els permisos "Editar" i "Llegir". Aquests permisos poden ser vàlids per a una sola pàgina o bé per a totes les pàgines que pengen d'un node (anomenat namespace) de la Wiki. A més, els usuaris del grup 'admin' tenen tots els permisos.

Un usuari singular del grup 'admin' és l'administrador del sistema, que podrà definir grups en

funció dels atributs dels usuaris assignats per l'IdP. El procediment es basa en la utilització de 'Authentication Processes Filters' inclòs en simpleSAMLphp des de la versió 1.5. Aquests filtres consisteixen en un conjunt de classes que permeten fer canvis en els atributs de l'usuari un cop l'usuari ha sigut autenticat per l'IdP i abans que aquest doni la resposta a l'SP. El perfil de l'administrador és tècnic, cal que tingui coneixements de desenvolupament web, concretament, ha de conèixer el llenguatge PHP.

La resta d'usuaris només tindran accés a les pàgines de la Wiki per modificar-les o llegir-les.

No cal implementar un nou interfície d'usuari. Si l'IdP és remot es mostrarà a l'usuari un formulari propi per accedir a Dowukiki i, en cas que l'IdP sigui local, simpleSAMLphp ja té inclòs un formulari al qual es pot afegir una imatge que el personalitzi.

4.4 Especificació del pla de proves

Es realitzaran les proves necessàries per cobrir tots els casos possibles d'autenticació:

1. Usuari registrat en l'IdP associat a l'SP intenta obrir sessió en Dokuwiki
   La resposta esperada és que pugi autenticar-se en l'IdP, mitjançant un formulari i accedeixi a la Wiki amb els permisos assignats als grups que pertanyi.
   Aquesta prova s'ha de realitzar amb usuaris de tots els grups definits.

2. Usuari no registrat en l'IdP associat al SP intenta obrir sessió en Dokuwiki
   La resposta esperada és que es mostri un formulari per autenticar-se en l'IdP, però no pugi accedir a Dokuwiki després d'introduir nom d'usuari i contrasenya .

3. Usuari tanca sessió en Dokuwiki
   La resposta esperada és que no es pugi accedir a Dokuwiki sense tornar a autenticar-se en l'IdP.

Les proves 1, 2 i 3 s'han de realitzar amb un IdP remot, com per exemple: Feide OpenIdP, i amb un IdP local construït amb simpleSAMLphp.

També cal realitzar les proves 1, 2 i 3 des d'un ordinador de la xarxa local amb sistema operatiu Windows per comprovar el bon funcionament amb els navegadors Explorer i Google Crome.

5.Disseny

5.1 Arquitectura

L'arquitectura bàsica del sistema es mostra a l'esquema de la figura 4:

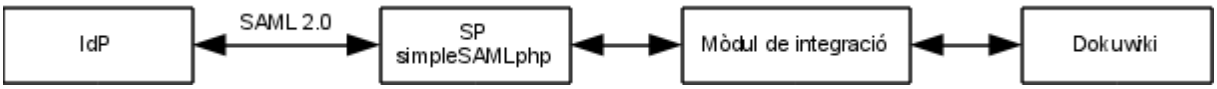

Figura 4

El mòdul de integració és un plugin de Dokuwiki que es defineix com una classe que estén la classe d'autenticació de Dokuwiki “auth_basic” i utilitza l'API “SimpleSAML_Auth_Simple” del SP simpleSAMLphp.

a) El perfil Single Sing-ON (SSO) utilitzat en l'intercanvi de dades SAML 2 és “SSO iniciat des de SP amb Redirecció i POST Bindings” que es descriu en la figura 5.

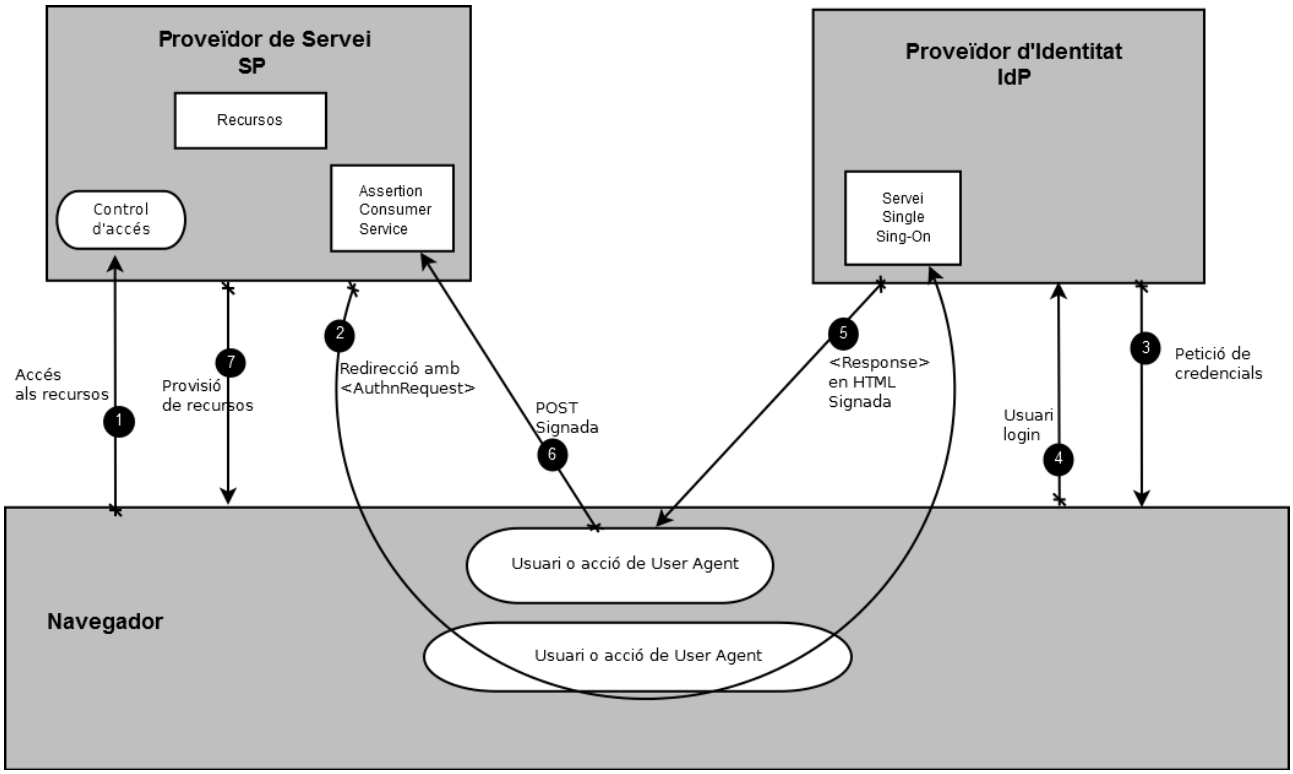

Figura 5

1. L'usuari intenta accedir a un recurs en l'SP. L'SP desa el recurs URL demanat localment.
2. L'SP envia una HTTP resposta de redirecció al navegador (HTTP status 302 o 303). La capçalera HTTP conté la destinació URL del servei Single Sing-On en l'IdP junt amb un missatge <AuthnRequest> codificat com una URL query variable anomenada SAMLRequest. El query string és codificat utilitzant la codificació DEFLATE. El navegador processa la resposta de redirecció i estableix una petició HTTP GET al servei Single Sing-On de l'IdP amb el query paràmetre de SAMLRequest. També s'inclou informació local d'estat en la resposta HTTP codificada en un RelayState query string paràmetre.
3. El servei Single Sing-On determina si l'usuari té a l'IdP un context de seguretat d'inici de sessió a partir de <AuthnRequest>. En cas contrari, interactua amb el navegador i fa una petició de credencials vàlides a l'usuari.
4. L'usuari proporciona credencials vàlides i es crea per l'usuari un context local de seguretat d'inici de sessió.
5. El servei Single Sing-On de l'IdP crea una afirmació SAML representant el context de seguretat d'inici de sessió de l'usuari. Donat que s'utilitzarà POST binding l'afirmació és digitalment signada i col·locada dins d'un missatge SAML <Response> . El missatge <Response> és aleshores col·locat dins d'una HTML FORM com a un formulari de control anomenat SAMLResponse . Si l'IdP rep un valor RelayState de l'SP, haurà de retornar-lo sense modificar-lo a l'SP en un formulari ocult de control anomenat RelayState. Usualment la HTML FORM va acompanyada d'un script que automàticament enviarà el formulari al lloc de destinació.
6. El navegador per acció de l'usuari o de la execució d'un “auto-submit” script emet una petició HTTP POST per enviar el formulari al ”Assertion Consumer Service” de l'SP. El ”Assertion Consumer Service” del proveïdor de servei obté el missatge <Response> des de la HTML FORM per processar-lo. Primer és valida la firma digital en l'afirmació SAML i, després, es processa el contingut de l'afirmació SAML per a crear un context de seguretat d'inici de sessió per a l'usuari en l'SP. Un cop completat el procés l'SP recupera la informació local d'estat indicada per la data del RelayState per demanar el recurs URL originalment requerit. Aleshores, envia una resposta HTTP amb redirecció al navegador dirigint-lo per accedir al recurs originalment demanat.

7. Es realitza un control d'accés per saber si l'usuari té l'autorització per accedir al recurs. Si es passa el control d'accés, el recurs és aleshores retornat al navegador.

b) Disseny del mòdul d'autenticació

El mòdul s'ubicarà al directori /inc/auth de Dokuwiki i l'arxiu s'anomenarà simplesamlphp.class.php. La classe serà una extensió de la classe auth_basic de Dokuwiki definida en /inc/auth/basic.class.php. Tindrà la següent declaració:

class auth_simplesamlphp extends auth_basic {...}

S'hauran d'omplir els camps següents:

$success
És una variable booleana que s'ha de fixar *true* en el constructor si el mòdul d'autenticació s'inicia correctament. S'utilitzarà per notificar al frontend si es produeix algun error posant-hi *false*

$cando
Aquest camp és una matriu associativa de booleans. S'han de fixar tots els camps a *true* per a totes les funcions que proporcioni el nostre backend. En el nostre cas seran:

external : Fa que el mòdul tingui un control extern d'autenticació
logoff : Fa que el mòdul tingui un mètode especial de logoff

Per tant, el constructor tindrà el codi següent:

```
function auth_simplesamlphp()
{
        this -> cando['external'] = true;
        this -> cando['logoff'] = true;
        this -> success = true;
}
```

trustExternal()

Aquesta funció s'utilitza per autenticar un usuari quan *cando['external']* és *true.* En aquest cas tots els altres mètodes d'autenticació interns de Dokuwiki no s'utilitzaran.

En aquesta funció es declararà *global* la matriu associativa *$USERINFO*. Aquesta variable contindrà informació de l'usuari que es passarà a Dokuwiki des del SP.

```
$USERINFO['name']       // Nom de l'usuari
$USERINFO['mail']       // Correu electrònic de l'usuari
$USERINFO['grps']       // Grups que pertany l'usuari
```

També cal considerar les següents variables globals que contindran informació sobre les dades d'autenticació de l'usuari.

```
$_SERVER['REMOTE_USER']                 //Atribut Id que identifica l'usuari
$_SESSION[DOKU_COOKIE]['auth']['user']  //Atribut Id que identifica l'usuari
$_SESSION[DOKU_COOKIE]['auth']['pass']  //Contrasenya de l'usuari
```

La darrera línia de la funció donarà contingut a la següent variable global
$_SESSION[DOKU_COOKIE]['auth']['info'] = $USERINFO

També s'inclourà la variable gobal *$conf* que és una matriu associativa amb claus i valors que estan definits al fitxer de configuració /conf/local.php de Dokuwiki.

És farà una crida a l'API del SP de simpleSAMLphp anomenat *SimpleSAML_Auth_Simple* per obtenir els atributs de l'usuari des del proveïdor de servei.
El mètodes que conté l'API *SimpleSAML_Auth_Simple* són el següents:

- *Constructor*

  Exemple: *$as = new SimpleSAML_Auth_Simple('default-sp');*

- *isAuthenticated*

  Testeja si l'usuari és autenticat. Retorna *true* si està autenticat i *false* en cas contrari.

- *requireAuth*

  Aquesta funció assegura que l'usuari esta autenticat. Només retorna si l'usuari està autenticat. En cas que l'usuari no estigués autenticat començarà el procés d'autenticació.

  Exemple: *$as -> requireAuth();*

- *logout*

  Tanca la sessió de l'usuari i retorna a l'URL donada.

  Exemple: *$as->logout('https://sp.example.org/');*

- *getAttributes*

  Recupera els atributs de l'usuari actual. Si l'usuari no està autenticat es retorna una matriu buida. Els atributs es retornen com una matriu associativa amb el nom de l'atribut com la clau i el valor com una matriu d'un o més strings.

- *getLoginURL*

  Recupera l'URL que va ser utilitzada a l'inici de l'autenticació.

