Joomla SAML2 Extension

SP deploy made simple (...SAMLphp)

Stefano Gargiulo (GARR)

Ancora BasicAuth?

Nonostante la maturità delle tecnologie ad accesso federato, ed i noti vantaggi da esse derivanti, ad oggi, vi è ancora una **forte tendenza** a sviluppare nuove applicazioni dotate di **sistemi di login realizzati ad-hoc** malgrado questa sia una scelta onerosa in termini di **tempo** e **difficoltà di gestione,** oppure si tende ancora a **mettere in produzione** applicazioni esistenti servendosi di (apparentemente comode) soluzioni **legacy** come il "BasicAuth" di Apache.

Perché sviluppatori e sistemisti prediligono ancora lavorare in un modo "che non gli conviene"?

Storia di un candidato SP

App

One App

Membership Network

INTERNET Network Research

<md:AssertionConsumerService Location="/SAML2/POST" index="1"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>

Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0

OASIS Standard, 15 March 2005

eduPerson and eduOrg are LDAP schema designed to i

<MetadataPro
uri
back
relo

<md:AssertionConsumerService Location="/SAML/Artifact" index="6"

```
[root@devora shib]# rpm -ivh log4shib-1.0.3-1.1
>      xerces-c-3.0.1-5.1.i386.rpm \
>      xml-security-c-1.5.1-3.2.i386.rpm \
>      xmltooling-1.2.2-1.i386.rpm \
>      opensaml-2.2.1-1.i386.rpm \
>      shibboleth-2.2.1-2.i386.rpm
warning: log4shib-1.0.3-1.1.i386.rpm: Header V3 DSA signature: NOKEY, key
error: Failed dependencies:
```

you must be a geek

Effort iniziale eccessivo!

Dear Boss,

The task of implementing federated authentication in our site requires two months of man time for studying these technologies, implement them in a correct way and productionalize all the stuff.

Do you authorize me to proceed?

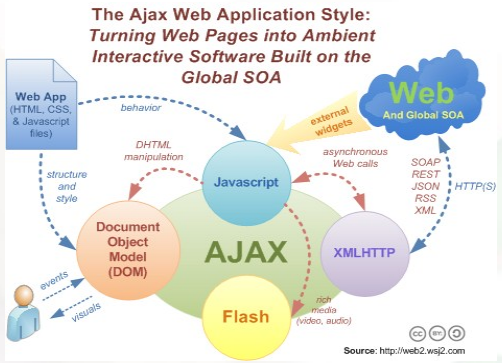
Incapusulare la complessità

Sicuramente la complessità teorica e pratica delle tecnologie su cui si basano le federazioni rappresenta un fattore bloccante per la loro diffusione in larga scala.

E' forse giunto il tempo di rendere queste tecnologie **accessibili a tutti: di incapsularne la complessità**.

D'altronde questo è sempre stato fatto nel mondo della tecnologia, ed in particolar modo in quello dell'informatica. Gli esempi che potremmo fare sono infiniti, ci basti citare il più recente:

Perché il web 2.0 sta avendo un così largo successo?



Mascherando tecnologie complesse con interfacce usabili, sta **offrendo a tutti gli utenti la possibilità di creare contenuti in maniera semplice.**

Joomla SAML2 Extension

L'estensione Joomla sviluppata al GARR è stata concepita proprio sotto quest'ottica: **facilitare la creazione di contenuti federati (servizi)**

- Fornendo un pacchetto renda semplice il deploy di un SP di federazione e che sollevi il provider dalla necessità di dover conoscere a fondo SAML ed i tecnicismi delle piattaforme che lo implementano.

distribuire sicurezza ed operatività out-of-the-box.

(Il pacchetto autoinstallante pesa circa 2MB e contiene tutte le dipendenze necessarie.)

Al fine di:

- favorire l'avvicinamento di nuove persone a queste tecnologie
- aiutare la federazione a crescere in una fase iniziale, nella quale sicuramente la **carenza di servizi** potrebbe rappresentare un fattore di stallo.

