Tutorial Moodle Single SignOn SAML 2.0

MoodleMoot 2018 - Milano

Marco Ferrante marco.ferrante@unige.it
Università di Genova

Agenda

- generalità del Single SignOn (SSO) SAML 2.0
- *gestione di un Service Provider*
- *metadata e servizi federati IDEM*
- *sviluppo con SimpleSAMLphp*
- Moodle e SAML
- il plugin SAML2 SSO

Single SignOn

Un sistema di Single SignOn (SSO) consente all'utente di effettuare un'unica autenticazione (authN) valida per più risorse

Non si occupa dell’autorizzazione (authZ) a cura della risorsa stessa

Ci sono meccanismi di SSO generali (Kerberos, smart card, SPNEGO, NTLMSSP) e sistemi specifici per applicazioni web

Scenario generale

L'utente si autentica presso un'*autorità* (IdP, *Authorization Server*, ...) e ottiene un *token* (o *ticket*)

L'utente poi presenta il *token* alle risorse (SP, *client*, ...) che lo valideranno e lo valuteranno per l'autorizzazione

Singole applicazioni web

Il *token* è un cookie che identifica la sessione nell'applicazione

Risposta

```
Set-Cookie:  OTRSAgentInterface=14VxxxxxQdkMiMCvxxxx; ↩
    domain=segreterie.unige.it;path=/otrs/; ↩
    expires=Tue, 04-Dec-2018 12:06:30 GMT; secure; HttpOnly
```

Richiesta successiva

```
Cookie:  OTRSAgentInterface=14VxxxxxQdkMiMCvxxxx
```

Domain o intra-organizational SSO

Il *token* è un cookie di dominio che identifica la sessione *sull'authN server*

Tipicamente un *back-channel* trasferisce i dati di sessione tra authN server e risorsa

Esempi: CAS, CoSign, Pubcookie

Autenticazione federata

Il *token* è un pacchetto XML (asserzione) legato alla sessione sull'authN server

L'asserzione viene scambiata, di solito via *front-channel*, con l'applicazione che genera una sessione locale

Esempi: SAML 1.x e 2.0, Microsoft ADFS

Shibboleth vs SAML

SAML è uno standard OASIS

Shibboleth è l'implementazione di riferimento di SAML, ma ne esistono altre: SimpleSAMLphp, Microsoft ADFS, OneLogin, Google, Authentic 2, JOSSO, PingFederate, ecc...

Tratteremo solo SAML 2.0

Riferimenti	http://xml.coverpages.org/SAML-ExecOverviewV206-11785-20050310.pdf
	https://en.wikipedia.org/wiki/SAML-based_products_and_services

Protocollo SAML 2.0

Agli inizi degli anni 2000, furono sviluppate diverse proposte di protocolli e implementazioni per autenticazione federata

- **Shibboleth 1.x** da parte del progetto Internet 2
- **SAML 1.0** OASIS Security Services Technical Committee
- **Liberty Identity Federation** consorzio Liberty Alliance

Nel 2005 sono confluite nello standard OASIS SAML 2.0

Adottare SAML 2.0 per il SSO intra-organizzazione ha come beneficio collaterale l'autenticazione federata

SAML 2.0 permette di integrare servizi di terzi in modo standard, senza passaggio di credenziali e con un controllo fine sulle informazioni trasmesse

IdP UniGe maggio 2017

Value	Data range
391025	All services
252979	AulaWeb, servizio e-learning
119428	https://servizionline.unige.it/
3132	Servizio di hosting UniGE
2302	READY - SAL
1917	SciuMegu ‹‹‹‹‹‹
1916	https://moodle3.aulaweb.unige.it/
1550	Servizi online UniGE
1470	https://unigepass.unige.it/sp
996	Siti federati UniGE
872	Siti di servizio UniGE
846	Elsevier ScienceDirect ‹‹‹‹‹‹
801	https://esami.aulaweb.unige.it/sp
765	https://ssounige.sbgnet.it/shibboleth
497	eduOpen MOOC Italy
238	Thomson Reuters
173	Servizio di liste UniGe
169	Sito DICCA
121	SheerID Verification Services
92	FileSender GARR
85	DreamSpark, e-academy WebStore erogato da e-academy, Inc
78	IEEE XploreDigital Library provided by IEEE
78	UNiDAYS
67	Incassi On Line
67	Nilde Utenti erogato da Biblio Area CNR Bologna
45	Compilatio - Prévention du plagiat
32	Siti web Dipartimento di Fisica (DIFI)
30	https://intranet.unige.it/sp
28	WiFi UniTO erogato da Università degli Studi di Torino

25	SpringerLink by Springer-Verlag London, Ltd.
23	https://vm-fad2.ker.csita.unige.it/
22	Società editrice il Mulino SP
19	Nature Publishing Group journals
19	Semantico Limited - OUP Shibboleth 2 SP
17	Atypon SP
14	ProQuest
12	ORCID
12	https://esami.aulaweb.unige.it /shibboleth
12	OVID SP
10	Cambridge Journals Online
9	Elearning U-GOV
8	Student Beans
7	Sito Web IDEM - https://www.idem.garr.it
7	ACS Publications
6	http://servizionline.unige.it
5	RSC Publishing
5	Bestr - Piattaforma Open Badge
4	Annual Reviews
4	Project MUSE provided by The Johns Hopkins University Press
3	Foodle
2	ACM Digital Library provided by ACM
2	Università di Genova
1	Learning GARR
1	GÉANT Trusted Certificate Service (TCS)
1	https://moodle-esterni.aulaweb.unige.it/
1	https://aulaweb.unige.it/test31

Attori

Subject
: ciò di cui parla l'asserzione

Service Provider (SP)
: controlla l'accesso a una risorsa

  gestito dal fornitore del servizio

Identity Provider (IdP)
: fornisce le asserzioni

  gestito dalla *home organization*

Relying party (RP)
: un sistema che riceve e trasmette informazioni SAML

Attribute Autority (AA)
: rilascia gli attributi

  spesso coincide con l'IdP

WAYF o Discovery Service
: media tra il SP e l'utente per determinare l'IdP

  integrato nel servizio o gestito dalla federazione

Servizi

Ogni componente fornisce dei *servizi*, caratterizzati da:

Binding
: il protocollo (SOAP, POST, ecc...) con cui utilizzarli

Location
: endpoint (URL) con cui si accede al servizio

Profili

Un *profilo* specifica come un'applicazione usa i formati, i protocolli, i messaggi e i *binding* SAML