  Exemple: $url = $as->getLoginURL();

- *getLogoutURL*

Recupera l'URL que va ser utilitzada al iniciar el logout.

Exemple: $url = $as->getLogoutURL();

c) Generació de grups

Per generar grups a partir dels atributs dels usuaris utilitzarem els filtres de "Authentication Processes Filters" de simpleSAMLphp. Concretament utilitzarem les classes *core:GenerateGroups* i *core:AttributeAdd.*

El codi per definir grups s'ha d'incloure al fitxer config.php de simpleSAMLphp

- *core:GenerateGroups*

Per defecte aquest filtre generarà grups des dels següents atributs: *eduPersonAffiliation* , *eduPersonOrgUnitDN* i *eduPersonEntitlement*

Intentarà determinar un domini al qual pertany l'usuari basant-se en l'atribut ID de l'usuari, si és present.

Els grups que genera aquest filtre són de la forma:

<*nom atribut*> - <*valor atribut*> i <nom atribut> - <domini> - <valor atribut>

Exemple de generació de grups amb l'atribute *eduPersonAffilitation* :

```
'authproc' => array(
    50 => array(
        'class' => 'core:GenerateGroups',
        'eduPersonAffiliation'
    ),
),
```

- *core:AttributeAdd*

Aquest filtre permet afegir atributs al conjunt d'atributs que serà processat. Si l'atribut ja existeix serà fusionat en un multi-valorat atribut. Si és vol reemplaçar en lloc de fusionar s'utilitzarà el

paràmetre '%replace'

Exemple on s'afegeix l'atribut multi-valorat *groups*

```
'authproc' => array(
    50 => array(
        'class' => 'core:AttributeAdd',
        'groups' => array('users', 'members')
    ),
),
```

5.2 Revisió dels casos d'ús

Des del proveïdor de servei (SP) és passaran al mòdul d'autenticació l'atribut groups i els atributs eduPersonPrincipalName, eduPersonAffiliation i eduPersonEntitlement de l'objectClass eduPerson, que tenen les característiques següents:

eduPersonPrincipalName

El valor d'aquest atribut es un string de la forma user@scope que identifica unívocament a l'usuari, on 'user' és l'identificador de l'usuari i 'scope' és el nom del domini. Només accepta un únic valor.

Per exemple: fgil2@fernando.org

eduPersonAffiliation

Aquest atribut especifica la relació de l'usuari amb la institució amb diferents categories tals com student, staff, teacher, member,.... És multi-valorat i els seus valors són strings. S'utilitzarà en el mòdul per definir grups.

Per exemple: staff, member

eduPersonEntitlement

És un atribut multi-valorat que accepta com a valors url's o urn's. S'utilitzarà en el mòdul per donar a l'usuari permisos administratius de la wiki. Concretament, és validaran en el mòdul urn del tipus:

urn:mace:scope:entitlement:wiki:valor

On scope és el nom del domini i valor un string que definirà un grup amb permisos específics.

Els administradors de la wiki, que pertanyen al grup admin, tindrán assignat la següent urn:

urn:mace:scope:entitlement:wiki:admin

El mòdul ha de ser operatiu en las situacions següents:

I) S'utilitza un proveïdor d'Identitat extern, com per exemple Feide OpenIdP.

   En aquest cas, els usuaris probablement no tindran assignat els atributs de la classe eduPerson. Per solucionar aquest problema s'utilitzaran els filtres core:AttributeAdd i coreAttributeAlter per crear-los i assignar directament valors a aquests atributs en el proveïdor de servei (SP).

II) S'utilitza un proveïdor d'identitat local construït amb simpleSAMLphp i una font d'autenticació estàtica.

   En aquest cas es donaran valors directament als atributs de la classe eduPerson. S'introduiran directament els usuaris en l'apartat 'example-userpass' del fitxer authsources.php de simpleSAMLphp.

III) S'utilitza un proveïdor d'identitat local construït amb simpleSAMLphp i com a font d'autenticació un servidor LDAP.

En aquest cas es crearà en una màquina virtual un servidor OpenLDAP i s'afegirà a la base de dades l'objectClass eduPerson. D'aquesta manera tots els usuaris tindran definits els atributs de la clase eduPerson. A més, mitjançant els filtres ldap:AttributeAddFromLDAP i ldap:AttributeAddUsersGroups , que apareixen en la versió 1.9 de simpleSAMLphp, es podran passar els grups que pertany l'usuari autenticat en el servidor LDAP al proveïdor de servei (SP), i indirectament, a través del mòdul, a Dokuwiki.

Dokuwiki incorpora des de la versió “Adora Belle” un template que permet visualitzar les wikis en dispositius mòbils. Donat que un dels requisits que ha de verificar el mòdul és que l'autenticació d'usuaris i la edició de wikis ha de ser factible amb Google Chrome caldrà, també, fer les proves en dispositius mòbils amb sistema operatiu Android. Per a realitzar-les s'utilitzarà l'Android Emulator que permet fer la simulació de dispositius mòbils Android en estacions de treball.

Principals components de la fase de desenvolupament

1) Estació de treball que inclou Dokuwiki i simpleSAMLphp

Component	**Paquet**	**Versió prevista**	**Llicència**
Sistema Operatiu	Ubuntu GNU/Linux	12.04	GPL
Servidor web	Apache	2.2.22	Apache Software License
Interpret d'scripts	PHP	5.3.10-1ubuntu3.6	GPL
Gestor de wikis	Dokuwiki	2012-10-13 “Adora Belle”	GPL
Framework d'autenticació	SimpleSAMLphp	1.10.0	LGPL
Entorn de desenvolupament (IDE)	Eclipse	3.7.2 “Indigo”	Eclipse Public License

2) Estació de treball amb el servidor LDAP

Component	**Paquet**	**Versió prevista**	**Llicència**
Sistema Operatiu	Debian GNU/Linux	Squeeze 6.07	Debian license
Programari de virtualització	Oracle VM VirtualBox	4.2.8 r83876	GPL v2
Sistema Operatiu de la màquina virtual	Ubuntu GNU/Linux	10.04	GPL
Servidor OpenLDAP	slapd	2.4.21-0ubuntu5.7	OpenLDAP Public License
Webfrontend per gestionar el directori LDAP	LDAP-Account Manager	2.9.0-1	GPL v2

3) Estació de treball amb Android Emulator

Component	**Paquet**	**Versió prevista**	**Llicència**
Sistema Operatiu	Microsoft Windows 7 Professional	6.1.7601 Service Pack 1	Microsoft
Dispositiu mòbil virtual	Android SDK	21.1.0	SDK license from Google

El mòdul tindrà llicència GPL que és compatible amb les llicències de les llibreries de PHP, Dokuwiki i simpleSAMLphp utilitzades en el desenvolupament.

Especificacions de desenvolupament i proves

S'utilitzarà l'entorn de desenvolupament Eclipse Indigo amb el plugin per PHP: “Aptana Studio 3 Plugin”.

El marc de treball de les proves és el mòdul PHP PEAR

La documentació de la instal·lació del mòdul estarà en format de text

S'utilitzaran ordinadors diferents, que estaran en xarxes locals diferents, per fer les proves en les situacions I) , II) i III)

En la situació I), en què l'IdP és Feide OpenIdP , la instal·lació de Dokuwiki i simpleSAMLphp es farà junt amb un servidor web anomenat “fernando.net”.
L'ordinador que s'utilitzarà té les característiques següents:

- Processador AMD Athlom(tm) II X2 250 Processor 3.0 Ghz
- Memòria (RAM) 4.0 Gb
- Partició de 200 Gb amb sistema operatiu Ubuntu 12.04

Té connexió ADSL a Internet mitjançant router de Telefònica.

En les situacions II) i III), on l'IdP és local, la instal·lació de Dokuwiki i simpleSAMLphp es farà junt amb un servidor web anomenat “fernan.net”.
L'ordinador que s'utilitzarà té les característiques següents:

- Processador Intel(R) Core(TM) 2 Duo CPU T7250 2.0 Ghz
- Memòria (RAM) 4.0 Gb
- Partició de 50 Gb amb sistema operatiu Ubuntu 12.04

Té connexió ADSL a Internet mitjançant un altre router de Telefònica i està en la mateixa xarxa local que les estacions de treball que contenen el servidor LDAP, anomenat “fernando.org”, i l'Android Emulator.

En totes les situacions es faran les proves de login i logout d'usuaris registrats i es comprovarà que Dokuwiki rep els grups assignats a l'usuari. També, es comprovarà que els usuaris no registrats no poden obrir sessió a Dokuwiki.

En la situació III) és comprovarà que l'SP rep correctament els DistinguishedName (DN) de tots

els grups que pertany l'usuari autenticat. També es comprovarà que es pot restringir la autorització al SP a un grup determinat d'usuaris definits al directori LDAP.

Es comprovarà que els usuaris s'autentiquen i que les wikis es visualitzen correctament en dispositius Android.

Requisits d'implantació

En un entorn de producció caldrà tenir un servidor web on s'instal·li Dokuwiki i simpleSAMLphp que tingui les característiques mínimes següents:

- Processador: Intel Core 2 Duo 2.0 Ghz
- Memòria (RAM): 4 Gb
- Sistema GNU/Linux instal·lat a una partició de 50 Gb

L'organització haurà de tenir un servidor LDAP que contingui tots els usuaris de la wiki, o bé, haurà de formar part d'una Federació, de manera que, els usuaris s'autentiquin en un IdP extern.

6. Desenvolupament

6.1 Planificació de les tasques

Es considera que el temps disponible per dedicar al projecte és de 3 hores per dia.

El projecte es descompon en les tasques següents:

Estudi de la viabilitat

Instal·lació i Configuració de Dokuwiki	6 hores (2 dies)
Instal·lació i Configuració de SimpleSAMLphp	9 hores (3 dies)
Prova del mòdul d'Andreas Åkre Solberg	15 hores (5 dies)

Anàlisi i disseny del sistema

Estudi del disseny de l'arquitectura de Dokuwiki	15 hores (5 dies)
Estudi de l'estàndard SAML 2	15 hores (5 dies)
Estudi del disseny de l'arquitectura de SimpleSAMLphp	15 hores (5 dies)

Desenvolupament i proves

Configurar l'SP per la situació I)	3 hores (1 dia)
Desenvolupar el mòdul	15 hores (5 dies)
Definir atribut eduPersonEntitlement a l'SP amb Auth Proc Filters	6 hores (2 dies)
Proves en la situació I)	6 hores (2 dies)
Configurar l'SP per la situació II)	9 hores (3 dies)
Proves per la situació II)	9 hores (3 dies)
Crear i provar el servidor OpenLDAP	15 hores (5 dies)
Configurar l'SP per la situació III)	3 hores (1 dia)
Definir filtre ldap:AttributeAddUsersGroups i proves situació III)	15 hores (5 dies)
Proves dispositius mòbils	6 hores (2 dies)

Documentació

Redacció de la memòria del projecte	33 hores (11 dies)

Diagrama de Gantt:

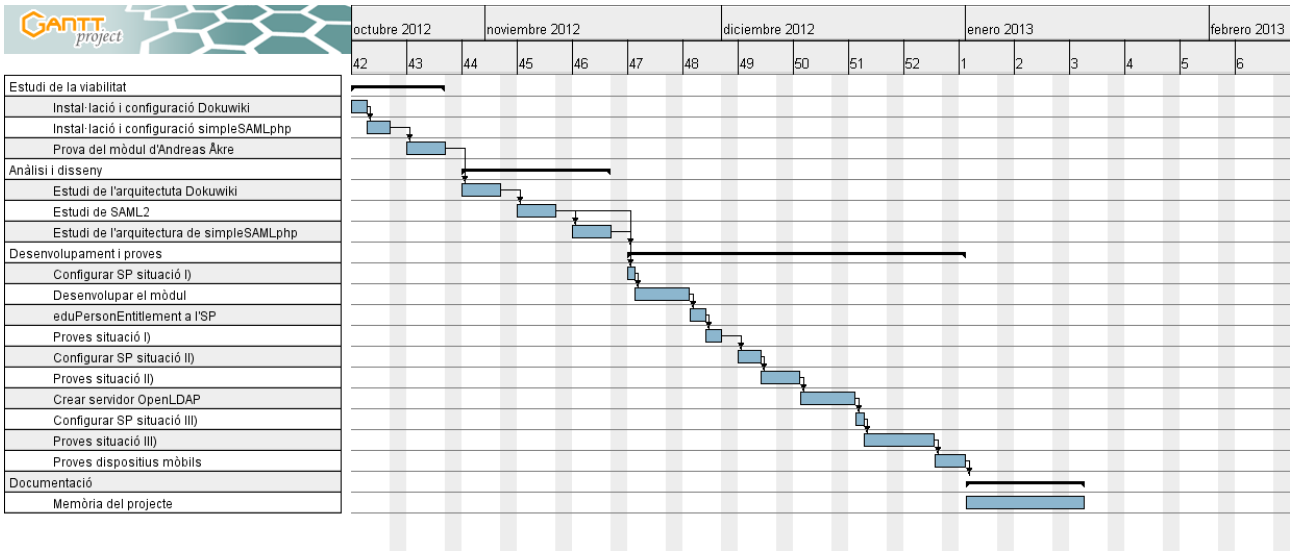

Figura 6

6.2 Desenvolupament

6.2.1 Configuració del Proveïdor de Servei (SP) per la situació I)

Faré la configuració en què el Proveïdor de Identitat (IdP) serà Feide OpenIdP

1) L'SP és configura per l'entrada al fitxer

config/authsources.php

La configuració mínima és

```
<?php
$config = array(

    /* This is the name of this authentication source, and will be used to access it later. */
    'default-sp' => array(
        'saml:SP',
    ),
);
```