Requisiti di progettazione

- **Portabilità**
- **Installazione semplificata**
- **Interoperabilità**
- **Aggiornamento dei metadati garantito**
- **Usabilità end-user**
- **Usabilità amministratore**
- **Supporto AuthZ Federata**
- **Flessibilità**
- **Grouping e AuthZ SP-Side**

simpleSAMLphp

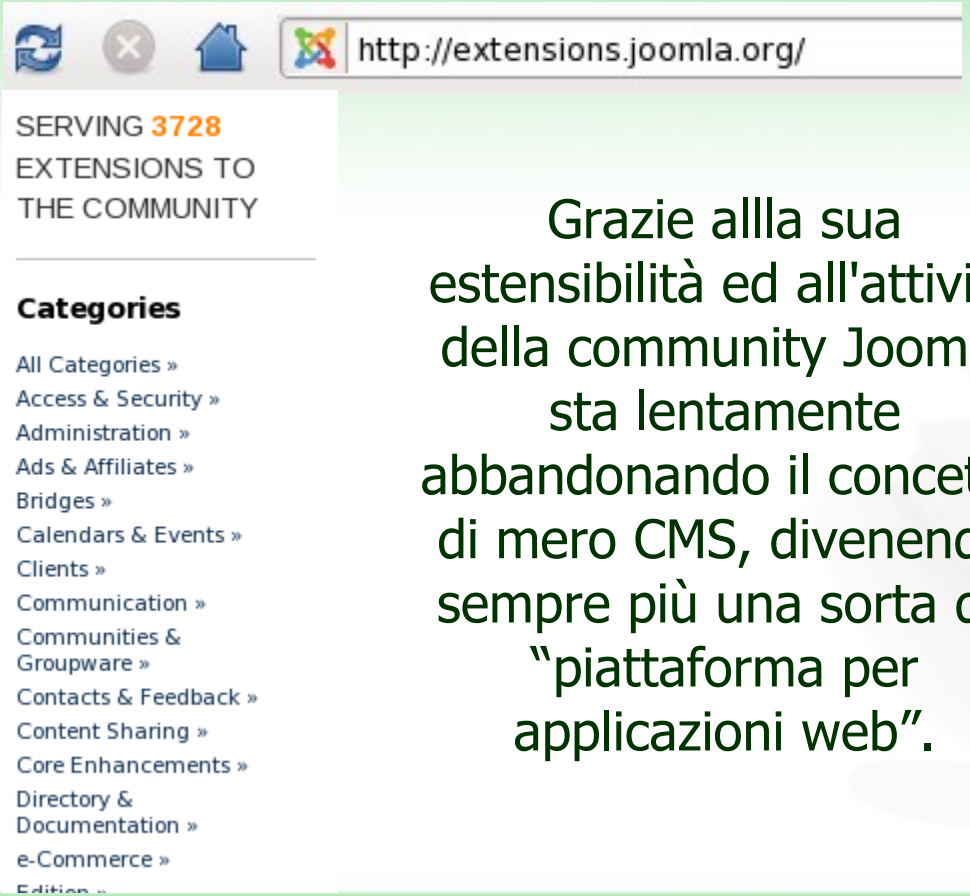
- Implementazione pure-PHP di SAML
- Software completo e modulare
  - Identity Provider
  - Service Provider
  - Discovery Service
- Liberia PHP ad Oggetti
  - Per federare nuove applicazioni / estendere il framework
- Interoperabilità e Bridging
  - Molto usato per il bridging di federazioni
  - eduGAIN complaiant
  - Moduli SAML 2.0, Shiboleth 1.3, A-Select, CAS, OpenID, Google Apps, WS-Federation, InfoCard, PAPI, LDAP (Multi), Radius ecc.
- Usato e sviluppato da
  - Feide (Norway), Haka (Finland), Wayf (Denmark), SWAMID (Sweden), Iceland, eduGAIN ecc.
- Learning & Understanding (SAML Debbugger)

simpleSAMLphp

WAYF
Where are you from

Joomla

Joomla è un CMS open source molto diffuso, usato sia nel settore privato che negli ambienti di istruzione e ricerca italiani.