Profilo

combinazione di *binding* e elementi *core* associata a uno specifico *use-case*

Binding

protocollo di accesso a un servizio

Core

formato messaggi e protocolli richiesta/risposta

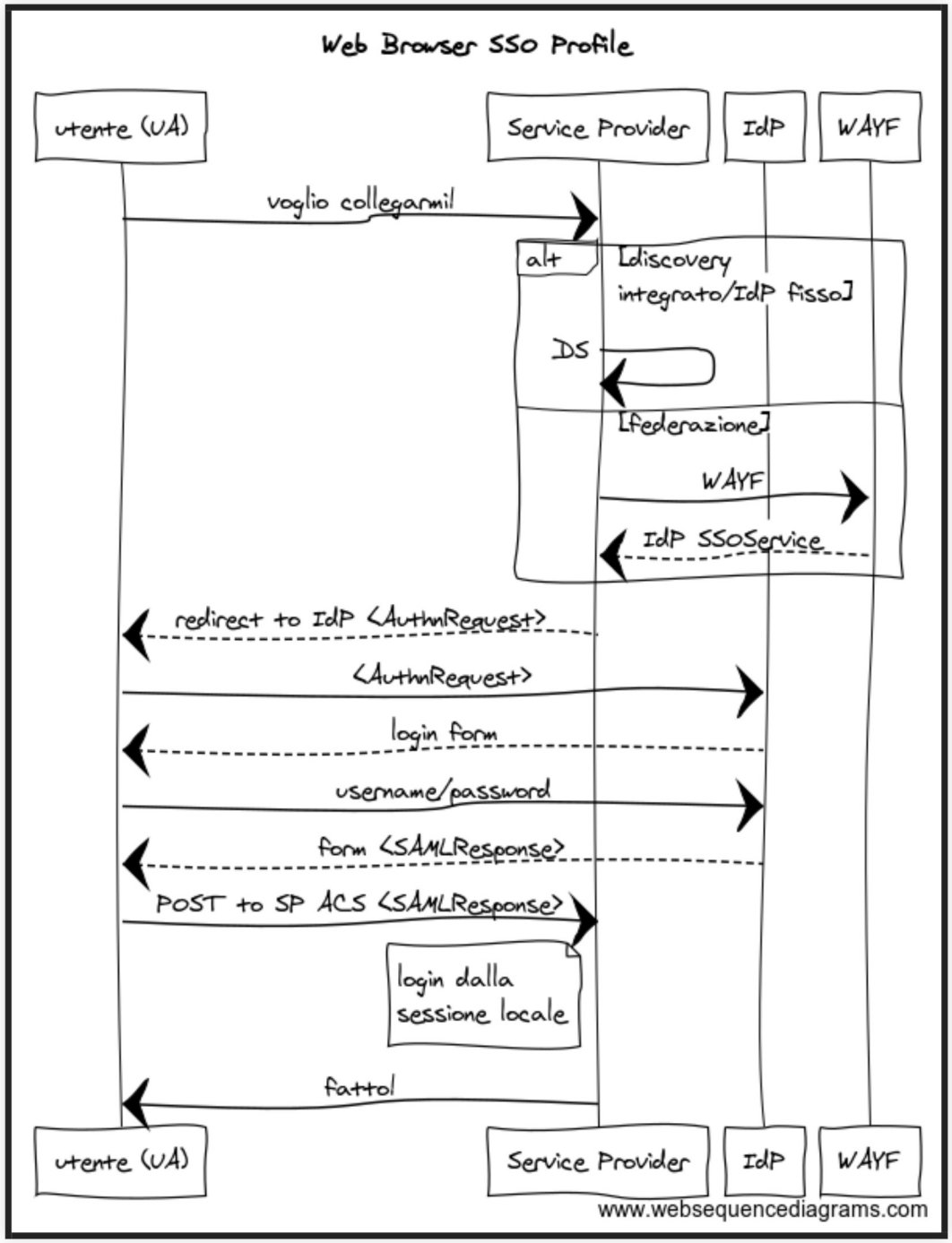
Esempi di Profili

- Web Browser SSO Profile
- Enhanced Client or Proxy (ECP) Profile
- Identity Provider Discovery Profile
- Single Logout Profile
- Name Identifier Management Profile
- Holder-of-Key (HoK) Web Browser SSO Profile
- ...

SAML2Int

Il profilo Interoperable SAML 2.0 Profile (SAML2Int) è una raccomandazione di comportamenti e opzioni per il deploy di un servizio WebSSO orientata alla massima interoperabilità

Supportato da Feide (Norvegia), Haka (Finlandia), eduGAIN (Geant), RedIRIS (Spagna), e altre RENs


Web Browser SSO Profile
utente (UA)
Service Provider
IdP
WAYF
voglio collegarmi!
alt
[discovery integrato/IdP fisso]
DS
[federazione]
WAYF
IdP SSOService
redirect to IdP <AuthnRequest>
<AuthnRequest>
login form
username/password
form <SAMLResponse>
POST to SP ACS <SAMLResponse>
login dalla sessione locale
fatto!
utente (UA)
Service Provider
IdP
WAYF
www.websequencediagrams.com

Comunicazioni

Le comunicazioni passano dal *front-channel*

C'è una tolleranza di circa 5 minuti tra i sistemi

Sincronizzate gli orologi! :-)

L'utente 'vede' il traffico

- usare sempre HTTPS
- i messaggi possono essere firmati e/o cifrati

*-first

Il 'minuetto' di autenticazione può essere iniziato da diversi attori

IdP-first/-initiated
l'UA accede all'IdP con un eventuale parametro tipo spentityId
l'IdP rimanda all'SP all'URL o al SP specificato

SP-first/-initiated
il SP redirige all'IdP con un messaggio di `AuthnRequest`
l'IdP rimanda all'SP con una token contenente un'asserzione

Asserzioni

'in un certo istante questo IdP asserisce che per un determinato soggetto valgono questi attributi'

Ha forma di un pacchetto XML comprendente:

- Issuer: entityId che ha rilasciato l'asserzione
- firme e chiavi
- Subject: l'oggetto dell'asserzione
- Conditions: condizioni di validità dell'asserzione
- AuthnStatement: le circostanze di autenticazione
- AttributeStatement: elenco degli attributi del soggetto

Issuer

```
<saml:Assertion
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        ID="_d5a64ffca10a1098db9e83ee90a9a696f6dfb5d48f"
        Version="2.0"
        IssueInstant="2017-09-20T07:10:21Z">
  <saml:Issuer>https://unigepass.unige.it/idp</saml:Issuer>
  ...
</saml:Assertion>
```

Firme e chiavi

```
...
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
                Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"...
  </ds:SignedInfo>
  <ds:SignatureValue
        iaw9oFF4A9LNcpk8isjnexUh...
  <ds:KeyInfo>
    <ds:X509Data>
         <ds:X509Certificate>MIIDXjCCAkYCCQD...
...
```

Subject

```
...
<saml:Subject>
  <saml:NameID
      SPNameQualifier="https://vm.csita.unige.it/"
          Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">↩
                 _ca04214ebdb2c...d
          </saml:NameID>
        <saml:SubjectConfirmation
            Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
          <saml:SubjectConfirmationData
            NotOnOrAfter="2017-09-20T07:15:21Z"
                Recipient="https://valido.aulaweb.unige.it/simplesaml/↩
                    module.php/saml/sp/saml2-acs.php/UniGePASS"
                InResponseTo="_1596ffb37ce5..."/>
```