2) Habilitar un certificat per l'SP

Creo un certificat al directori cert/

```
cd cert
openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out saml.crt -keyout saml.pem
```

Edito al fitxer authsources.php les entrades següents:

```
 'default-sp' => array(
    'saml:SP',
    'privatekey' => 'saml.pem',
    'certificate' => 'saml.crt',
),
```

3) IdP per defecte

Incloc per defecte Feide OpenIdP com a IdP , introduint les següents entrades a authsources.php

```
<?php
$config = array(

    'default-sp' => array(
        'saml:SP',
```

```
        /*
         * The entity ID of the IdP this should SP should contact.
         * Can be NULL/unset, in which case the user will be shown a list of available IdPs.
         */
        'idp' => 'https://openidp.feide.no',
    ),
);
```

4) Intercanvi de metadata amb l'IdP

Creo un compte a Feide OpenIdP Metadata Self-Service Registry

El metadata per a Feide OpenIdP està inclòs en el metadata distribuït amb simpleSAMLphp

Per connectar l'SP i Feide OpenIdp s'ha d'afegir el metadata per al SP a l'IDP. El metadata per al SP es troba a la pestanya Federation de la página d'instal·lació:

http://fernando.net/simplesaml

Copio el SAML 2.0 XML Metadata document automaticament generat per simpleSAMLphp i torno a Feide OpenIdP Metadata Self-Service Registry

M'autentico clicant l'enllaç “Managing Service Providers”. A continuació clico l'enllaç “Add from SAML 2.0XML metadata” i pego el meu SAML 2.0 XML Metadata. Els camps de text per a AssertionConsumerService i SingleLogoutService hauran de contenir dues URL's:

AssertionConsumerService
https://fernando.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

SingleLogoutService
https://fernando.net/simplesaml/module.php/saml/sp/saml2-logout.php/default-sp

Després de comprovar el metadata i completar el formulari clico save.

4) Provar l'SP

La pàgina d'instal·lació de simpleSAMLphp té un enllaç per provar les fonts d'autenticació. Quan es clica l'enllaç es rep una llista de fonts d'autenticació que inclou la creada per a l'SP.

Després de clicar l'enllaç es redirigeix cap a l'IdP. Un cop s'introdueixen les meves credencials es torna a redirigir cap a la pàgina de prova, on s'exposa una llista amb els meus atributs.

6.2.2 Desenvolupament del mòdul

El codi del mòdul és una modificació del mòdul d'Andreas Åkre Solberg. Es segueixen les pautes descrites en el disseny. A més, s'inclou la validació de l'atribut eduPersonEntitlement de l'usuari autenticat, assignant-li un nou grup de Dokuwiki. El valor urn d'aquest atribut ha de tenir el format:

urn:mace:nom_domini:entitlement:wiki:valor

S'han de tenir en compte les consideracions següents:

$domain = substr($groups[0], 6);

Aquesta línia permet assignar a la varible $domain el nom del domini perquè el primer grup passat des de l'SP a Dokuwiki és realm-nom_domini. Això esta justificat perquè el filtre core:GenerateGroups genera en primer lloc el grup:

realm-nom_domini

i després els grups:

eduPersonAffiliation-valor

eduPersonAffiliation-realm-valor

on valor correspon a cadascun dels valors de l'atribut eduPersonAffiliation. Donat que l'apartat 'authproc.sp' de config.php inclou la línia

60 => array('class' => 'core:GenerateGroups', 'eduPersonAffiliation'),

$pattern = '/^urn:mace:'.$domain.':entitlement:wiki:[A-Za-z0-9_]+$/';

Defineix el patró que segueix la urn. Si el format del valor urn de l'atribut eduPersonEntitlement és diferent s'ha de canviar el patró.

Codi del mòdul d'autenticació

```
<?php

class auth_simplesamlphp extends auth_basic {

  var $as;

  function auth_simplesamlphp()
  {
    $this->cando['external'] = true;
    $this->cando['logoff']   = true;
    $this->success = true;
  }

  function trustExternal($user,$pass,$sticky=false)
  {
    global $USERINFO;
    global $conf;

    $sticky ? $sticky = true : $sticky = false;
    //sanity check

    $path = '/var/simplesamlphp';
    if (array_key_exists('simplesamlphp_path', $conf)) {
      $path = $conf['simplesamlphp_path'];
    }
    require_once($path . '/lib/_autoload.php');

    $sp_auth = 'default-sp';
```

```
if (array_key_exists('simplesamlphp_sp_auth', $conf)) {
  $sp_auth = $conf['simplesamlphp_sp_auth'];
}

$this->as = new SimpleSAML_Auth_Simple($sp_auth);
$this->as->requireAuth();

$attributes = $this->as->getAttributes();

$attr_user = 'eduPersonPrincipalName';
if (array_key_exists('simplesamlphp_attr_user', $conf)) {
  $attr_user = $conf['simplesamlphp_attr_user'];
}

$attr_name = 'cn';
if (array_key_exists('simplesamlphp_attr_name', $conf)) {
  $attr_name = $conf['simplesamlphp_attr_name'];
}

$attr_mail = 'mail';
if (array_key_exists('simplesamlphp_attr_mail', $conf)) {
  $attr_mail = $conf['simplesamlphp_attr_mail'];
}

$attr_grps = 'eduPersonAffiliation';
if (array_key_exists('simplesamlphp_attr_grps', $conf)) {
  $attr_grps = $conf['simplesamlphp_attr_grps'];
}

if (!array_key_exists($attr_user, $attributes)) {
```

```
  die("no attribute \"" . $attr_user . "\" provided by IDP");
 }
 $user = $attributes[$attr_user][0];

 if (!array_key_exists($attr_name, $attributes)) {
  die("no attribute \"" . $attr_name . "\" provided by IDP");
 }
 $USERINFO['name'] = $attributes[$attr_name][0];

 if (!array_key_exists($attr_mail, $attributes)) {
  $USERINFO['mail'] = "";
 } else {
  $USERINFO['mail'] = $attributes[$attr_mail][0];
 }

 if (!array_key_exists($attr_grps, $attributes)) {
  $groups = array($conf['defaultgroup']);
} else {
  $groups = $attributes[$attr_grps];
}


$domain = substr($groups[0], 6);
$pattern = '/^urn:mace:'.$domain.':entitlement:wiki:[A-Za-z0-9_]+$/';

$attr_service='eduPersonEntitlement';
if (array_key_exists('simplesamlphp_attr_service', $conf)) {
   $attr_service = $conf['simplesamlphp_attr_service'];
 }
if (isset($attributes[$attr_service]) && is_array($attributes[$attr_service])) {
```

```
      foreach ($attributes[$attr_service] AS $ni) {
        if (preg_match($pattern, $ni, $matches)){
            $service = explode(":", $matches[0]);
         $groups[] = end($service);
        }
      }
     }

$USERINFO['grps']=$groups;

    $_SERVER['REMOTE_USER'] = $user;
    $_SESSION[DOKU_COOKIE]['auth']['user'] = $user;
    $_SESSION[DOKU_COOKIE]['auth']['pass'] = $pass;
    $_SESSION[DOKU_COOKIE]['auth']['info'] = $USERINFO;

    return true;
  }

  function logoff()
  {
    $this->as->logout();
  }
}
```

Integració de DokuWiki i simpleSAMLphp

1) Copio la classe simplesamlphp.class.php al directori inc/auth de DokuWiki

2) Per assegurar que DokuWiki i simpleSAMLphp poden compartir cookie canvio al fitxer de configuració config/config.php de simpleSAMLphp la següent línia:

```
'session.phpsession.cookiename'  => 'DokuWiki'
```

3) Perquè Dokuwiki i simpleSAMLphp puguin compartir sessió comento les següents línies al fitxer

inc/init.php de DokuWiki

```
if (!headers_sent() && !defined('NOSESSION')){
    session_name("DokuWiki");
    $cookieDir = empty($conf['cookiedir']) ? DOKU_REL : $conf['cookiedir'];
    if (version_compare(PHP_VERSION, '5.2.0', '>')) {
//      session_set_cookie_params(0,$cookieDir,'',($conf['securecookie'] && is_ssl()),true);
    }else{
//      session_set_cookie_params(0,$cookieDir,'',($conf['securecookie'] && is_ssl()));
    }
```

4) Introdueixo al fitxer de configuració local.php de DokuWiki les següents opcions de configuració:

```
/*
 * Section for access control and authentication
 */
$conf['useacl'] = 1;
$conf['authtype'] = 'simplesamlphp';
$conf['openregister'] = 0; // users are not allowed to register themselves
/*
 * Specific for simpleSAMLphp integration
 */
$conf['requirelogin'] = 'false';
$conf['simplesamlphp_path'] = '/var/simplesamlphp';
$conf['simplesamlphp_urlprefix'] = 'simplesaml/';
$conf['simplesamlphp_protocol'] = 'saml2';

$conf['simplesamlphp_attr_user']  = 'eduPersonPrincipalName';
$conf['simplesamlphp_attr_name'] = 'cn';
$conf['simplesamlphp_attr_mail']  = 'mail';
$conf['simplesamlphp_attr_grps'] = 'groups';
$conf['simplesamlphp_attr_service'] = 'eduPersonEntitlement';
```

Informació dels grups

Per habilitar la monitorització dels grups a Dokuwiki edito el fitxer dokuwiki/lib/tpl/default/footer.html

Afegeixo les línies següents després de

```
<?php
        echo "Membre del grup: ";
        global $USERINFO;
```

```
        echo join(“, “, $USERINFO['grps']).”<br />”;
?>
```

Al fons de la pàgina de DokuWiki apareixerà:

Membre del grup: users

Això significa que SimpleSAML ha mapejat per defecte l'usuari en el grup users

Versió “Adora Belle”

En la última versió estable de Dokuwiki s'ha canviat el template per defecte. Per poder visualitzar els grups a la wiki s'ha de copiar el fitxer footer.html al directori /lib/tpl/dokuwiki/

```
sudo cp ../dokuwiki/lib/tpl/default/footer.html ../dokuwiki/lib/tpl/dokuwiki/footer.html
```

Després s'ha d'editar l'arxiu footer.html de manera que només contingui en el següent codi:

```
<?php
        echo “Membre del grup: “;
        global $USERINFO;
        echo join(“, “, $USERINFO['grps']).”<br />”;
?>
```

6.2.3 Definir l'atribut eduPersonEntitlement a l'SP amb Auth Proc Filters

Generalment els atributs eduPersonAffiliation i eduPersonEntitlement no estan definits per a tots els usuaris en l'IdP FeideOpenIdP. Aquest problema es pot solucionar utilitzant en config.php els filtres *core:AttributeAdd* i *core:AttributeAlter* per assignar aquests atributs als usuaris en l'SP.