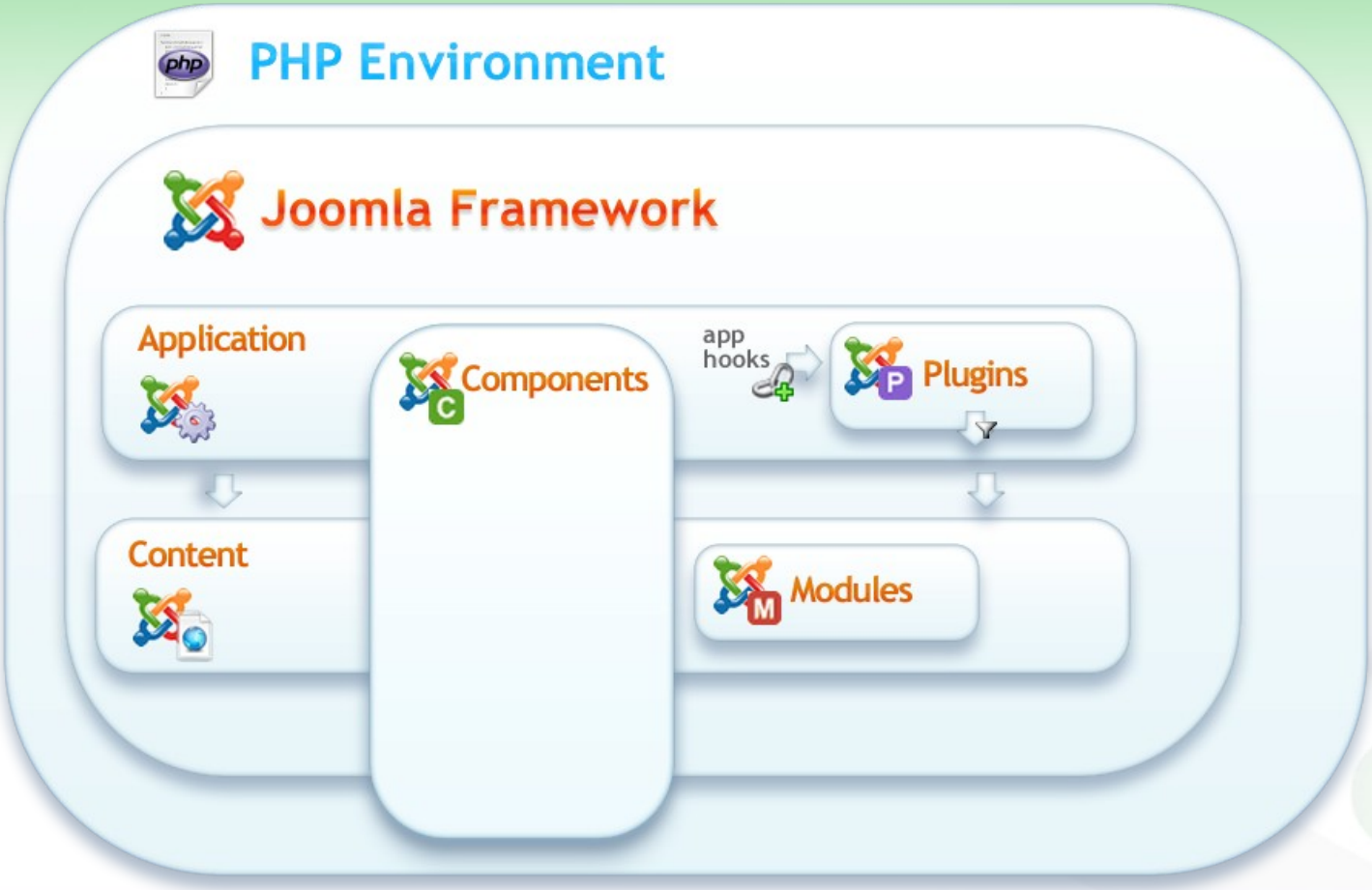


Grazie allla sua estensibilità ed all'attività della community Joomla sta lentamente abbandonando il concetto di mero CMS, divenendo sempre più una sorta di "piattaforma per applicazioni web".

