



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

**Projeto PNUD BRA/12/018** - "Documento com análise de arquiteturas de sistemas de identidade distribuída, estratégia de implantação considerando os sites parceiros e contendo propostas de códigos."

**Consultora: Joenio Marques da Costa**  
**Contrato nº: 2013/000564**  
**Produto / nº: 02**

**Assinatura do Consultor**

Local e data: Brasília/DF, \_\_\_\_ de \_\_\_\_\_ de 2014

Assinatura do Consultor: \_\_\_\_\_

**Assinatura do Supervisor**

Atesto que os serviços foram prestados conforme estabelecido no Contrato de Consultoria.

Local e data: Brasília/DF, \_\_\_\_ de \_\_\_\_\_ de 2014

Assinatura e Carimbo: \_\_\_\_\_



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

<b>Título</b>	"Documento com análise de arquiteturas de sistemas de identidade distribuída, estratégia de implantação considerando os sites parceiros e contendo propostas de códigos."
<b>Língua do documento</b>	Português - Brasil
<b>Documentação de referência</b>	Português
<b>Unidade responsável</b>	Secretaria Geral da Presidência da República (SG/PR)
<b>Criador</b>	Joenio Marques da Costa- joenio@colivre.coop.br
<b>Taxonomias</b>	Desenvolvimento
<b>Data de aprovação</b>	
<b>Público</b>	SG/PR, Parceiros e Sociedade Civil
<b>Faz parte do</b>	Projeto PNUD BRA/12/018
<b>Em conformidade com a</b>	Secretaria Geral da Presidência da República
<b>Documentos anexos</b>	Nenhum
<b>Revisado em</b>	



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

## **Sumário**

<b>1</b>	<b>Apresentação</b>	<b>6</b>
<b>2</b>	<b>SSO - Single Sign-on</b>	<b>6</b>
2.1	O que é SSO? . . . . .	6
2.2	SSO no Noosfero . . . . .	7
2.3	Qual problema SSO resolve? . . . . .	7
2.4	Como SSO funciona? . . . . .	8
2.5	Quais soluções de SSO existem? . . . . .	8
2.5.1	Accounts & SSO . . . . .	9
2.5.2	Central Authentication Service (CAS) . . . . .	9
2.5.3	Distributed Access Control System (DACS) . . . . .	10
2.5.4	Enterprise Sign On Engine . . . . .	11
2.5.5	FreeIPA . . . . .	11
2.5.6	IBM Enterprise Identity Mapping . . . . .	11
2.5.7	JBoss SSO . . . . .	12
2.5.8	JOSSO . . . . .	12
2.5.9	Kerberos . . . . .	12
2.5.10	OpenAM . . . . .	13
2.5.11	Pubcookie . . . . .	13
2.5.12	SAML . . . . .	14
2.5.13	Shibboleth . . . . .	15
2.5.14	ZXID . . . . .	16
<b>3</b>	<b>IdP - Identity Provider</b>	<b>16</b>
3.1	O que é IdP? . . . . .	16
3.2	IdP no Noosfero . . . . .	17
3.3	Qual problema IdP resolve? . . . . .	17
3.4	Quais soluções de IdP existem? . . . . .	17
3.4.1	Mozilla Persona . . . . .	17
3.4.2	OAuth . . . . .	18
3.4.3	OpenID . . . . .	18
3.4.4	OpenID Connect . . . . .	19
<b>4</b>	<b>Outras iniciativas</b>	<b>19</b>
4.1	OpenAthens - Reino Unido . . . . .	19
4.2	Microsoft account . . . . .	19
4.3	Liberty Alliance . . . . .	20
<b>5</b>	<b>Discussão</b>	<b>20</b>



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

5.1	Iniciativas (Governo e Comunidade) . . . . .	21
5.1.1	Login Cidadão . . . . .	21
5.1.2	Id da Cultura . . . . .	21
5.2	Proposta para o Participa.BR . . . . .	21
<b>6</b>	<b>Considerações finais</b>	<b>22</b>