Primer es creen els atributs per a tots els usuaris assignant-los un valor específic:

```
51 => array(
        'class' => 'core:AttributeAdd',
        'eduPersonAffiliation' => array('member'),
```

```
'eduPersonEntitlement' => array('urn:mace:rnd.feide.no:entitlement:wiki:readonly'),
),
```

Després es modifica el valor de l'atribut eduPersonEntitlement per alguns usuaris amb el filtre *core:AttributeAlter* per assignar grups específics a aquests usuaris en Dokuwiki. Indirectament, també, es defineix l'administrador de Dokuwiki que pertany al grup admin. A continuació es mostra el procediment amb tres usuaris registrats en Feide OpenIdP: fgil2, fegil2 i ggil2.

```
52 => array(
    'class' => 'core:AttributeAlter',
    'subject' => 'eduPersonPrincipalName',
    'pattern' => '/fgil2@rnd.feide.no/',
    'replacement' => 'urn:mace:rnd.feide.no:entitlement:wiki:admin',
    'target' => 'eduPersonEntitlement',
    '%replace',
    ),

53 => array(
    'class' => 'core:AttributeAlter',
    'subject' => 'eduPersonPrincipalName',
    'pattern' => '/fegil2@rnd.feide.no/',
    'replacement' => 'urn:mace:rnd.feide.no:entitlement:wiki:readwrite',
    'target' => 'eduPersonEntitlement',
    '%replace',
    ),
54 => array(
    'class' => 'core:AttributeAlter',
    'subject' => 'eduPersonPrincipalName',
    'pattern' => '/ggil2@rnd.feide.no/',
    'replacement' => 'urn:mace:rnd.feide.no:entitlement:wiki:othergroup',
```

'target' => 'eduPersonEntitlement',
'%replace',
),

6.2.4 Proves en la situació I)

Test 1

Introduïm al navegador la direcció https://fernando.net/dokuwiki per autenticar l'usuari registrat fgil2@rnd.feide.no que té permisos d'administrador de la wiki. Es redirigeix al formulari d'autenticació de l'IdP, com es pot veure en la figura següent:

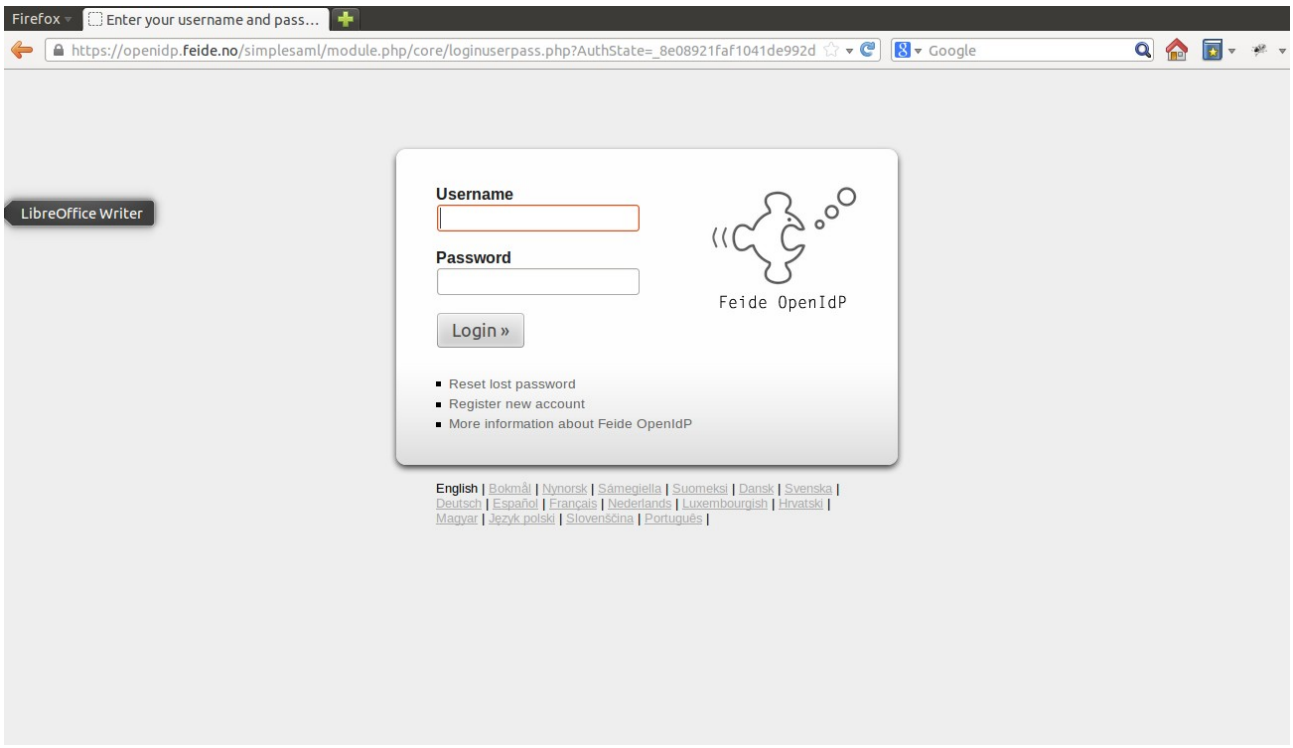

Figura 7

L'usuari s'autentica i s'accedeix a Dokuwiki

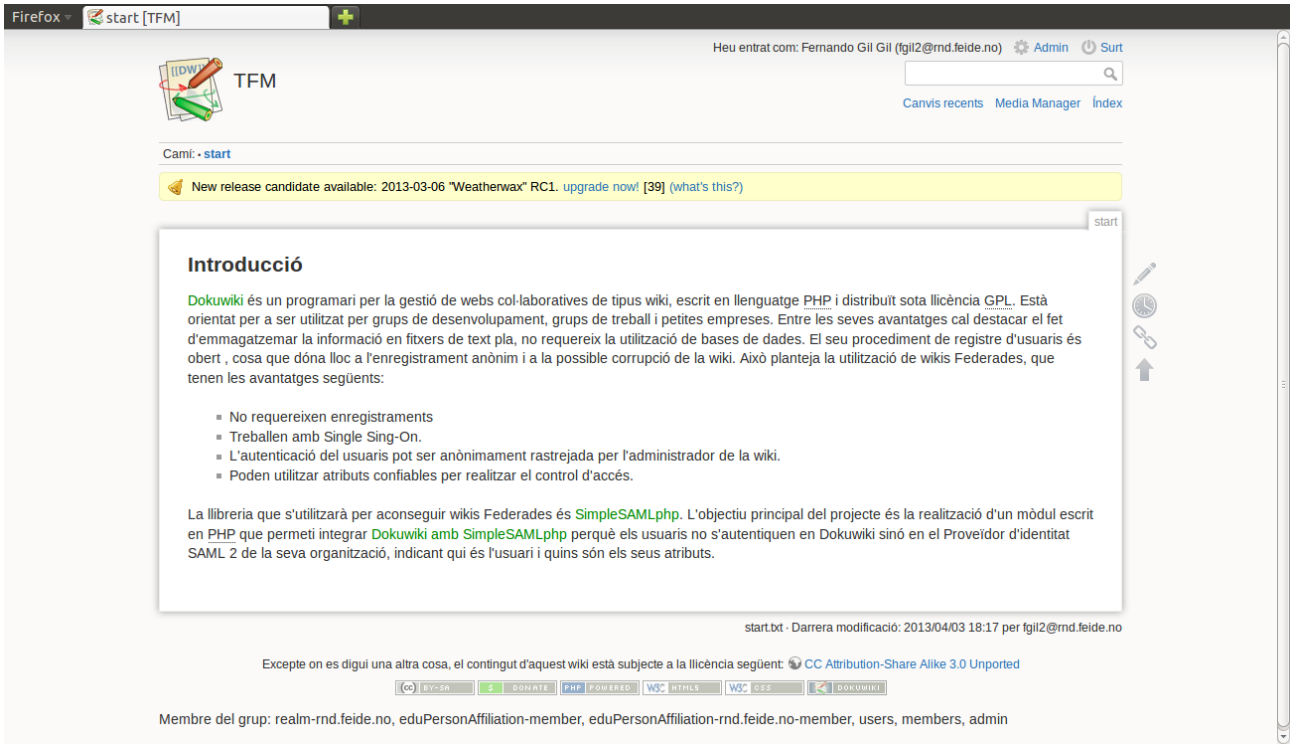

Figura 8

Es pot apreciar que apareixen al fons els grups. També, apareix el botó “Admin” que permet a l'usuari realitzar tasques d'administració de la wiki, com la gestió de grups i permisos ACL.

Es repeteix la prova amb els usuaris fegil2@rnd.feide.no i ggil2@rnd.feide registrats a Feide OpenIdP i s'obtenen els resultats esperats.

Test 2

Es fa l'autenticació amb un usuari no registrat. En aquest cas el formulari de l'IdP torna a demanar nom d'usuari i contrasenya.

Test 3

Es fa l'autenticació amb un usuari registrat, però aquest no pertany a un grup amb permisos ACL definits a Dokuwiki. En aquest cas s'accedeix a Dokuwiki però no es mostra cap pàgina de la wiki, surt el missatge “Permís Denegat”.

Test 4

Es realitza el procés de logout clicant el botó “Surt” de la wiki. El resultat és l'esperat, es tanca sessió i torna a sortir el formulari de l'IdP. Per introduir un altre usuari cal tornar a introduir la direcció https://fernando.net/dokuwiki al navegador.

6.2.5 Configuració del Proveïdor de Servei (SP) per la situació II)

Configuració del Proveïdor d'Identitat (IdP)

1) Habilitar la funcionalitat de Proveïdor d'Identitat

S'edita el fitxer config/config.php i s'escriu:

'enable.saml20-idp' => true,

2) Mòdul d'autenticació

Escollo el mòdul d'autenticació exampleauth:UserPass , on s'autentica contra una llista de noms d'usuari i contrasenyes.

3) Configuració del mòdul d'autenticació

S'habilita el mòdul exampleauth:UserPass creant un fitxer al directori /modules/exempleauth/. Mitjançant el comandament següent:

sudo touch /var/simplesamlphp/modules/exampleauth/enable

Es creen els usuaris escrivint-los al fitxer config/authsources.php

```
<?php
'example-userpass' => array(
        'exampleauth:UserPass',
                'fegil2:1234' => array(
                'uid' => array('fegil2'),
                 'cn'  => array('Fernando Gil'),
                 'mail' => array('fgilgi@uoc.edu'),
                 'eduPersonPrincipalName' => array('fegil2@fernan.net'),
                 'eduPersonAffiliation' => array('member', 'teacher'),
                 'eduPersonEntitlement' => array('urn:mace:fernan.net:entitlement:wiki:readwrite')
            ),
                'ggil2:1235' => array(
                 'uid' => array('ggil2'),
                 'cn'  => array('Gemma Gil'),
                 'mail' => array('ggilgi@gmail.com'),
                'eduPersonPrincipalName' => array('ggil2@fernan.net'),
                 'eduPersonAffiliation' => array('member', 'student'),
                 'eduPersonEntitlement' => array('urn:mace:fernan.net:entitlement:wiki:readonly')
            ),
                'fgil2:1236' => array(
                 'uid' => array('fgil2'),
                 'cn'  => array('Fernando Gil'),
                 'mail' => array('fgilgi@uoc.edu'),
                 'eduPersonPrincipalName' => array('fgil2@fernan.net'),
                 'eduPersonAffiliation' => array('member', 'employee'),
                 'eduPersonEntitlement' => array('urn:mace:fernan.net:entitlement:wiki:admin')
            ),
        ),
);
```

La configuració crea tres usaris: fegil2, ggil2 i fgil2 amb contrasenyes 1234, 1235 i 1236 , respectivament.

L'IdP retornarà els atributs: 'uid', 'cn', 'mail' , 'eduPersonPrincipalName', 'eduPersonAffiliation' i 'eduPersonEntitlement' quan l'usuari s'autentiqui.

4) Creació d'un certificat SSL

S'accedeix al directori /cert

cd /var/simplesamlphp/cert

Es creen el certificat vàlid per 10 anys fernan.net.crt i la clau privada fernan.net.pem

sudo openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out fernan.net.crt -keyout fernan.net.pem

5) Configuració de l'IdP

L'IdP es configura amb les metadades emmagatzemades a metadata/saml20-idp-hosted.php

```
<?php
$metadata['__DYNAMIC:1__'] = array(
    /*
     * The hostname for this IdP. This makes it possible to run multiple
     * IdPs from the same configuration. '__DEFAULT__' means that this one
     * should be used by default.
     */
    'host' => '__DEFAULT__',

    /*
     * The private key and certificate to use when signing responses.
     * These are stored in the cert-directory.
     */
    'privatekey' => 'fernan.net.pem',
    'certificate' => 'fernan.net.crt',

    /*
     * The authentication source which should be used to authenticate the
     * user. This must match one of the entries in config/authsources.php.
     */
    'auth' => 'example-userpass',
);
```

6) Utilització del uri NameFormat en els atributs

El perfil d'interoperabilitat SAML 2.0 especifica que els atributs han de ser lliurats utilitzant el NameFormat urn:oasis:names:tc:SAML:2.0:attrname-format:uri. Es recomana utilitzar això en noves instal·lacions. Això es pot fer afegint al fitxer de configuració saml20-idp-hosted les línies següents:

```
'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',
'authproc' => array(
    // Convert LDAP names to oids.
    100 => array('class' => 'core:AttributeMap', 'name2oid'),
),
```

7) Afegir SPs a l'IdP

Per afegir un SP a l'IdP s'han d'incloure les seves metadades al fitxer de configuració metadata/saml20-sp-remote.php

La configuració mínima és la següent:

```
<?php
$metadata['https://fernan.net/simplesaml/module.php/saml/sp/metadata.php/default-sp'] = array(
    'AssertionConsumerService' => 'https://fernan.net/simplesaml/module.php/saml/sp/saml2-
acs.php/default-sp',
    'SingleLogoutService' => 'https://fernan.net/simplesaml/module.php/saml/sp/saml2-
logout.php/default-sp',
);
```

Configuració del Proveïdor de Servei (SP) amb IdP local

Faré la configuració en què el Proveïdor de Identitat (IdP) serà el construït amb simpleSAMLphp al servidor fernan.net.