NameID

Identificativo del soggetto, può avere diverse forme:

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
l'interpretazione è un accordo tra IdP e SP

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
ovvio

urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
persistente tra sessioni, opaco, differente da SP e SP

urn:oasis:names:tc:SAML:2.0:nameid-format:transient
di sessione, opaco e differente da SP e SP

Riferimenti https://wiki.shibboleth.net/confluence/display/CONCEPT/NameIdentifiers

NameID e attributi

Il NameID serve ai relying party per correlare i messaggi, ma non è necessario per le retrostanti applicazioni. Tipicamente, Shibboleth e le federazioni RENs identificano il soggetto con un attributo

entryDN (o altro nome custom)
DN LDAP o del certificato X.509, uso interno

eduPersonPrincipalName (eppn)
`<identificativo>@<organizzazione>`

eduPersonTargetedID (ePTID)
`<organizzazione>!<servizio>!<stringa opaca>`

mail

Riferimenti Specifiche tecniche per la compilazione e l'uso degli Attributi IDEM GARR

Conditions

```
...
<saml:Conditions
    NotBefore="2017-09-20T07:09:51Z"
        NotOnOrAfter="2017-09-20T07:15:21Z">
  <saml:AudienceRestriction>
    <saml:Audience>https://vm.csita.unige.it/</saml:Audience>
...
```

`Audience` è un entityId, non l'URL del servizio

AuthnStatement

```
...
<saml:AuthnStatement
    AuthnInstant="2017-09-20T07:09:12Z"
        SessionNotOnOrAfter="2017-09-20T15:09:12Z"
        SessionIndex="_5b594bc61778598703b25364ce8e53f10ad1d203f4">
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>↩
        urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport↩
        </saml:AuthnContextClassRef>
...
```

AttributeStatement

```
...
<saml:AttributeStatement>
  <saml:Attribute FriendlyName="mail"
      Name="urn:oid:0.9.2342.19200300.100.1.3"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    ...
  </saml:Attribute>
  <saml:Attribute ...>
  </saml:Attribute>
  <saml:Attribute ...>
  ...
```

Attribute

```
...
  <saml:Attribute FriendlyName="mail"
      Name="urn:oid:0.9.2342.19200300.100.1.3"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue xsi:type="xs:string">↩
            marco@csita.unige.it</saml:AttributeValue>
    <saml:AttributeValue xsi:type="xs:string">↩
            ferrante@csita.unige.it</saml:AttributeValue>
...
```

Gli attributi ammettono valori multipli

NameFormat

urn:oasis:names:tc:SAML:2.0:attrname-format:uri
OID LDAP o URN mace: o URL
urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
come dice il nome...
urn:oasis:names:tc:SAML:2.0:attrname-format:basic
nomi LDAP

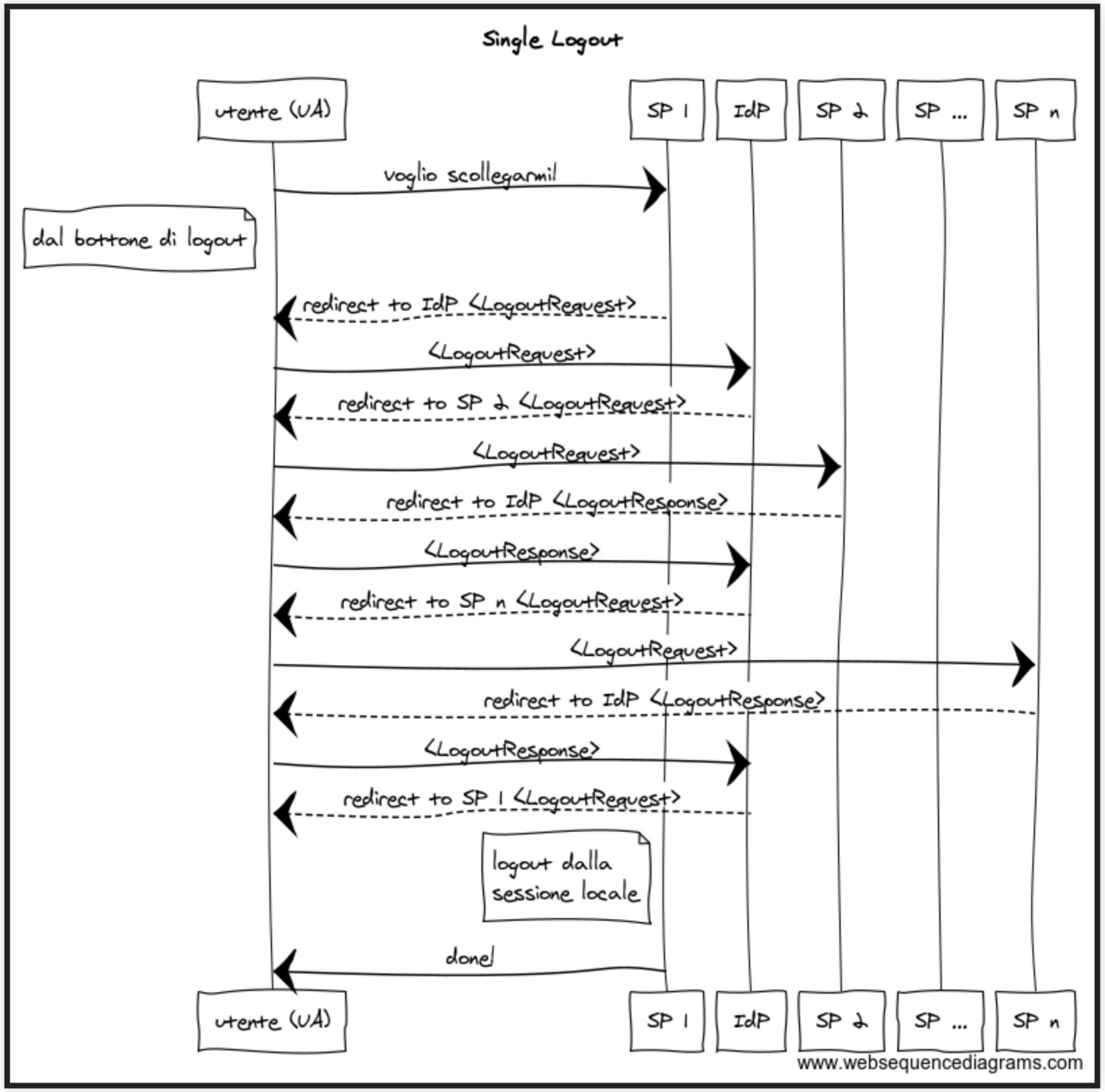
Single Logout (SLO)

Il Single Logout è controintuitivo per gli utenti, sia per l'uso del *front-channel* sia per le applicazioni con sessioni proprie

- si disconnette da un servizio e, se va tutto bene, si trova disconnesso da tutti
- oppure si ritrova con una sessione *zombie* locale
- oppure riceve un errore da un servizio che non ricorda di aver aperto
- o altro ancora...