Joomla!™
...because open source matters

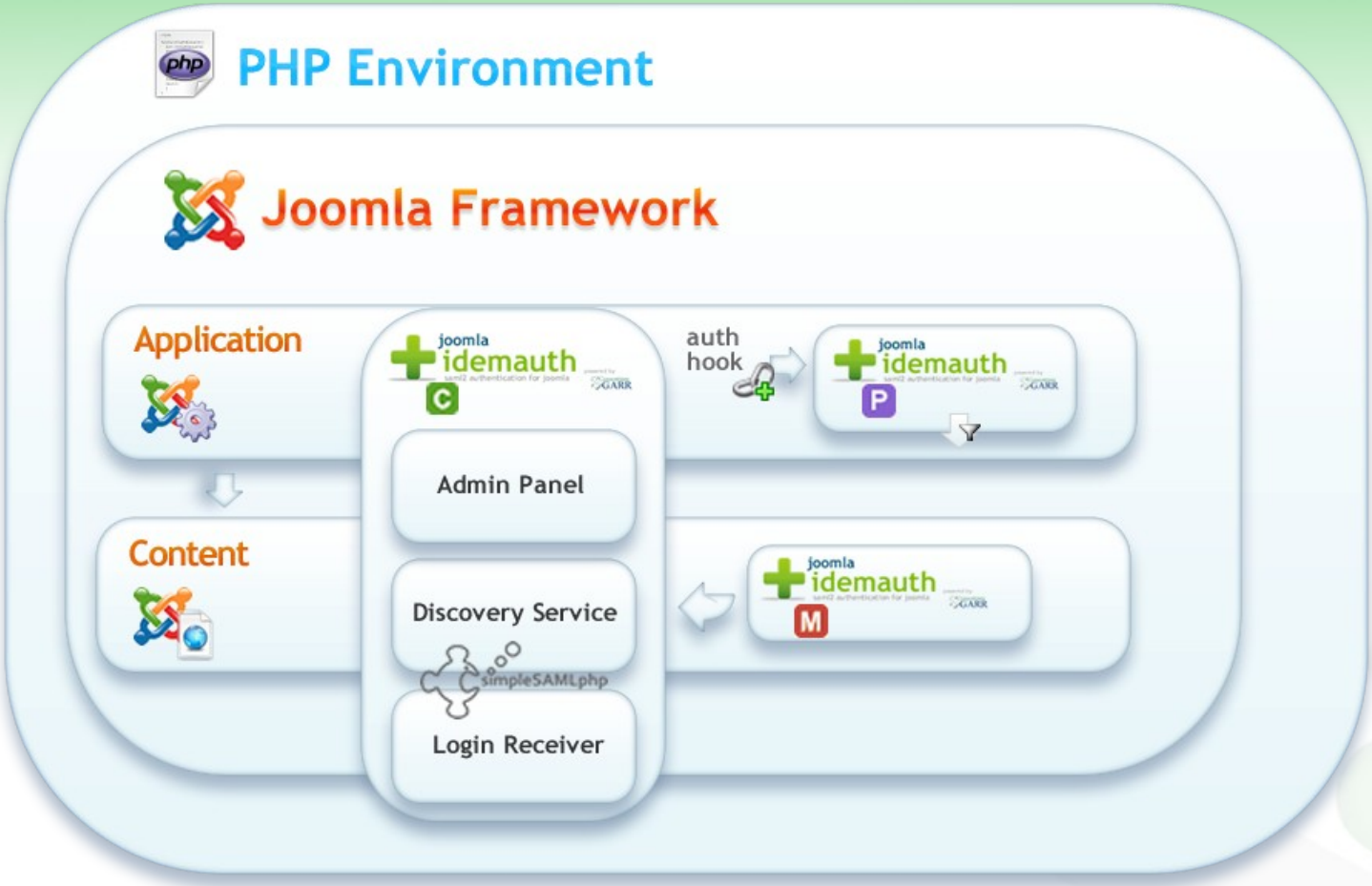
Overview dell'Architettura

Ecco una rappresentazione dell'architettura di Joomla osservata dal punto di vista della sua estensibilità:



Architettura di idemauth

Ed ecco come la nostra estensione vi si posiziona:



Come funziona?

Mapping degli Attributi (default)

Joomla User Property	SAML Attribute	Notes
birthdate	-	Configurable, not required
country	urn:oid:1.3.6.1.4.1.25178.1.2.1 (schacMotherTongue) *	Configurable, not required
email	**urn:oid:0.9.2342.19200300.100.1.3 (mail)**	**Configurable (or ePTID@fakedomain in privacy mode), required**
fullname	**"<urn:oid:2.5.4.42> <urn:oid:2.5.4.4>" ("<givenName> <sn>")**	**Configurable (ePTID in privacy mode), required**
gender	1.3.6.1.4.1.25178.1.2.2 (schacGender)	Configurable, not required