1) L'SP és configura per l'entrada al fitxer
config/authsources.php
La configuració mínima és

```
<?php
$config = array(

    /* This is the name of this authentication source, and will be used to access it later. */
    'default-sp' => array(
        'saml:SP',
    ),
);
```

2) Habilitar un certificat per l'SP

Creo un certificat al directori cert/

```
cd cert
openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out saml.crt -keyout saml.pem
```

Edito al fitxer authsources.php les entrades següents:

```
 'default-sp' => array(
    'saml:SP',
    'privatekey' => 'saml.pem',
```

```
    'certificate' => 'saml.crt',
),
```

3) Afegir IdPs a l'SP

Per afegir un IdP a l'SP s'han d'incloure les seves metadades al fitxer de configuració metadata/saml20-idp-remote.php

El fitxer XML amb les metadades de l'IdP construït amb simpleSAMLphp es pot obtenir a partir de la direcció https://fernan.net/simplesaml/saml2/idp/metadata.php?output=xhtml

Copio la conversió a un fitxer en format simpleSAMLphp del les metadades XML i la pego al fitxer metadata/saml20-idp-remote.php, obtenint el resultat següent:

```
$metadata['https://fernan.net/simplesaml/saml2/idp/metadata.php'] = array (
  'metadata-set' => 'saml20-idp-remote',
  'entityid' => 'https://fernan.net/simplesaml/saml2/idp/metadata.php',
  'SingleSignOnService' => 'https://fernan.net/simplesaml/saml2/idp/SSOService.php',
  'SingleLogoutService' => 'https://fernan.net/simplesaml/saml2/idp/SingleLogoutService.php',
  'certData' =>
'MIIEETCCAvmgAwIBAgIJAK5Se9h6KCUFMA0GCSqGSIb3DQEBBQUAMIGeMQswCQYDVQQ
GEwJFUzESMBAGA1UECAwJQmFyY2Vsb25hMRAwDgYDVQQHDAdSdWLDg8KtMRQwEgYDV
QQKDAtFbnNlbnlhbWVudDEZMBcGA1UECwwQSU5TIERyLiBQdWlndmVydDETMBEGA1UEAw
wKZmVybmFuLm5ldDEjMCEGCSqGSIb3DQEJARYUZmdpbDJAdGVsZWZvbmljYS5uZXQwHhc
NMTMwMTAzMDgwOTA5WhcNMjMwMTAzMDgwOTA5WjCBnjELMAkGA1UEBhMCRVMxEjAQB
gNVBAgMCUJhcmNlbG9uYTEQMA4GA1UEBwwHUnViw4PCrTEUMBIGA1UECgwLRW5zZW55
YW1lbnQxGTAXBgNVBAsMEElOUyBEci4gUHVpZ3ZlcnQxEzARBgNVBAMMCmZlcm5hbi5uZXQ
xIzAhBgkqhkiG9w0BCQEWFGZnaWwyQHRlbGVmb25pY2EubmV0MIIBIjANBgkqhkiG9w0BAQE
FAAOCAQ8AMIIBCgKCAQEApLa81Af6zYaLV8M/VAQhACSKKCX7LbgLlt51C7BypFLtVA2wBIHa
g2sB+Xd4zA8a0Nv355BKApp3mDEEvsk6sfi+cxetY/Wu2HWxS91ef5+Zhuw3QtnRq/i/WN5iGJMz
PpFmhPt/9JkJZ+riy58h3xBAKitedtoVBl0s0udNNeC4nvsgQT0bmsFLZWB68KUUVsmohyhE2E+p
A/SqgePV8RI5x+SEfwP3F186Wzzjghf8UliJmqjchhwSSBbMmaU2WdhTfaTGtHDhKuYMa+dBVtH
c/8u8Fl6xcj2b2eVjckFfGSOuxOaRq/C4iDRVJ10WXuplAtcToBWTFH2KWSubEQIDAQABo1AwTjA
dBgNVHQ4EFgQUvMxE7LOsgRdDaYcWxei1V+9o0/AwHwYDVR0jBBgwFoAUvMxE7LOsgRdDa
YcWxei1V+9o0/AwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAlXfO+YcgQPBs
RnjnkV10zZzLH7T5mWDudBzhP6qZynSot+L8KlyRQXmo/dq64GQB67y8ZpcwDQIYg+XkafLS2+
DPiAgskEdlJ+pva6bIi8JpWD+THBjol0bmbW0cWquw2tDa+HzC68aHdXACk5e9PQqavNWMmup
QZUEiWYG9pKf2k10RvHIyg+dZMjWcCLOSiv8n2rRE/NxI9KvB5VEsamorwIqXK/bDpjeVomufI+JB
+fNGI+ihdbZbX3I7nBU8qOFOsWnpk/JfAMItNNarETuAwAmmpuJioprrj71aN+b/BIqT6uDJOs3eDKj
7/RJfwIV/H0bXIwyJbQaFXZ7yKA==',
  'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',
);
```

4) IdP per defecte

Incloc per defecte fernan.net com a IdP , introduint les següents entrades a authsources.php

```
<?php
$config = array(

    'default-sp' => array(
        'saml:SP',

        /*
         * The entity ID of the IdP this should SP should contact.
         * Can be NULL/unset, in which case the user will be shown a list of available IdPs.
         */
        'idp' => 'https://fernan.net/simplesaml/saml2/idp/metadata.php',
    ),
);
```

5) Conversió dels oid noms dels atributs a noms LDAP

Donat que en el modul d'autenticació per a Dokuwiki s'utilitzen LDAP noms en els atributs, hem de convertir en el SP per defecte els oid noms dels atributs en LDAP noms. Això es pot fer editant en authsouuces.php les línies següents:

```
'default-sp' => array(

                    // Auth Proc Filter core:AttributeMap with the file oid2name
                    'authproc' => array(
                    50 => array(
                            'class' => 'core:AttributeMap',
                            'oid2name',
                            ),
                    ),
),
```

6.2.6 Proves per la situació II)

Test 1

Introduïm al navegador la direcció https://fernando.net/dokuwiki per autenticar l'usuari registrat

fgil2 que té permisos d'administrador de la wiki. Es redirigeix al formulari d'autenticació de l'IdP, com es pot veure en la figura següent:

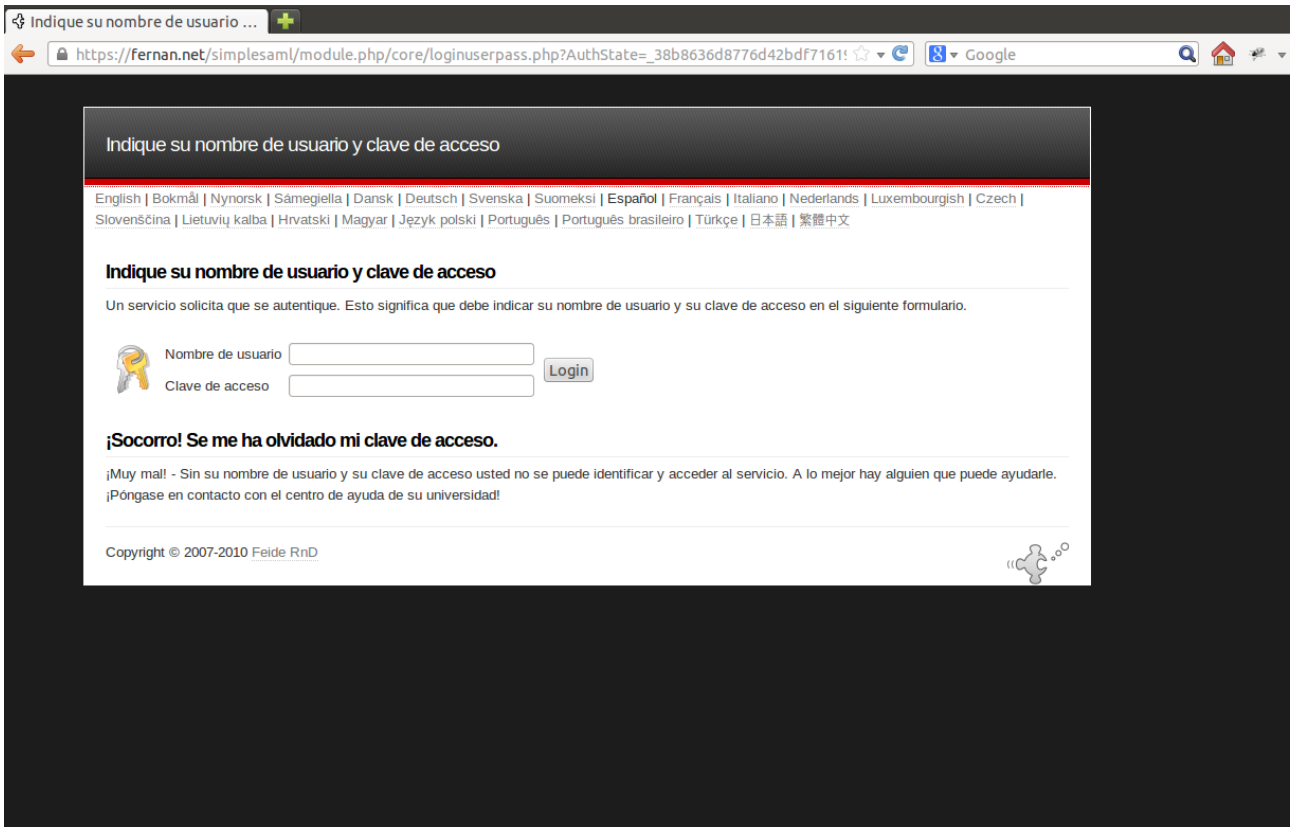

Figura 9

L'usuari s'autentica i s'accedeix a Dokuwiki

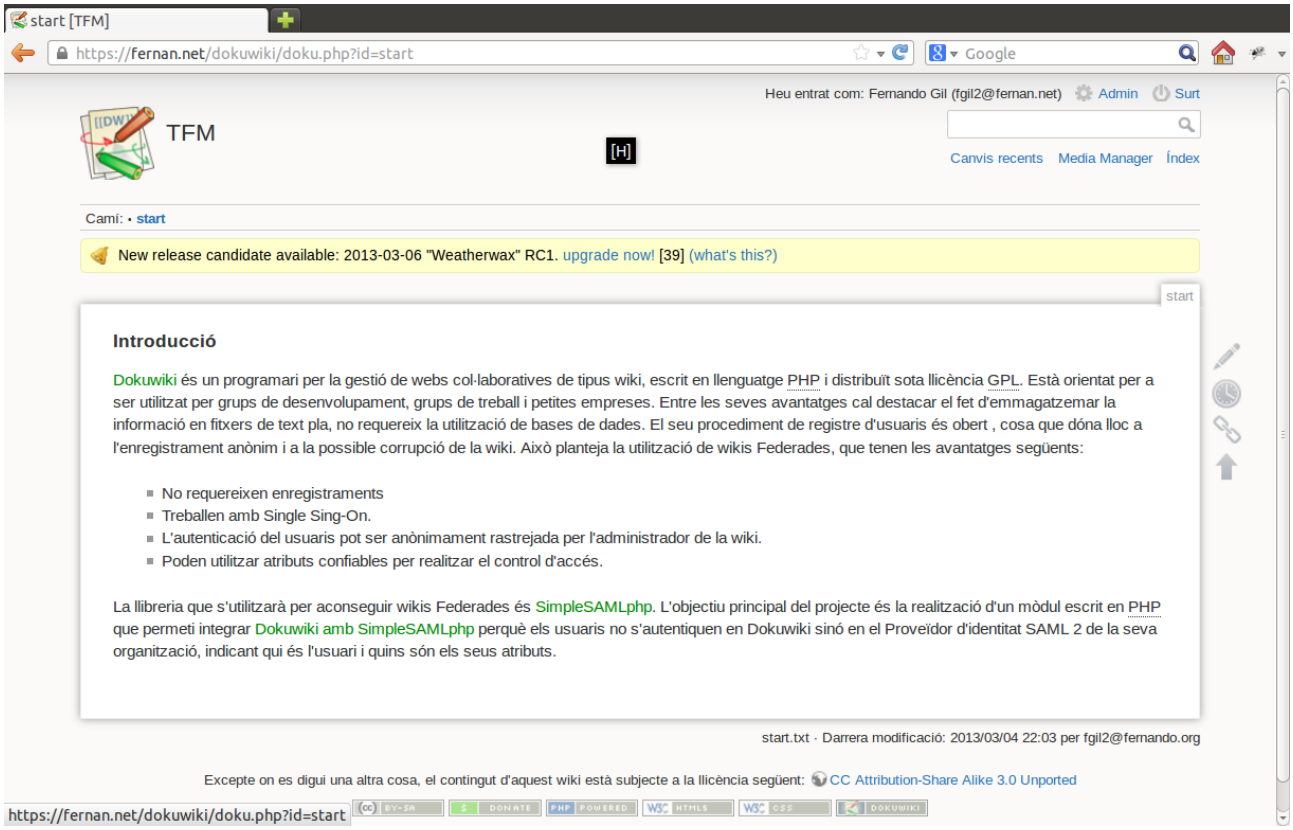

Figura 10

S'observa a la part superior el valor fgil2@fernan.net de l'atribut eduPersonPrincipalName i el botó “Admin”.