L'unico meccanismo di SLO affidabile è la chiusura del browser

Riferimenti SWITCH Shibboleth SP Logout Support - Shibboleth Training 2015


Single Logout
utente (UA)
SP 1
IdP
SP 2
SP ...
SP n
voglio scollegarmi!
dal bottone di logout
redirect to IdP <LogoutRequest>
<LogoutRequest>
redirect to SP 2 <LogoutRequest>
<LogoutRequest>
redirect to IdP <LogoutResponse>
<LogoutResponse>
redirect to SP n <LogoutRequest>
<LogoutRequest>
redirect to IdP <LogoutResponse>
<LogoutResponse>
redirect to SP 1 <LogoutRequest>
logout dalla sessione locale
done!
utente (UA)
SP 1
IdP
SP 2
SP ...
SP n
www.websequencediagrams.com

Partial Logout

Se l'IdP non riesce ad avere conferma del logout da tutti i servizi, presenta un errore di 'Partial Logout'

Il Service Provider

Un *Service Provider* SAML (SP) è un relying party che consuma asserzioni SAML

In pratica, controlla gli accessi ad una risorsa in base alle asserzioni fornite da un IdP

Spesso è indicato come SP il componente software (libreria o modulo) che gestisce il protocollo SAML per fornire informazioni ad una retrostante applicazione

Metadata

Come fanno IdP e SP a 'conoscersi'? Si scambiano i *metadata*

- ogni attore è identificato da un *EntityID* (un URI nel namespace dell'organizzazione)
- informazioni di contorno per l'utente (nome del servizio, contatti, loghi, ecc...)
- chiavi crittografiche (pubbliche :-) e loro uso
- il formato di nomi supportato (NameIDFormat)
- per IdP: binding e location dei servizi supportati SSO, SLO, Artifact Resolution, AA, ecc...
- per SP: binding e location dei servizi supportati ACS, SLO, Artifact Resolution, ecc...

Esempi metadata

- IdP Università Politecnica delle Marche
- SP Wiki IDEM

Metadata: gestione e scambio

Gestione e scambio dei metadata all'interno di un'organizzazione può essere manuale dove:

- un solo IdP e molti SP
- i metadata degli SP sono conservati in file XML
- i metadata sono scambiati via mail, sharing, ecc...
- la fiducia è basata sulla conoscenza degli interlocutori.

Funziona, ma non scala ed è una modalità di gestione utilizzabile solo all'interno di un'unica organizzazione.

Metadata: fiducia

Lo scambio di metadata stabilisce relazioni di fiducia

Per gli IdP:

- Utilizzare i servizi di autenticazione di un'organizzazione (l'IdP).
- Ricevere gli attributi di un utente di un'organizzazione.

Per gli SP:

- Permettere l'uso del servizio agli utenti di una organizzazione.
- Ricevere dati autoritativi sugli utenti (ad. es. affiliazione).

Metadata: federazione

Quando si esce dai confini di un'organizzazione la fiducia non si può più basare solo sui rapporti tra gli interlocutori, serve una terza parte fidata

Le *federazioni* hanno esattamente questo scopo

Per gli enti GARR è attiva la federazione IDEM

Integrare il SSO SAML nelle applicazioni

applicazione

nuova: può usare una libreria generica di autenticazione che comprenda SAML

esistente: deve far inizializzare la sessione dell'applicazione da un'asserzione dell'IdP

configurazione

gestita da sistema

integrata nell'applicazione/plugin

contesto SSO

intra-organizzazione presumendo il controllo sull'IdP

federato con IdP multipli

Gestione autenticazione

dal web server/container

un modulo del server è incaricato di gestire tutta la negoziazione SAML e passa all'applicazione le asserzioni pre-elaborate come variabili CGI

da applicazioni/librerie

l'applicazione usa, a vari livelli, una libreria che gestisce il processo di autenticazione

Esempi autenticazione da container

Shibboleth Native Service Provider (SP)

mod_auth_mellon

modulo Apache con un semplice SAML 2.0 service provider
https://github.com/UNINETT/mod_auth_mellon

Spring Security SAML

componenti e filter per servlet container Java
http://projects.spring.io/spring-security-saml/

Esempi autenticazione da applicazioni

SimpleSAMLphp
- a dopo...

Onelogin
- librerie per PHP, Python, Ruby, Java, .NET
- https://developers.onelogin.com/saml

PySAML2
- Python
- http://pysaml2.readthedocs.io/

Esempi altre possibilità

Auth0

Servizio *cloud* che gestisce anche il protocollo SAML (chiamato SAMLP)
https://auth0.com/docs/connections/enterprise/samlp

SATOSA

proxy tra SAML 2.0 e SAML2, OpenID Connect, Google, Facebook
https://github.com/SUNET/SATOSA

SAML2 SSO

Panoramica

Sviluppo iniziato da Daniel Miranda allora all'Università di Belo Horizonte (BRA)

Al momento, Università di Genova è co-mantainer su GitHub

Usa direttamente l'installazione di SimpleSAMLphp di sistema

Caratteristiche

Configurazione SAML unica per tutte le istanze Moodle sullo stesso host

Sincronizza gli utenti con altri backend

Può importare gli utenti di plugin obsoleti (e non...)

Non solo SAML: Facebook, LinkedIn, Twitter, LDAP avanzato e LDAP DIT, file .htpasswd, ecc...

Completamente tradotto in italiano

Installazione

```
$ wget https://github.com/dmirandaa/moodle-auth_saml2sso/archive/master.zip
$ unzip master.zip
$ mv moodle-auth_saml2sso-master /opt/moodle/auth/auth_saml2sso
```

poi aggiornare il db di Moodle e verificare le impostazioni con "Test settings"

Don't panic

Con errori di configurazione dei plugin di autenticazione è possibile 'chiudersi fuori' da Moodle.
È prevista una via d'accesso d'emergenza:
`/login/index.php?saml=off`

Impostazioni generali

Percorso librerie SimpleSAMLphp `sp_path`
Se SSP è stato installato come indicato prima, lo trova da solo.
Specificare altrimenti o se si vogliono usare istanze diverse

Nome sorgente autenticazione SP `authsource`
l'authsource definita in `ssp/config/autsources.php`

Single Sign Off `single_signoff`
ne parliamo dopo...

URL di logout `logout_url_redir`
URL a cui ridirigere dopo il logout se diverso dalla home

Autenticazione varia

Non necessariamente si autentica verso un IdP SAML: può essere usato per configurazione LDAP avanzate (es. multi DIT), per Facebook, ecc...