language	urn:oid:2.16.840.1.113730.3.1.39 (preferredLanguage)	Configurable, not required (default EN)
password	-	**Never stored (remote authenticated user)**
postcode	-	Configurable, not required
timezone	-	Configurable, not required
type	"Registered"	AuthZ. Assignment Rules (coming soon)
username	**urn:oid:1.3.6.1.4.1.5923.1.1.1.6 (eduPersonPrincipalName)**	**Configurable (or ePTID@fakedomain in privacy mode), required**
-	urn:oid:1.3.6.1.4.1.5923.1.1.1.9 (eduPersonScopedAffiliation)	Used for AuthZ. Filters (reqExp)
-	urn:oid:1.3.6.1.4.1.5923.1.1.1.7 (eduPersonEntitlement)	Used for AuthZ. Filters (strict)

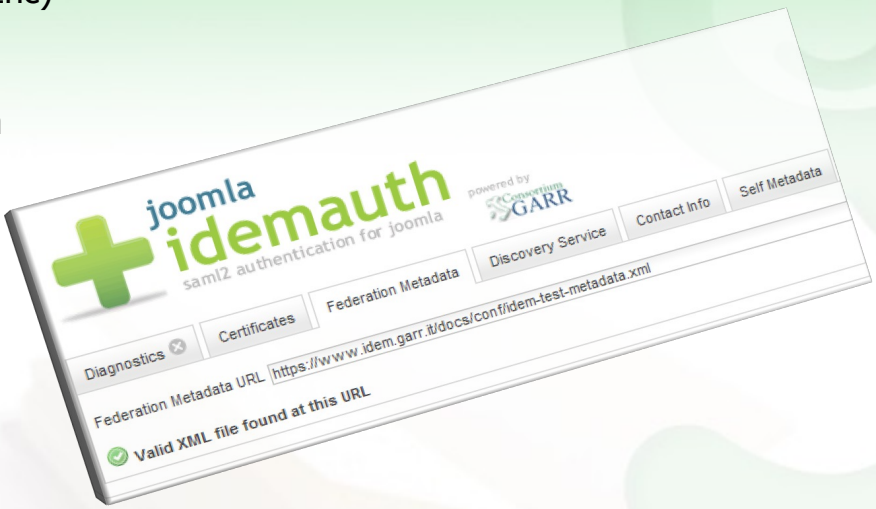
Tutti I mapping sono riconfigurabili al fine rendere il prodotto adattabile anche ad altre federazioni e profili.