Es repeteix la prova amb els altres usuaris definits: fegil2 i ggil2 i s'obtenen el resultats esperats com en el cas anterior.

De manera anàloga es realitzen els tests 2, 3 i 4 del cas anterior i s'obtenen resultats idèntics.

6.2.7 Instal·lació d'un servidor LDAP

A una màquina virtual amb sistema Ubuntu 10.04 creada amb VirtualBox instal·laré un servidor LDAP. El nom del servidor serà fernando.org

1) S'instal·la el dimoni LDAP slapd i ldap-utils

sudo apt-get install slapd ldap-utils

2) Es carreguen des d'el terminal alguns esquemes addicionals

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
```

3) El mòdul d'autenticació utilitza alguns atributs de la classe eduPerson

Des de la direcció https://spaces.internet2.edu/display/macedir/LDIFs descarrego el fitxer ldif que defineix l'esquema LDAP de la classe eduPerson per a OpenLDAP.

Copio els fitxers eduperson.ldif i eduperson.schema als directori /etc/ldap/schema/

Carrego des del terminal l'esquema eduPerson

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/eduperson.ldif
```

4) Edito el fitxer backend.fernando.org.ldif

```
# Load dynamic backend modules
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb

# Database settings
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=fernando,dc=org
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=fernando,dc=org
```

olcRootPW: XXXX
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=fernando,dc=org" write by anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=fernando,dc=org" write by * read

Afegeixo el LDIF al directori:

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f backend.example.com.ldif

5) El directori frontend està ara enllestit per ser omplert. Edito el fitxer frontend.fernando.org.ldif amb el contingut següent:

Create top-level object in domain
dn: dc=fernando,dc=org
objectClass: top
objectClass: dcObject
objectclass: organization
o: Fernando Organization
dc: fernando
description: LDAP Example

Admin user.
dn: cn=admin,dc=fernando,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: XXXX

dn: ou=people,dc=fernando,dc=org
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=fernando,dc=org
objectClass: organizationalUnit
ou: groups

```
dn: uid=fgil2,ou=people,dc=fernando,dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: fgil2
sn: Gil
givenName: Fernando
cn: Fernando Gil
displayName: Fernando Gil
uidNumber: 1000
gidNumber: 10000
userPassword: XXXX
gecos: Fernando Gil
loginShell: /bin/bash
homeDirectory: /home/fernando
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: fgilgi@uoc.edu
postalCode: 08197
l: Barcelona
o: Fernando Organization
mobile: xx xx xx xx
homePhone:  xx xx xx xx
title: System Administrator
postalAddress:
initials: FG

dn: cn=example,ou=groups,dc=fernando,dc=org
objectClass: posixGroup
cn: example
gidNumber: 10000
```

Afegeixo l'entrada al directori LDAP:

```
sudo ldapadd -x -D cn=admin,dc=fernando,dc=org -W -f frontend.fernando.org.ldif
```

6) Instal·lo l'aplicació LDAP Account Manager

```
sudo apt-get install ldap-account-manager
```

S'accedeix a l'aplicació web des del navegador amb la direcció http://localhost/lam

Configuro LDAP Account Manager perquè reconegui el servidor LDAP, fernando.org, i introdueixo alguns usuaris amb els atributs inclosos al mòdul d'autenticació de Dokuwiki: uid, cn, mail, eduPersonPrincipalName, eduPersonAffiliation i eduPersonEntitlement.

6.2.8 Configuració del Proveïdor de Servei (SP) per la situació III)

1) A l'ordinador on està instal·lat l'IdP amb simplesamlphp edito el fitxer /etc/hosts

Introdueixo la línia amb la direcció IP del servidor LDAP, fernando.org:

192.168.1.38 fernando.org

2) Habilito el modul LDAP de simpleSAMLphp:

sudo touch /var/simplesamlphp/modules/ldap/enable

3) Modifico authsources.php perquè tingui com a font d'autenticació el servidor LDAP, fernando.org

```
'example-ldap' => array(
    'ldap:LDAP',

    /* The hostname of the LDAP server. */
    'hostname' => 'fernando.org',

    /* Whether SSL/TLS should be used when contacting the LDAP server. */
    'enable_tls' => FALSE,

    /*
     * Which attributes should be retrieved from the LDAP server.
     * This can be an array of attribute names, or NULL, in which case
     * all attributes are fetched.
     */
    'attributes' => NULL,

    /*
     * The pattern which should be used to create the users DN given the username.
     * %username% in this pattern will be replaced with the users username.
```

```
     *
     * This option is not used if the search.enable option is set to TRUE.
     */
    'dnpattern' => 'uid=%username%,ou=people,dc=fernando,dc=org',

    /*
     * As an alternative to specifying a pattern for the users DN, it is possible to
     * search for the username in a set of attributes. This is enabled by this option.
     */
    'search.enable' => FALSE,

    /*
     * The DN which will be used as a base for the search.
     * This can be a single string, in which case only that DN is searched, or an
     * array of strings, in which case they will be searched in the order given.
     */
    'search.base' => 'ou=people,dc=fernando,dc=org',

    /*
     * The attribute(s) the username should match against.
     *
     * This is an array with one or more attribute names. Any of the attributes in
     * the array may match the value the username.
     */
    'search.attributes' => array('uid', 'mail'),

    /*
     * The username & password the simpleSAMLphp should bind to before searching. If
     * this is left as NULL, no bind will be performed before searching.
     */
    'search.username' => NULL,
    'search.password' => NULL,
),
```

4) Modifico metadata/saml20-idp-hosted.php per configurar l'IdP amb la font d'autenticació del servidor LDAP:

```
<?php
$metadata['__DYNAMIC:1__'] = array(
    /*
     * The hostname for this IdP. This makes it possible to run multiple
     * IdPs from the same configuration. '__DEFAULT__' means that this one
     * should be used by default.
     */
    'host' => '__DEFAULT__',
```

```
    /*
     * The private key and certificate to use when signing responses.
     * These are stored in the cert-directory.
     */
    'privatekey' => 'server.pem',
    'certificate' => 'server.crt',

    /*
     * The authentication source which should be used to authenticate the
     * user. This must match one of the entries in config/authsources.php.
     */
    'auth' => 'example-ldap',
);
```

6.2.9 Instal·lació de l'overlay memberOf

Per poder passar al proveïdor de servei (SP) els grups definits a la base de dades del servidor LDAP és necessari que els usuaris tinguin definit l'atribut memberOf. A més, això només serà possible en un servidor OpenLDAP si els grups pertanyen a l'objectClass groupOfNames. A continuació es descriu com fer la instal·lació:

Creo el primer ldif per overlay:

sudo nano memberof1.ldif

dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulePath: /usr/lib/ldap
olcModuleLoad: memberof

Afegeixo a config database:

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f memberof1.ldif

Creo el segon ldif per overlay:

sudo nano memberof2.ldif

dn: olcOverlay=memberof,olcDatabase={1}hdb,cn=config
objectClass: olcMemberOf
objectClass: olcOverlayConfig
objectClass: olcConfig
objectClass: top
olcOverlay: memberof
olcMemberOfDangling: ignore
olcMemberOfRefInt: TRUE
olcMemberOfGroupOC: groupOfNames
olcMemberOfMemberAD: member
olcMemberOfMemberOfAD: memberOf

Afegeixo a config database:

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f memberof2.ldif

Amb LAM (LDAP Account Manager) creo nous grups de groupOfNames:
S'ha d'insertar a member el distiguishedName de cada usuari, per exemple:
uid=fgil2,ou=people,dc=fernando,dc=org

Es pot comprovar el funcionament correcte de l'atribut memberOf fent les consultes següents:

ldapsearch -h fernando.org -x -b "dc=fernando,dc=org" '(uid=ggil2)' memberOf

Donà els dn dels grups de l'usuari ggil2

ldapsearch -h fernando.org -x -b "dc=fernando,dc=org" '(&(objectClass=inetOrgPerson)(memberOf=cn=students,ou=groups,dc=fernando,dc=org))'

Dóna els dn dels usuaris del grup cn=students,ou=groups,dc=fernando,dc=org

6.2.10 Definir el filtre ldap:AttributeAddUsersGroups

Introdueixo a l'apartat authproc.sp del fitxer config.php de simpleSAMLphp el filtre ldap:AttributeAddFromLDAP per afegir un atribut groupsLDAP que conté els dn dels grups definits al servidor LDAP de l'usuari autenticat

```
62 => array(
    'class' => 'ldap:AttributeAddFromLDAP',
    'authsource' => 'example-ldap',
    'ldap.basedn' => 'DC=fernando,DC=org',
    'attribute.username' => 'uid',
    'attribute.new' => 'groupsLDAP',
    'search.attribute' => 'memberOf',
    'search.filter' => '(uid=%uid%)'
),
```

Amb el filtre ldap:AttributeAddUsersGroups s'afegeixen els grups definits al servidor LDAP de l'usuari autenticat a l'atribut groups. Perquè funcioni aquest filtre s'ha de tenir en compte l'esquema de la base de dades LDAP. En el cas utilitzat amb openLDAP l'objecClass dels usuaris és inetOrgPerson i l'objectClass dels grups és groupOfNames.

```
63 => array(
```

```
    'class' => 'ldap:AttributeAddUsersGroups',
    'authsource' => 'example-ldap',
    'ldap.basedn' => 'DC=fernando,DC=org',
    'attribute.username' => 'uid',
    'attribute.memberof' => 'groupsLDAP',
    'type.group' => 'groupOfNames',
    'type.user' => 'inetOrgPerson',
),
```

Amb el filtre authorize:Authorize es pot restringir l'autorització a un grup definit al servidor LDAP . Per exemple faig la restricció al grup *cn=teachers,ou=groups,dc=fernando,dc=org*

```
64 => array(
     'class' => 'authorize:Authorize',
     'regex' => FALSE,
     'groups' => 'cn=teachers,ou=groups,dc=fernando,dc=org'
),
```

6.2.11 Proves en la situació III)

Test 1

Per comprovar que l'SP rep correctament els grups definits al servidor LDAP de l'usuari autenticat cal mostrar els seus atributs. Per fer això, obrim simpleSAMLphp introduint al navegador la direcció https://fernan.net/simplesaml. Cliquem la pestanya "Autenticación" >> "Probar fuentes de autenticación" i l'opció "default-sp". A continuació introduïm usuari i contrasenya. En la figura següent es mostren els atributs de l'usuari ggil2:

Ejemplo de SAML 2.0 SP

Hola, esta es la página de estado de simpleSAMLphp. Desde aquí puede ver si su sesión ha caducado, cuanto queda hasta que lo haga y todos los atributos existentes en su sesión.

Atributos

Nombre común (CN)	Gemma Gil
Apellidos	Gil
Identificador de usuario	ggil2
Afiliación	student
Derecho relativo al servicio	• urn:mace:fernando.org:entitlement:wiki:readonly • urn:mace:fernando.org:entitlement:wiki:othergroup
objectClass	• eduPerson • inetOrgPerson • shadowAccount • top
Identificador único de la persona en su organización de origen	ggil2@fernando.org
Clave o contraseña y método de encriptación utilizado	{SSHA}TtCXUaMyTiWtQWpJURWvusnAmEkuM5rv
Nombre	Gemma
Correo electrónico	ggil2@gmail.com
groups	• realm-fernando.org • eduPersonAffiliation-student • eduPersonAffiliation-fernando.org-student • users • members • cn=students,ou=groups,dc=fernando,dc=org • cn=french,cn=students,ou=groups,dc=fernando,dc=org
groupsLDAP	• cn=students,ou=groups,dc=fernando,dc=org • cn=french,cn=students,ou=groups,dc=fernando,dc=org

Salir

[Salir]

Sobre simpleSAMLphp

Figura 11

S'observa que s'ha afegit un nou atribut groupsLDAP amb els dn dels grups que pertany l'usuari en el servidor LDAP. A més, tots aquests grups estan inclosos en l'atribut groups. Per tant, podran ser utilitzats per Dokuwiki mitjançant el mòdul d'autenticació. El fet d'afegir els distinguishedName

dels grups permet mantenir en Dokuwiki la jerarquia de grups i subgrups que hi havia en el servidor LDAP. D'aquesta manera es podrà fer una assignació de permisos ACL que sigui coherent amb la jerarquia de grups.