/var/simplesamlphp/authsources.php

```
'facebook' => array(
    'authfacebook:Facebook',
    'api_key' => '1111111111',
    'secret' => 'esicheveladico',
),
```

Impostazioni utente

Attributo nome utente `idpattr`

L'attributo ricevuto dall'IdP da usare come `Username`. Deve essere univoco, rispettare le regole di Moodle e verrà convertito in minuscolo. Ad esempio `eppn`, `uid` o `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn`.

~~**Campo identificativo `moodle_mapping`**~~

~~La "chiave" utente. Sono possibili `Username`, `Indirizzo mail`~~ **o** ~~`Codice identificativo`~~ MDL-64287 e Issue #27

Sul logout

È difficile disattivare il Single SignOff (Single LogOut o SLO) perché, se esiste una sessione sull'IdP, riaprendo Moodle si verrà automaticamente ricollegati.

esempio

Ipotesi: forzare il Remote Login in ogni sessione?

Login multiplo

Il plugin intercetta e previene la maschera di login, quindi non vengono invocati gli altri plugin nell'ordine del pannello di configurazione

Dual login `dual_login`
: Se 'sì', appare la maschera di login e l'utente deve scegliere SAML2 SSO tra gli IdP

URL icona `button_url`

Etichetta bottone `button_name`
: Nome e icona del bottone IdP di SAML2 SSO

Sincronizzazione utenti

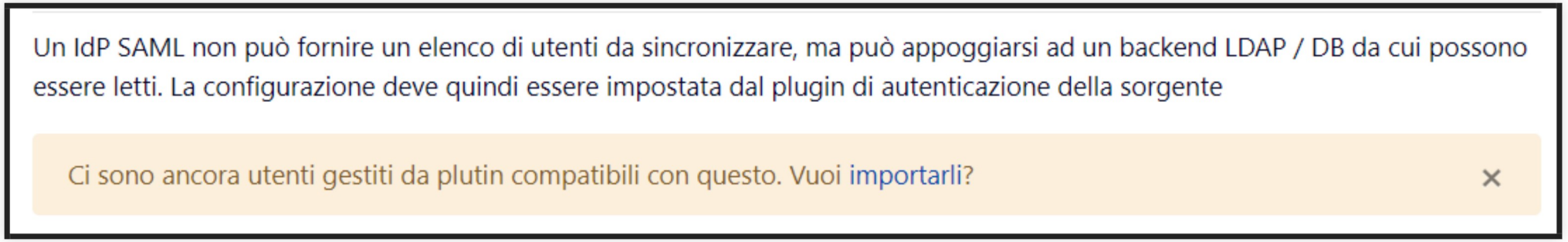
Si possono sincronizzare gli utenti da altri backend (LDAP o Database) configurando il relativo plugin

Gli utenti gestiti da altri plugin possono essere importati *una tantum*

Origine utenti `user_directory`

Il backend, la sincronizzazione si gestisce come un'operazione pianificata (Scheduled Task)

Pagina migrazione



Nascondi pagina di importazione `hide_takeover_page`
per non farsi più annoiare...

Attributi SAML e profilo utente

Oltre la mappatura standard di Moodle.

L'utente può modificarsi il profilo? `edit_profile`

Accetta email nulle `allow_empty_email`

Alcuni IdP non forniscono gli indirizzi oppure l'utente non ne ha uno associato. L'utente dovrà completare il profilo

~~**Nome completo dall'IdP?, Attributo IdP del nome, Attributo IdP del cognome**~~

deprecati

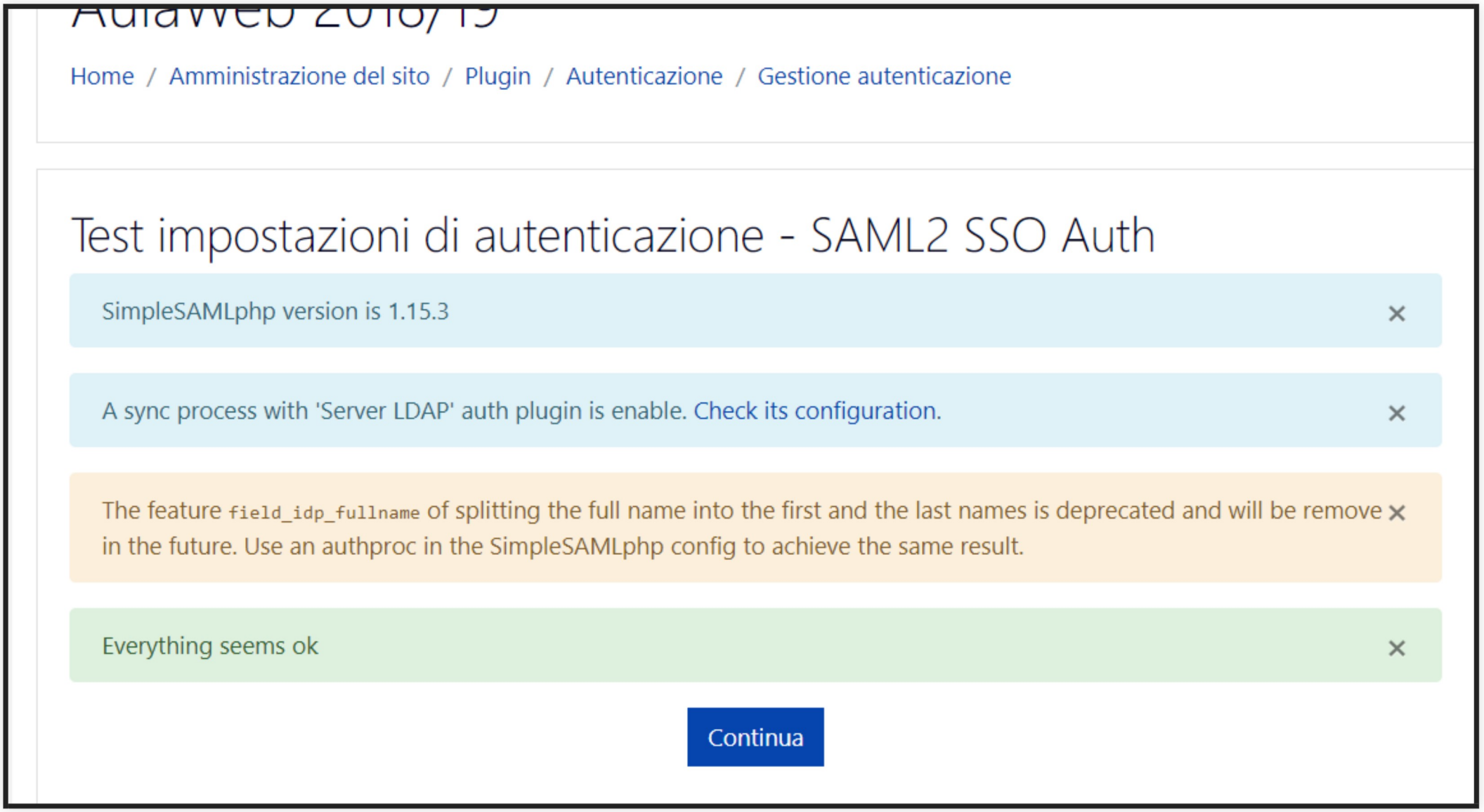
Split del nome

Ammesso che qualche IdP fornisca solo il `cn`...

```
/var/simplesamlphp/authsources.php
'authproc' => array(
    15 => array(
        'class' => 'core:AttributeAlter',
        'subject' => 'urn:oid:2.5.4.3',
        'pattern' => '/^([^\\s]+)/',
        'target' => 'givenName',
        '%replace',
    ),
    16 => array(
        'class' => 'core:AttributeAlter',
        'subject' => 'urn:oid:2.5.4.3',
        'pattern' => '/([^\\s]+)$/',
        'target' => 'sn',
        '%replace',
    )
```