Nota: vi sono due profili di mapping configurabili separatamente: **privacy mode** e normal.

I valori di default sono compatibili con le specifiche IDEM, eduGAIN ed Interoperable SAML2 Profile

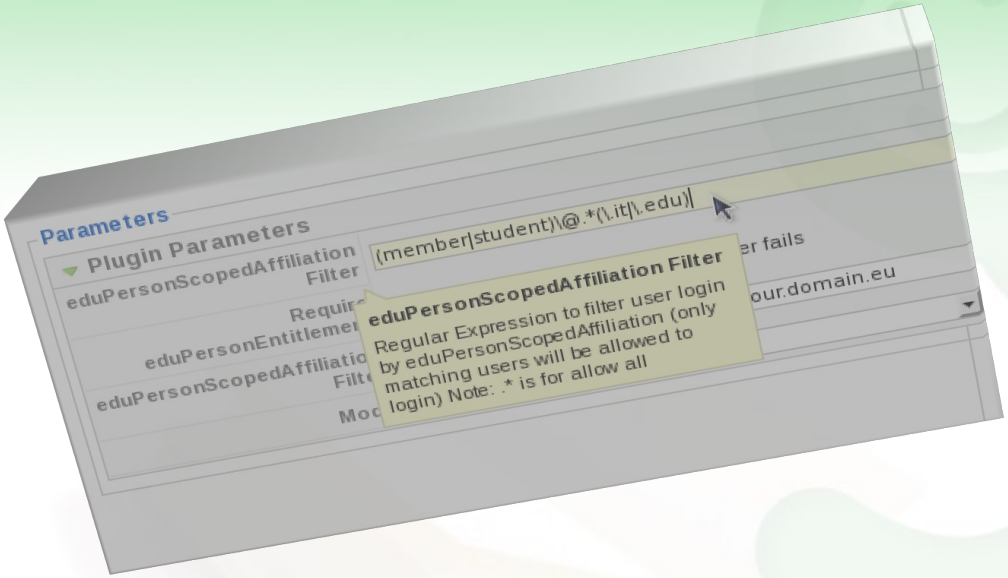
Implementazione dei requisiti

- **Portabilità**
  - Full PHP: No dipendeze con Apache o SO
  - Richiede solamente PHP >= 5.1.2 ed alcune librerie PHP molto diffuse e disponibili su tutte le piattaforme
  - Encryption delle Assertion in PHP nativo (Mcrypt → XMLEnc)
- **Installazione facilitata**
  - Essendo un estensione Joomla 1.5 nativa, si installa attraverso il sistema di gestione delle estensioni di Joomla (basta un click)
- **Interoperabilità**
  - Aggiunto a simpleSAMLphp il supporto per l'EncryptedNameID (Shibboleth2 IdP)
  - Patch per l'autodetect dell'algoritmo di Encryption usato sulle Assertions ricevute dall'IdP
- **Aggiornamento dei metadati di federazione garantito**
  - Updater automatico PHP based (no cronjobs)
  - L'utente deve semplicemente inserire l'url dei metadati xml di federazione
- **Usabilità end-user**
  - Discovery Service integrato (Searchable Combobox)