Test 2

Introduïm al navegador la direcció https://fernando.net/dokuwiki per autenticar l'usuari ggil2 . Es redirigeix al formulari d'autenticació de l'IdP. Introduïm usuari i contrasenya i es mostra la pantalla següent:

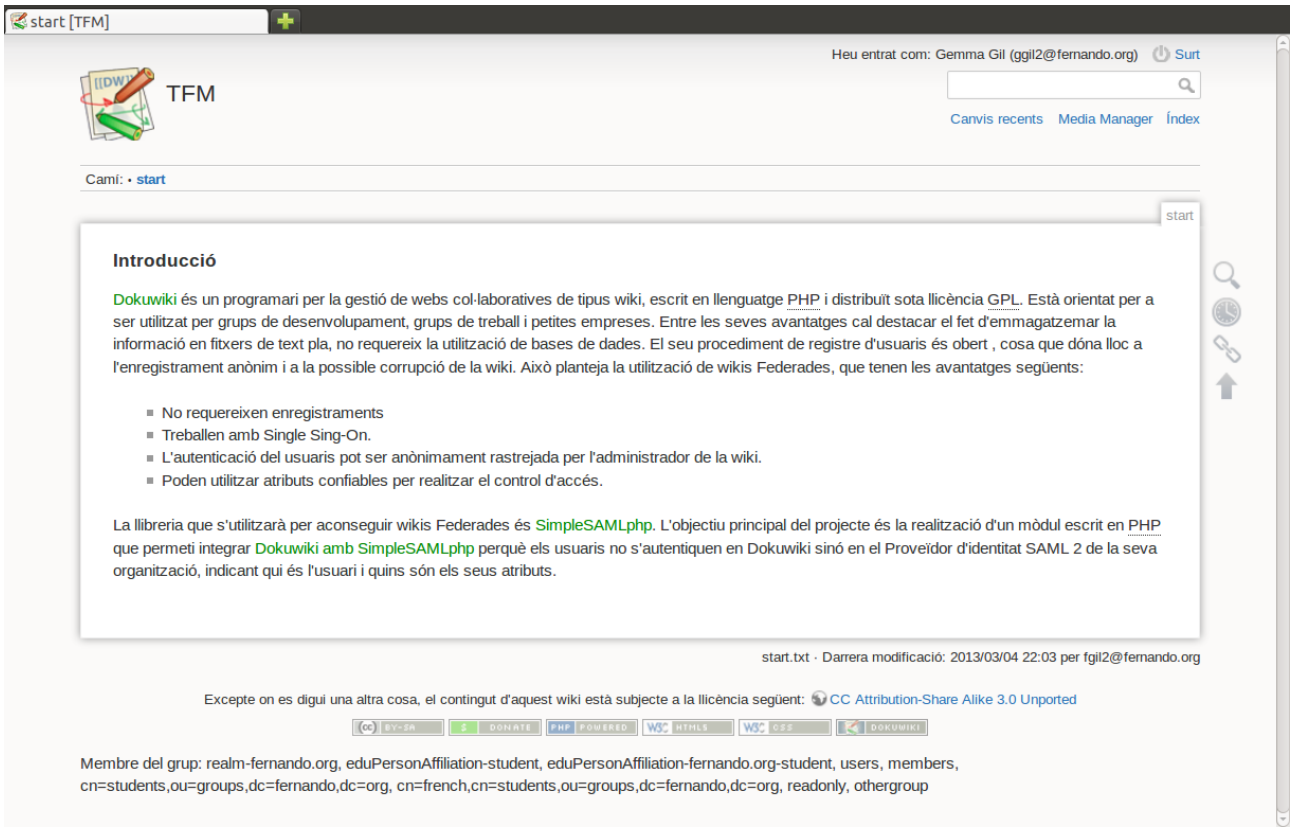

Figura 12

S'observa en la capçalera l'identificador ggil2@fernando.org de l'usuari en el domini i, en el peu de pàgina tots els grups de l'usuari a Dokuwiki definits a partir dels seus atributs.

Test 3

Es fa l'autenticació amb un usuari no registrat al servidor LDAP. En aquest cas el formulari de l'IdP torna a demanar nom d'usuari i contrasenya.

Test 4

Es fa l'autenticació amb un usuari registrat al servidor LDAP, però aquest no pertany a un grup amb permisos ACL definits a Dokuwiki. En aquest cas s'accedeix a Dokuwiki però no es mostra cap pàgina de la wiki, surt el missatge “Permís Denegat”.

Test 5

Es realitza el procés de logout clicant el botó “Surt” de la wiki. El resultat és l'esperat, es tanca sessió i torna a sortir el formulari de l'IdP. Per introduir un altre usuari cal tornar a introduir la direcció https://fernando.net/dokuwiki al navegador.

Test 6

Es comprova el funcionament del filtre authorize:Authorize restringint la wiki al grup cn=teachers,ou=groups,dc=fernando,dc=org. Els usuaris d'aquest grup accedeixen a Dokuwiki, i es denega l'accés a l'SP als altres, mostrant el missatge “Acceso denegado”, tal com es mostra a la figura següent:

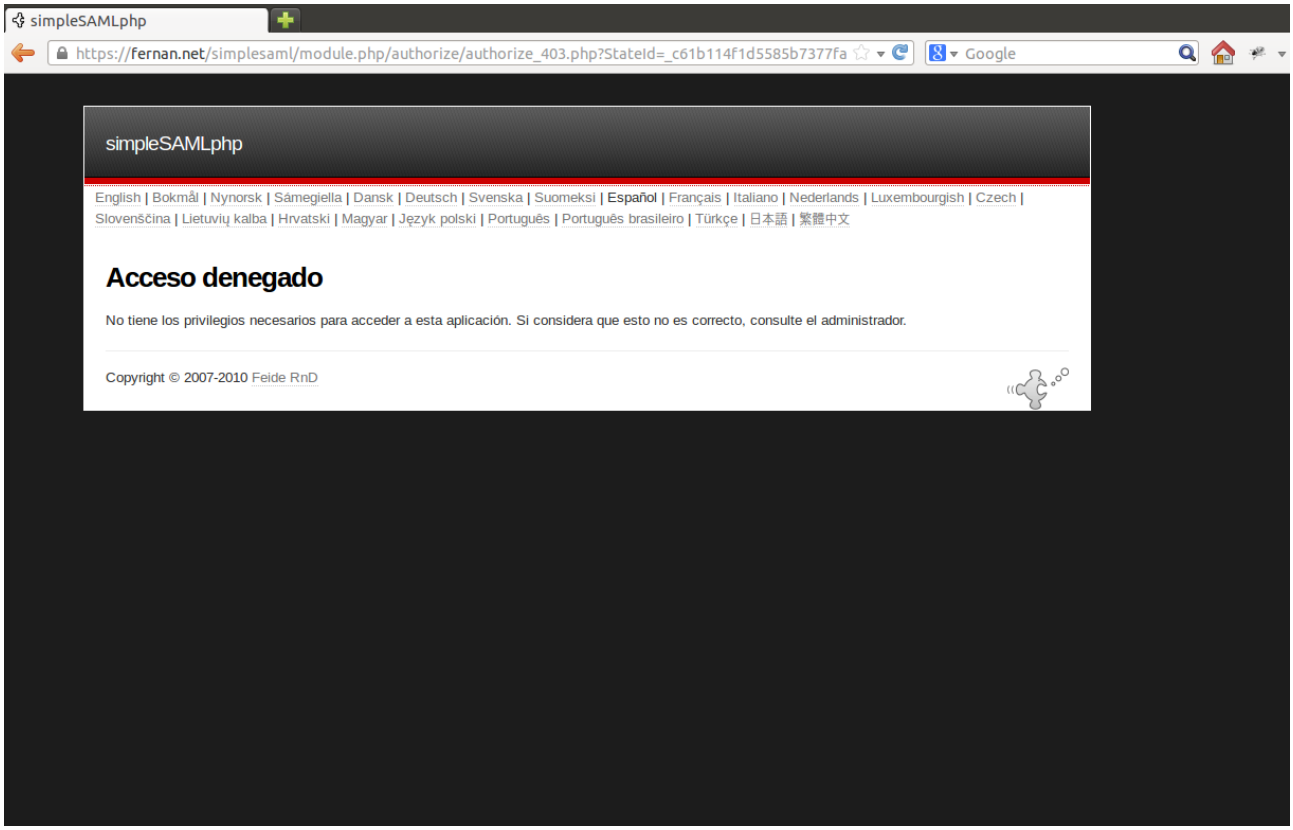

Figura 13

Degut a un error en el filtre authorize:Authorize cal tancar el navegador i tornar-lo a obrir per accedir a l'SP després d'haver estat denegada l'autorització a un usuari.

6.2.12 Prova amb el navegador Explorer

Es fa la prova en un ordinador amb sistema operatiu Windows 7.
Executem com a administrador el programa cmd.
cd \windows\system32\drivers\etc
Editem amb notepad el fitxer hosts, afegint la línia que dóna la direcció IP del servidor web:
192.168.1.36 fernan.net

Al navegador Explorer s'introdueix la direcció https://fernan.net/dokuwiki. Es redirigeix al formulari d'autenticació de l'IdP. Ens autentiquem i apareix la pàgina de Dokuwiki com es mostra a la figura següent:

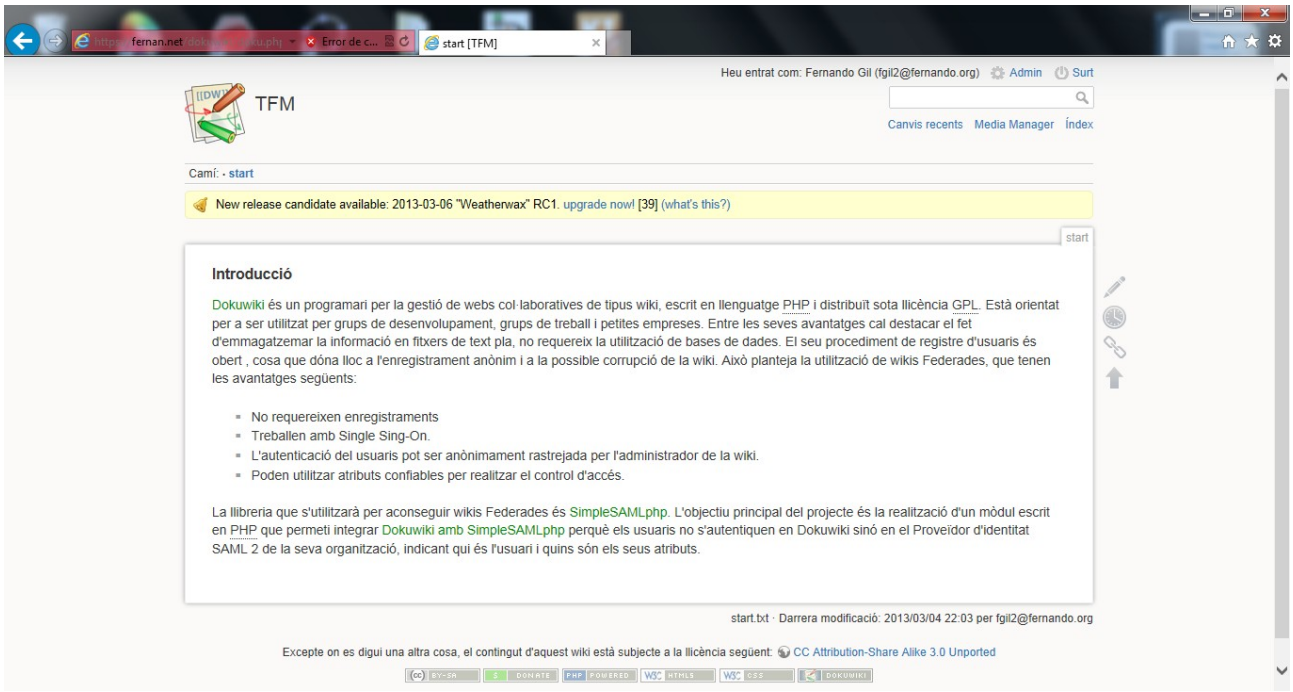

Figura 14

6.2.13 Proves en dispositius mòbils

Prova del nou template de Dokuwiki en un dispositiu mòbil amb Android

S'ha fet la prova en un ordinador amb sistema operatiu Windows 7 on s'ha instal·lat Android Emulator al directori d:\development. El dispositiu mòbil creat s'anomena “testandroid”.

Per provar el nou template de la versió de Dokuwiki “Adora Belle” cal modificar el fitxer hosts del dispositiu mòbil definit a Android Emulator :

Executem cmd a Windows.