Riferimenti https://simplesamlphp.org/docs/stable/simplesamlphp-authproc

/auth/test_settings.php?auth=saml2sso



Metadata per virtual host

Il problema di fornire i metadata all'IdP in caso di istanze multiple di Moodle rimane aperto

Moodle e SAML 2.0 SSO

Panoramica

Out-of-the-box Moodle supporta diversi sistemi di SSO:

- CAS
- LDAP con NTLM
- OAuth 2
- **Shibboleth**

Plugin SAML 2.0

SAML2 Single sign on `auth_saml2`
basato su simpleSAMLphp, single-tenant, configurazione da amministrazione

`auth_saml2sso`
ne parliamo dopo...

`auth_onelogin_saml`
https://github.com/onelogin/moodle-saml
basato su OneLogin, single-tenant, configurazione da amministrazione, fermo alla versione 2.1

miniOrange, SSOeasy, ...
poco usate, freemium, datate, *ad-hoc*

Obsoleti

auth_saml
: basato su simpleSAMLphp, gestisce l'enrollment, multi-tenant, fermo alla versione 3.2

auth_onelogin_saml
: basato su OneLogin, single-tenant, configurazione da amministrazione, fermo alla versione 2.1

auth_zilink_saml
: obsoleto e specializzato

Segnaliamo

auth_samlidp
trasforma Moodle in un IdP
bridge HTTP-Basic Auth
per usare mod_mellon o simili

Shibboleth: pro

- supporto nativo Moodle
- protegge risorse generiche Apache
- usabile a livello di reverse-proxy

Shibboleth: contro

- configurazione (complessa) a livello di sistema
- non può sfruttare le competenze in PHP
- richiede un demone long-running
- collassa tutti i valori in una stringa separata da "`;`"

Filtro su attributi

```
<attributefilterpolicy id="example1">
  <policyrequirementrule xsi:type="Requester" value="https://sp.example.org">
  <attributerule attributeid="eduPersonPrincipalName">
    <permitvaluerule xsi:type="Value" value="jsmith" ignorecase="true">
  </permitvaluerule></attributerule>
</policyrequirementrule></attributefilterpolicy>
```

Filtro Script

```
<attributerule attributeid="email">
    <permitvaluerule xsi:type="Script">
        <script>
        <![CDATA[
            hashSetType = Java.type("java.util.HashSet");
            result = new hashSetType();
            result.add(attribute.getValues().iterator().next());
            result;
        ]]>
        </script>
    </permitvaluerule>
</attributerule>
```

Plugin SAML in PHP

Molti plugin per SAML usano altre librerie SAML

- usi più generali
- può integrare in Moodle la configurazione dell'SP
- le richieste sono indipendenti tra loro

Librerie SAML PHP

- SimpleSAMLphp
- ONE Login
- ...

SAML2 Single sign on `auth_saml2`

Catalyst IT Australia https://www.catalyst-au.net/

- https://github.com/catalyst/moodle-auth_saml2/issues
- 775 siti (al 30/11/2018)
- **54 issues** (al 30/11/2018)
- SimpleSAMLphp embedded (v1.15.4)

auth_saml2

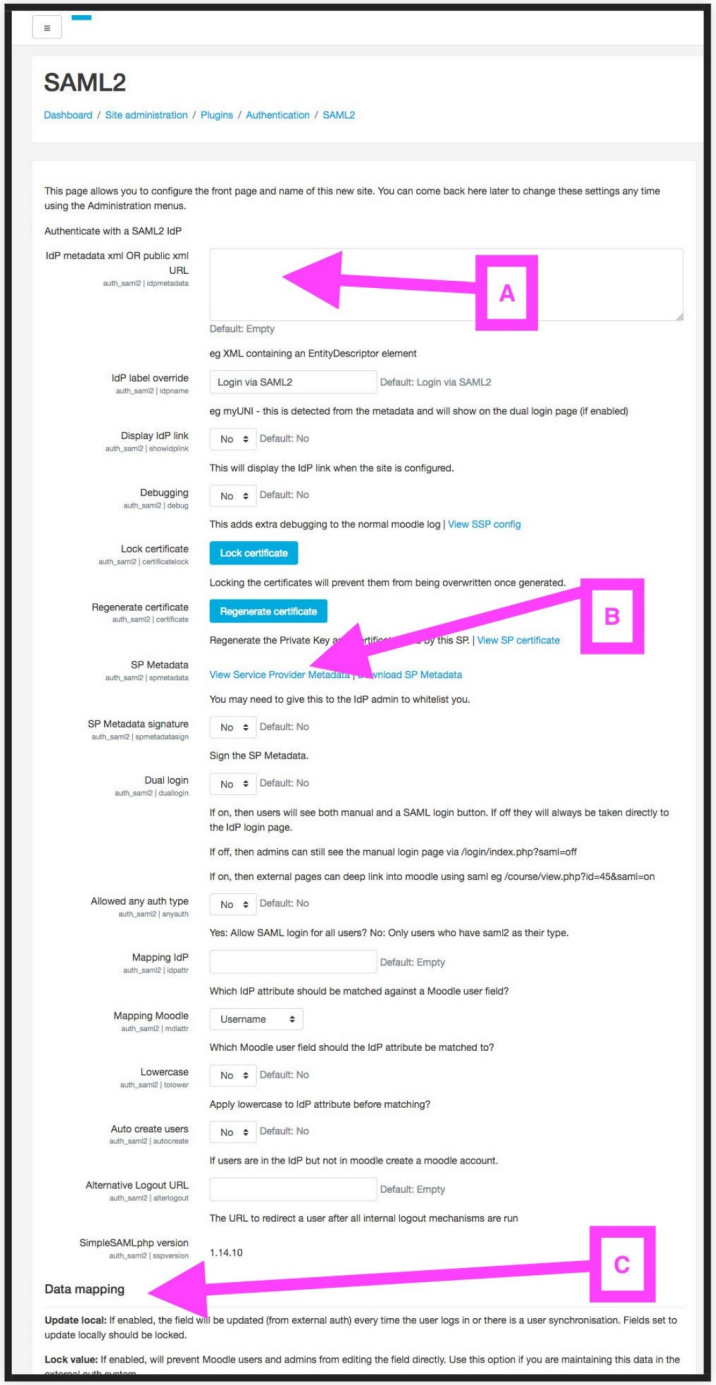
dalla descrizione ufficiale:

- 100% configured in the Moodle GUI - no installation of a whole separate app, and no touching of config files or generating certificates
- Minimal configuration needed, in most cases just copy the IdP metadata in and then give the SP metadata to your IdP admin and that's it
- Fast! - 3 redirects instead of 7
- Supports back channel Single Logout which most big organisations require (unlike OneLogin)

auth_saml2

dalla descrizione ufficiale:

- Dual login VS forced login for all as an option, with ?saml=off on the login page for manual accounts, and ?saml=on supported everywhere to deep link and force login via saml if dual auth is on
- SAML attributes to Moodle user field mapping
- Automatic certificate creation
- Optionally auto create users


SAML2
Dashboard / Site administration / Plugins / Authentication / SAML2
This page allows you to configure the front page and name of this new site. You can come back here later to change these settings any time using the Administration menus.
Authenticate with a SAML2 IdP
IdP metadata xml OR public xml URL
auth_saml2 | idpmetadata
A
Default: Empty
eg XML containing an EntityDescriptor element
IdP label override
auth_saml2 | idpname
Login via SAML2
Default: Login via SAML2
eg myUNI - this is detected from the metadata and will show on the dual login page (if enabled)
Display IdP link
auth_saml2 | showidplink
No
Default: No
This will display the IdP link when the site is configured.
Debugging
auth_saml2 | debug
No
Default: No
This adds extra debugging to the normal moodle log | View SSP config
Lock certificate
auth_saml2 | certificatelock
Lock certificate
Locking the certificates will prevent them from being overwritten once generated.
Regenerate certificate
auth_saml2 | certificate
Regenerate certificate
B
Regenerate the Private Key a
by this SP. | View SP certificate
SP Metadata
auth_saml2 | spmetadata
View Service Provider Metadata
Download SP Metadata
You may need to give this to the IdP admin to whitelist you.
SP Metadata signature
auth_saml2 | spmetadatasign
No
Default: No
Sign the SP Metadata.
Dual login
auth_saml2 | duallogin
No
Default: No
If on, then users will see both manual and a SAML login button. If off they will always be taken directly to the IdP login page.
If off, then admins can still see the manual login page via /login/index.php?saml=off
If on, then external pages can deep link into moodle using saml eg /course/view.php?id=45&saml=on
Allowed any auth type
auth_saml2 | anyauth
No
Default: No
Yes: Allow SAML login for all users? No: Only users who have saml2 as their type.
Mapping IdP
auth_saml2 | idpattr
Default: Empty
Which IdP attribute should be matched against a Moodle user field?
Mapping Moodle
auth_saml2 | mdlattr
Username
Which Moodle user field should the IdP attribute be matched to?
Lowercase
auth_saml2 | tolower
No
Default: No
Apply lowercase to IdP attribute before matching?
Auto create users
auth_saml2 | autocreate
No
Default: No
If users are in the IdP but not in moodle create a moodle account.
Alternative Logout URL
auth_saml2 | alterlogout
Default: Empty
The URL to redirect a user after all internal logout mechanisms are run
SimpleSAMLphp version
auth_saml2 | sspversion
1.14.10
C
Data mapping
Update local: If enabled, the field will be updated (from external auth) every time the user logs in or there is a user synchronisation. Fields set to update locally should be locked.
Lock value: If enabled, will prevent Moodle users and admins from editing the field directly. Use this option if you are maintaining this data in the

auth_onelogin_saml

Molto simile a `auth_saml2` ma basato su librerie OneLogin
Il mantainer principale principale lavorava con SimpleSAMLphp

SAML2 SSO

Panoramica

Sviluppo iniziato da Daniel Miranda allora all'Università di Belo Horizonte (BRA)

Al momento, Università di Genova è co-mantainer su GitHub

Usa direttamente l'installazione di SimpleSAMLphp di sistema

Caratteristiche

Configurazione SAML unica per tutte le istanze Moodle sullo stesso host

Sincronizza gli utenti con altri backend

Può importare gli utenti di plugin obsoleti (e non...)

Non solo SAML: Facebook, LinkedIn, Twitter, LDAP avanzato e LDAP DIT, file .htpasswd, ecc...

Completamente tradotto in italiano

Installazione

```
$ wget https://github.com/dmirandaa/moodle-auth_saml2sso/archive/master.zip
$ unzip master.zip
$ mv moodle-auth_saml2sso-master /opt/moodle/auth/auth_saml2sso
```

poi aggiornare il db di Moodle e verificare le impostazioni con "Test settings"

Don't panic

Con errori di configurazione dei plugin di autenticazione è possibile 'chiudersi fuori' da Moodle.
È prevista una via d'accesso d'emergenza:
`/login/index.php?saml=off`

Impostazioni generali

Percorso librerie SimpleSAMLphp `sp_path`
Se SSP è stato installato come indicato prima, lo trova da solo.
Specificare altrimenti o se si vogliono usare istanze diverse

Nome sorgente autenticazione SP `authsource`
l'authsource definita in `ssp/config/autsources.php`

Single Sign Off `single_signoff`
ne parliamo dopo...

URL di logout `logout_url_redir`
URL a cui ridirigere dopo il logout se diverso dalla home

Autenticazione varia

Non necessariamente si autentica verso un IdP SAML: può essere usato per configurazione LDAP avanzate (es. multi DIT), per Facebook, ecc...

/var/simplesamlphp/authsources.php

```
'facebook' => array(
    'authfacebook:Facebook',
    'api_key' => '1111111111',
    'secret' => 'esicheveladico',
),
```

Impostazioni utente

Attributo nome utente `idpattr`

L'attributo ricevuto dall'IdP da usare come `Username`. Deve essere univoco, rispettare le regole di Moodle e verrà convertito in minuscolo. Ad esempio `eppn`, `uid` o `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn`.

~~**Campo identificativo `moodle_mapping`**~~

~~La "chiave" utente. Sono possibili `Username`, `Indirizzo mail`~~ **o** ~~`Codice identificativo`~~ MDL-64287 e Issue #27

Sul logout

È difficile disattivare il Single SignOff (Single LogOut o SLO) perché, se esiste una sessione sull'IdP, riaprendo Moodle si verrà automaticamente ricollegati.

esempio

Ipotesi: forzare il Remote Login in ogni sessione?