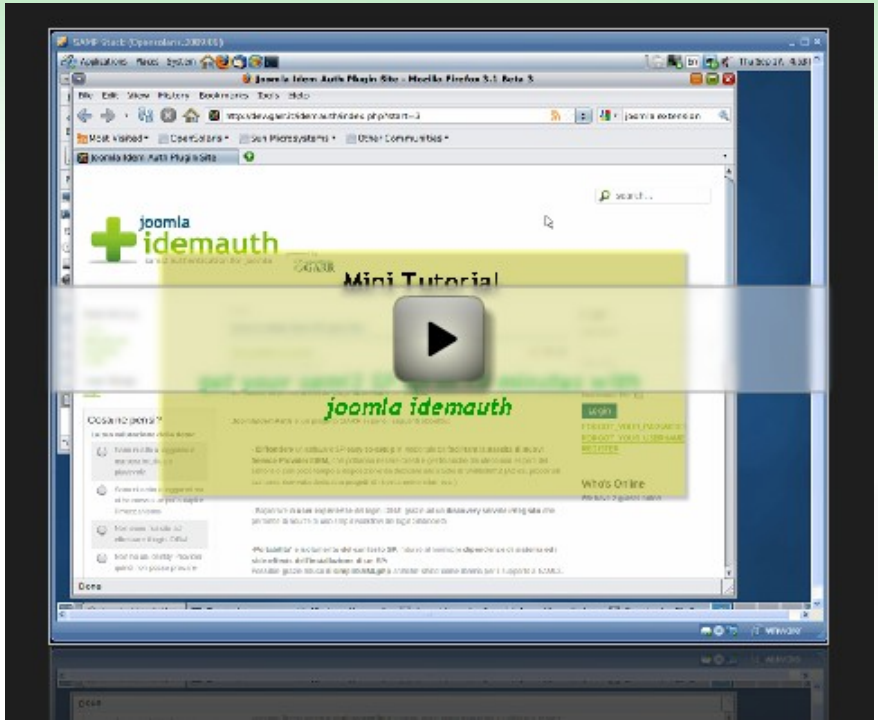
Implementazione dei requisiti (2)

- **Usabilità per l'amministratore**
  - Semplice pannello amministrativo per la configurazione dell'SP (interamente web-based)
- **Gestione autorizzazione federata**
  - eduPersonEntitlement filter
  - eduPersonScopedAffiliation RegExp filter
- **Flessibilità**
  - L'applicativo viene fornito con una serie di preset per lavorare con la federazione IDEM, ma il comportamento e gli attributi utilizzati possono essere riconfigurati per aderire anche a profili di altre federazioni
- **Grouping ed autorizzazione SP-side**
  - Email all'amministratore al primo login di ogni utente federato al fine di offrire un supporto di base per approvazione a posteriori del livello e del gruppo dell'utente (funzionalità inspirata da SWITCH GMT)



SP in 15 minuti

http://dev.garr.it/idemauth/SPin15mins



Per mettere in produzione un nuovo SP Joomla bisogna semplicemente:

- Installare idemauth
- Generare un nuovo certificato
- Inserire l'url dei metadati
- Inviare il proprio spezzone di metadati alla federazione

Prospettive per il futuro

- **Funzioni di Grouping ed Autorizzazione avanzate:** Joomla 1.6 (ora in Alpha) sarà dotato di un sistema di grouping e gestione dei permessi molto più potente dell'attuale (che è decisamente insoddisfacente) il prossimo passo sarà quindi integrare l'estensione con le nuove funzioni di Joomla fornendo ad esempio la possibilità di definire regole per l'assegnamento di utenti a gruppi e livelli in base ai valori degli attributi.

- **Sempre un occhio di riguardo verso l'usabilità:** piu' controlli accattivanti, IdP-in-a-ligthbox, nuovi helper e wizard per la configurazione di altri dettagli ecc.

- **Supporto Multifederazione:** offrire la possibilità di annettere l'SP a più di una federazione

Links

- Demo and Download: http://dev.garr.it/idemauth
- Project homepage: http://idemauth.kenai.com
- simpleSAMLphp: http://rnd.feide.no/simplesamlphp
- simpleSAMLphp project: http://code.google.com/p/simplesamlphp/
- Interoperable SAML2 Profile: http://saml2int.org/
- Joomla Official Extensions: http://extensions.joomla.org
- A Joomla framework introduction: http://www.slideshare.net/JohanJanssens/phpbootcamp-joomla-framework
- JoomlaDay 2009: http://www.joomladay.it