D:
cd development\adt-bundle-windows-x86_64-20130219\sdk\tools

1) Arrenquem el dispositiu virtual Android (AVD)

emulator -avd testandroid -partition-size 256

2) Remontem la imatge del dispositiu com a writeable

cd ..
cd platform-tools

adb remount

3) Desem una copia de l'actual fitxer hosts a un directori temporal

adb pull /system/etc/hosts c:\temp

4) Afegim una línia al fitxer hosts amb la direcció IP del nostre servidor

echo 192.168.1.36 fernan.net >> c:\temp\hosts

5) Desem el nou fitxer hosts al nostre Android emulator

adb push c:\temp\hosts /system/etc

Ara podem navegar cap al nostre servidor amb el navegador d'Android. La figura següent mostra la pantalla de Dokuwiki:

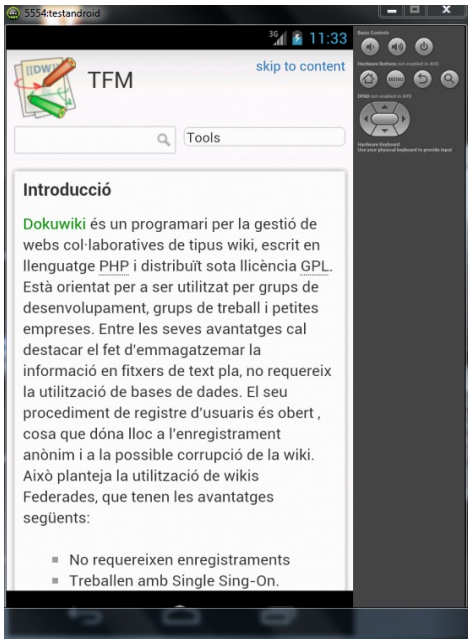

Figura 15

Prova del nou template de Dokuwiki en dispositius mòbils amb Google Chrome

Es pot provar el nou template de Dokuwiki en diferents dispositius mòbils amb el navegador Google Chrome:

1) Personaliza y configura Google Chrome >>Herramientas >> Herramientas para desarrolladores
2) Botó del fons Settings
3) Override user agent >> Android 4.0.2-Galaxxy Nexus

6.3 Documentació

Es farà referencia als manuals de Dokuwiki i simpleSAMLphp com a eines bàsiques per resoldre qualsevol incidència en la utilització de Dokuwiki i simpleSAMLphp. També, s'afegirà un document de text amb les indicacions per instal·lar el mòdul d'integració de Dokuwiki i simpleSAMLphp. D'altra banda, s'inclourà un altre fitxer de text amb les indicacions per crear un servidor OpenLDAP amb una base de dades que inclogui en el seu esquema l'objectClass eduPerson i l'overlay memberOff.

7. Implantació

La implantació d'aquest projecte ha de tenir en compte el nombre d'usuaris amb permís d'escriptura a la wiki. En el cas que aquest sigui petit es poden utilitzar els models I) o II) que estan descrits en el desenvolupament. El fet d'haver de definir un filtre core:AttributeAlter per a cadascun dels usuaris en el fitxer config.php de simpleSAMLphp , o d'haver d'editar els usuaris en el fitxer authsources.php, condiciona que el nombre d'usuaris amb dret d'escriptura o administració sigui molt petit. D'altra banda, si es vol implantar el projecte en una organització amb un nombre indeterminat d'usuaris amb dret d'escriptura caldrà utilitzar el model III). Si el servidor és OpenLDAP es poden seguir les indicacions del desenvolupament per definir el filtre ldap:AttributeAddUsersGroups. Mentre que, en el cas que l'organització utilitzi la implementació de Microsoft del protocol LDAP, Active Directory, serà suficient prendre els valors per defecte del filtre ldap:AttributeAddUsersGroups per passar al proveïdor de servei (SP) els grups definits a Active Directory.

8. Manteniment

El cicle de vida del projecte està condicionat pels canvis que es produeixin en les properes versions de Dokuwiki i simpleSAMLphp. Per tant, caldrà actualitzar periòdicament aquestes aplicacions. El procés per realitzar les actualitzacions es descriu a continuació:

Actualització de simpleSAMLphp des d'una versió prèvia

S'extreu la nova versió

```
cd /var
tar xzf simplesamlphp-1.x.y.tar.gz
```

Copio els fitxers de configuració de la versió previa

```
cd /var/simplesamlphp-1.x.y
sudo rm -rf config metadata
sudo cp -rv ../simplesamlphp/config config
sudo cp -rv ../simplesamlphp/metadata metadata
```

Reemplaço la versió antiga per la nova versió

```
cd /var
sudo mv simplesamlphp simplesamlphp.old
sudo mv simplesamlphp-1.x.y simplesamlphp
```

També cal copiar els certificats propis inclosos a la antiga versió a la nova versió

```
sudo cp /var/simolesamlphp.old/cert/saml.pem  /var/simplesamlphp/cert/saml.pem
sudo cp /var/simolesamlphp.old/cert/saml.crt  /var/simplesamlphp/cert/saml.crt
sudo cp /var/simolesamlphp.old/cert/fernan.net.pem  /var/simplesamlphp/cert/saml.pem
sudo cp /var/simolesamlphp.old/cert/fernan.net.crt  /var/simplesamlphp/cert/saml.crt
```

Actualització de Dokuwiki

1) Fer una copia de seguretat de la wiki

```
sudo cp -a /var/www/fernan.net/dokuwiki/* /var/wikibackup
```

2) Es descarrega i desempaqueta la nova versió de dokuwiki

```
cd /var/www
```

sudo tar xzvf dokuwiki-xxxx-xx-xx.tgz

3) Es copien tots els arxius sobre dokuwiki

sudo cp -rf /var/www/dokuwiki-xxxx-xx-xx/* /var/www/fernan.net/dokuwiki/

4) S'esborren els arxius vells que no s'utilitzen

5) Es comproven els permisos; inclús els de possibles nous directoris sota data/ com a index/ o tmp/

6) S'actulitzen els plugins

Annex 1. Instal·lació de Dokuwiki

```
cd /var/www
sudo wget http://www.splitbrain.org/_media/projects/dokuwiki/dokuwiki-2012-10-13.tgz
sudo tar xvf dokuwiki-2012-10-13.tgz
sudo mv dokuwiki-2012-10-13 dokuwiki
sudo chown -R www-data:www-data /var/www/dokuwiki
```

Reinicio Apache

```
sudo /etc/init.d/apache2 restart
```

A continuació accedeixo a la pàgina d'instal·lació de Dokuwiki

http://localhost/dokuwiki/install.php

Annex 2. Instal·lació de simpleSAMLphp

Faig la instal·lació en Ubuntu 12.04

Descarrego de code.google.com/p/simplesamlphp/

simplesamlphp-1.10.0.tar.gz

```
cd /var
sudo tar xzf  simplesamlphp-1.10.0.tar.gz
sudo mv simplesamlphp-1.10.0 simplesamlphp
```

Configuració d'Apache

1) sudo mkdir /var/www/fernando.net

2) Introdueixo a /etc/hosts
192.168.1.34 fernando.net

La direcció IP de l'ordinador local és 192.168.1.34

3) Creo un Virtual Host

Introdueixo al fitxer httpd.conf

```
<VirtualHost *>
        ServerName fernando.net
        DocumentRoot /var/www/fernando.net

        Alias /simplesaml  /var/simplesamlphp/www
</VirtualHost>
```

L'Alias /simplesaml pot ser qualsevol però ha d'aparèixer a config.php:

```
$config = array (
        'baseurlpath'   =>      'simplesaml/',
```

Reinicio Apache

```
sudo /etc/init.d/apache2 restart
```

Configuració de config.php

1) Contrasenya d'administrador

'auth.adminpassword' => 'novacontrasenya' ,

2) Introdueixo un “secret salt” que és una cadena aleatòria

Utilitzo el següent comandament per generar una cadena aleatòria

```
tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1
2>/dev/null;echo
```

3) Introdueixo la informació pel contacte tècnic

```
'technicalcontact_name' => 'Fernando Gil',
'technicalcontact_email' => 'fegil2@gmail.com',
```

4) Zona horària
'timezone' => 'Europe/Madrid',

Enable modules

Es crea un fitxer buit anomenat enable per habilitar els mòduls que estan instal·lats amb simpleSAMLphp, però estan deshabilitats per defecte

```
cd modules
ls -l
cd consent
sudo touch enable
```

Per deshabilitar el mòdul

```
cd modules/consent
sudo mv enable disable
```

Pàgina web de la instal·lació de simpleSAMLphp

S'accedeix a la pàgina de simpleSAMLphp introduint al navegador la direcció:

http://fernando.net/simplesaml/

Annex 3. Com crear un certificat SSL en Apache per a Ubuntu 12.04

Activar el mòdul SSL

sudo apt-get install apache2

A continuació reiniciar Apache

sudo service apache2 restart

Crear un nou directori

sudo mkdir /etc/apache2/ssl

Crear un auto signat SSL certificat

Es crea un certificat de 365 dies de validesa i es desen l'auto signat certificat i la clau que protegeix el servidor en el directori anterior.

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

Configuració del servidor

Editem el fitxer default-ssl d'Apache

sudo nano /etc/apache2/sites-available/default-ssl

En la secció <VirtualHost _default_:443> fem els canvis següents:

Darrera de la línia que inclou l'email de Server Admin escrivim el nom del servidor:

ServerName fernan.net:443

Perquè simplesamlphp es pugi connectar mitjançant SSL canviem el directori arrel i afegim el següent Alias:

DocumentRoot /var/www/fernan.net

Alias /simplesaml /var/simplesamlphp/www

Busquem i reemplacem les línies següents:

SSLEngine on
SSLCertificateFile /etc/apache2/ssl/apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache.key

Desem i sortim del fitxer.

Activació del nou Virtual Host

sudo a2ensite default-ssl

Reinicio Apache

sudo service apache2 reload

Canvi de httpd.conf

Editem httpd.conf

sudo nano /etc/apache2/httpd.conf

Canviem la primera línia del fitxer de configuració per evitar l'error “ssl_error_rx_record_too_long” que es produeix en la connexió SSL al servidor Apache

*<VirtualHost *>*
ServerName fernan.net
DocumentRoot /var/www/fernan.net

Alias /simplesaml /var/simplesamlphp/www
</VirtualHost>

El fitxer de configuració del Virtual Host queda de la manera següent:

*<VirtualHost *:80>*
ServerName fernan.net
DocumentRoot /var/www/fernan.net

Alias /simplesaml /var/simplesamlphp/www
</VirtualHost>

Reinicio Apache

sudo service apache2 restart

Annex 4. Seguretat a Dokuwiki

Per no poder accedir des de la web als directoris data, conf, bin i inc de dokuwiki afegim al fitxer de configuració d'Apache /etc/apache2/sites-available/default-ssl les directives següents:

```
<Directori /var/www/fernan.net/dokuwiki>
        order deny, allow
        allow from all
</Directori>

<LocationMatch "/dokuwiki/(data|conf|bin|inc)/">
        order allow,deny
        deny from all
        satisfy all
</LocationMatch>
```

Conclusions

El mòdul desenvolupat per Andreas Åkre Solberg permetia l'autenticació federada amb un IdP SAML 2.0 o Shibboleth 1.3 i va ser provat en les versions 1.6.2 de simpleSAMLphp i 20080505 de Dokuwiki. En el tractament de grups s'utilitzava la funció attributealter que actualment està obsoleta i es var substituir per Athentication Processing Filters. Per aquesta raó, s'han utilitzat aquests filtres en el tractament dels grups.

D'altra banda, s'havia d'indicar a Dokuwiki quan un usuari pertanyia al grup d'administradors, "admin". Això es podia fer passant els grups a Dokuwiki, a través del mòdul, des d'un fitxer on estaven definits, però tenia l'inconvenient que es creava un problema de seguretat perquè no s'utilitzava l'SP per passar la informació dels grups. Per tant, vaig decidir utilitzar un nou atribut eduPersonEntitlement per passar a Dokuwiki grups personalitzats tals com "admin".

Els filtres ldap:AttributeFromLDAP i ldap:AttributeUsersGroups van ser introduïts a les versions 1.8 i 1.9 de simpleSAMLphp, respectivament. Aquest fet em va permetre obrir una altra via en el projecte que consistia en configurar-los per passar els grups jerarquitzats en un servidor LDAP a Dokuwiki. La principal dificultat que vaig trobar va ser afegir a l'esquema de la base de dades del servidor OpenLDAP l'atribut memberOf.

Un altre aspecte que es podria tenir en compte per millorar el mòdul és afegir-hi nou codi perquè l'administració de la wiki fossi més àgil: Els grups que es passen a Dokuwiki des del servidor LDAP contenen subgrups. Si el nombre d'usuaris amb permís d'escriptura és relativament gran serà difícil per l'administrador discernir quan un subgrup té permís més feble que el grup que el conté en el mateix node de la wiki. En aquest cas el permís donat al subgrup serà redundant. Podria ser interessant modificar el mòdul perquè s'informés en un log sobre aquests permisos redundants.

Bibliografia

Dokuwiki (https://www.dokuwiki.org/)

simpleSAMLphp (http://simplesamlphp.org)

SAML (http://saml.xml.org/)

PHP Manual (http://php.net/manual/es/index.php)

PHP TUTORIAL (http://www.w3schools.com/php/)

Official Ubuntu Documentation (https://help.ubuntu.com)

OpenLDAP (http://www.openldap.org)

Internet LDIFs (https://spaces.internet2.edu/display/macedir/LDIFs)

eduPerson Object Class Specification
(http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-200806.html)

Licencias GNU (http://www.gnu.org/licenses/licenses.es.html)