Login multiplo

Il plugin intercetta e previene la maschera di login, quindi non vengono invocati gli altri plugin nell'ordine del pannello di configurazione

Dual login `dual_login`
: Se 'sì', appare la maschera di login e l'utente deve scegliere SAML2 SSO tra gli IdP

URL icona `button_url`

Etichetta bottone `button_name`
: Nome e icona del bottone IdP di SAML2 SSO

Sincronizzazione utenti

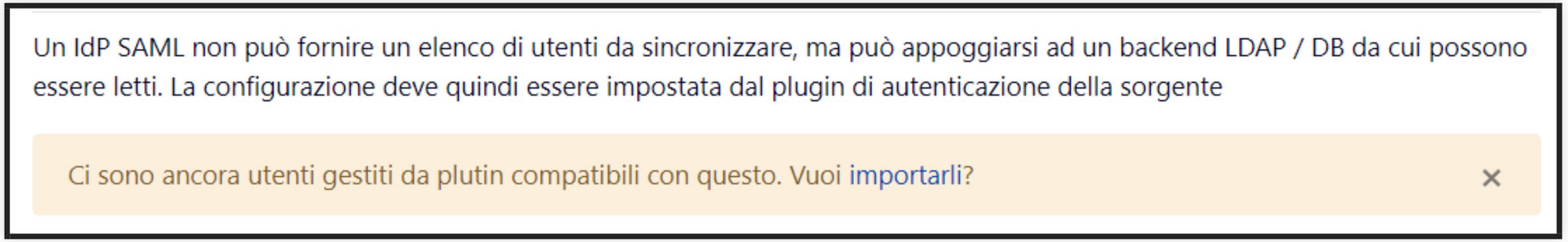
Si possono sincronizzare gli utenti da altri backend (LDAP o Database) configurando il relativo plugin

Gli utenti gestiti da altri plugin possono essere importati *una tantum*

Origine utenti `user_directory`

Il backend, la sincronizzazione si gestisce come un'operazione pianificata (Scheduled Task)

Pagina migrazione



Nascondi pagina di importazione `hide_takeover_page`
per non farsi più annoiare...

Attributi SAML e profilo utente

Oltre la mappatura standard di Moodle.

L'utente può modificarsi il profilo? `edit_profile`

Accetta email nulle `allow_empty_email`

Alcuni IdP non forniscono gli indirizzi oppure l'utente non ne ha uno associato. L'utente dovrà completare il profilo

~~**Nome completo dall'IdP?, Attributo IdP del nome, Attributo IdP del cognome**~~

deprecati

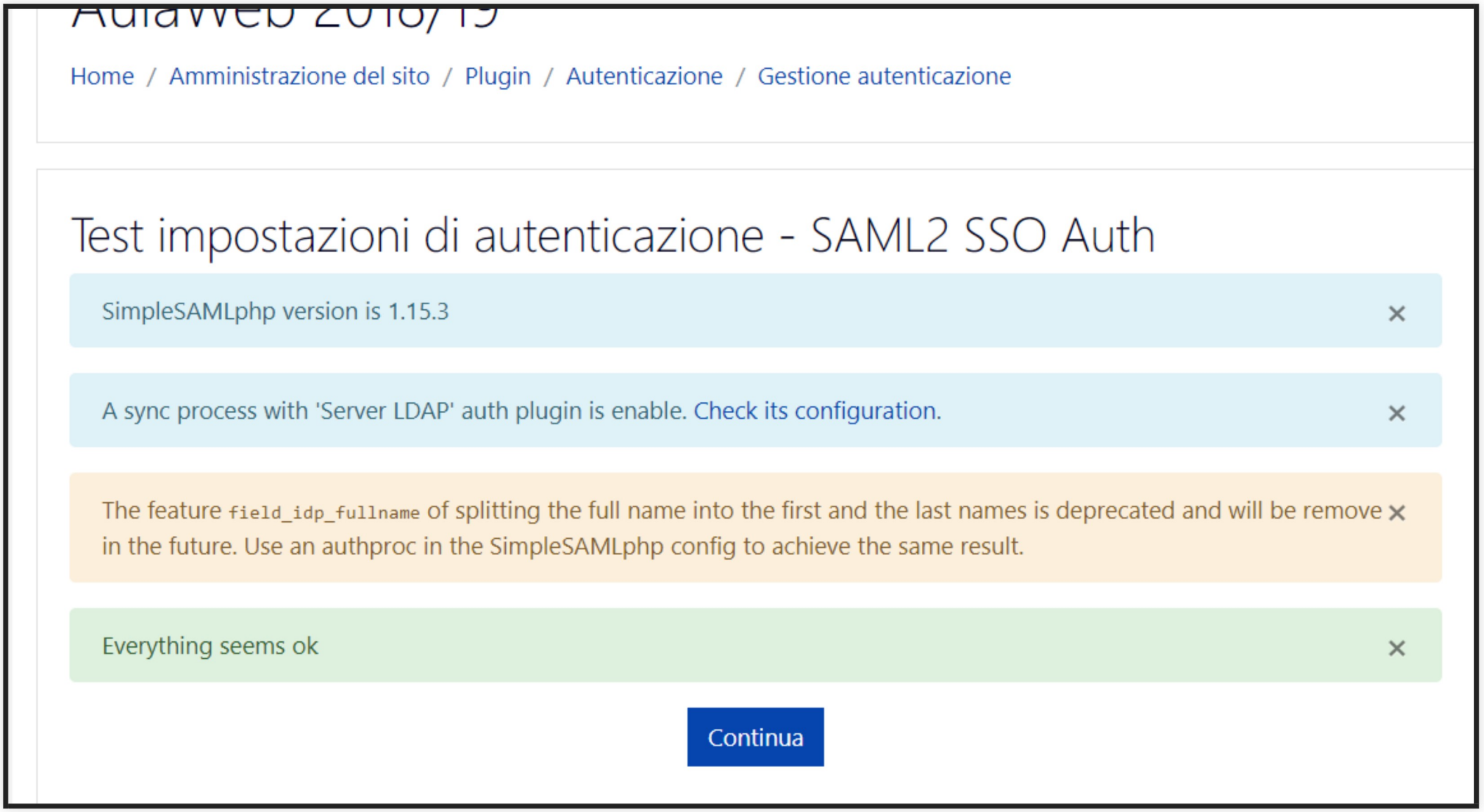
Split del nome

Ammesso che qualche IdP fornisca solo il `cn`...

```
/var/simplesamlphp/authsources.php
'authproc' => array(
    15 => array(
        'class' => 'core:AttributeAlter',
        'subject' => 'urn:oid:2.5.4.3',
        'pattern' => '/^([^\\s]+)/',
        'target' => 'givenName',
        '%replace',
    ),
    16 => array(
        'class' => 'core:AttributeAlter',
        'subject' => 'urn:oid:2.5.4.3',
        'pattern' => '/([^\\s]+)$/',
        'target' => 'sn',
        '%replace',
    )
```

Riferimenti https://simplesamlphp.org/docs/stable/simplesamlphp-authproc

/auth/test_settings.php?auth=saml2sso



Metadata per virtual host

Il problema di fornire i metadata all'IdP in caso di istanze multiple di Moodle rimane aperto