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

**Lista de Figuras**

1	Exemplo de implementação de SSO do SiteMinder . . . . .	8
2	Diagrama do RubyCAS, implementação do protocolo CAS em Ruby . . . . .	10
3	Diagrama de negociação do Kerberos . . . . .	13
4	Exemplo de federação com OpenAM para um portal de viagens . . . . .	14
5	Single Sign-on com SAML2 . . . . .	15



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

## **1 Apresentação**

Em consonância com os objetivos e cronograma previsto no âmbito do projeto BRA/12/018: **Desenvolvimento de Metodologias de Articulação e Gestão de Políticas Públicas para Promoção da Democracia Participativa**, firmado entre a Secretaria-Geral da Presidência da República (SG/PR) e o Programa das Nações Unidas para o Desenvolvimento (PNUD), o presente documento apresenta "Documento com análise de arquiteturas de sistemas de identidade distribuída, estratégia de implantação considerando os sites parceiros e contendo propostas de códigos." .

Essa proposta está configurada como produto 02 da consultoria técnica para especificação da construção dos códigos das metodologias de organização da informação e interação participativa do portal de participação social.

## **2 SSO - Single Sign-on**

### **2.1 O que é SSO?**

Single Sign-on, ou Web Browser Single Sign-on é a propriedade de controle de acesso a sistemas Web onde usuários efetuam login apenas uma vez e ganham acesso a outros sistemas que tenham relação com tal sistema sem a necessidade de fornecer suas credenciais de autenticação uma segunda vez. Os sistemas que possuem relação são definidos previamente pela implementação e configuração do ambiente de SSO e é feito pelos desenvolvedores e administradores dos sistemas envolvidos. Analogamente, single sign-off é a propriedade inversa, onde o usuário finaliza sua sessão de login em um sistema e de forma automática ele é deslogado também dos outros sistemas que façam parte deste mesmo ambiente.

Usualmente, ambientes SSO compartilham servidores de autenticação para servir cada aplicação, com objetivo de autenticar e garantir que usuários não necessitem entrar com suas credenciais de autenticação mais de uma vez<sup>1</sup>. Estes servidores fornecem serviços de autenticação em rede para aplicações externas, a autenticação pode ser feita por diversos métodos, mas normalmente usa-se usuário/senha<sup>2</sup> em aplicações Web.

O uso de SSO aumenta drasticamente o impacto negativo em caso de roubo de informações, uma vez que o acesso a esta informação possibilita acesso a diversos sistemas, portanto a proteção dessas informações devem ser dobradas. É preciso também ter cuidado com a disponibilidade do serviço, uma vez que sua queda implica em indisponibilidade dos serviços que fazem parte do ambiente de SSO.

---

<sup>1</sup>[http://en.wikipedia.org/wiki/Single\\_sign-on](http://en.wikipedia.org/wiki/Single_sign-on)

<sup>2</sup>[http://en.wikipedia.org/wiki/Authentication\\_server](http://en.wikipedia.org/wiki/Authentication_server)



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

## **2.2 SSO no Noosfero**

O Noosfero não implementa mecanismos de SSO, nem há referências na comunidade de utilização dele num ambiente como este. O mecanismo de autenticação presente no Noosfero está implementado nos seguintes arquivos:

- noosfero/lib/authenticated\_system.rb
- noosfero/app/controllers/public/account\_controller.rb
- noosfero/app/model/user.rb

Esta implementação presente no *core* do Noosfero realiza autenticação através de usuário/senha e armazena estas informações em banco de dados de forma encriptada. É possível alterar o método de autenticação através de plugins, um exemplo é o plugin Ldap distribuído junto ao Noosfero em:

- noosfero/plugins/ldap

Este plugin possibilita realizar autenticação a partir de um servidor LDAP.

## **2.3 Qual problema SSO resolve?**

SSO resolve um problema bem comum e conhecido, o usuário de um serviço Web (site, sistema, rede social, etc) quer logar apenas uma vez e manter sua sessão entre diversos serviços (outros sites, outras redes, etc) sem necessidade de fornecer seus dados de acesso uma segunda vez.

A solução para esta questão precisa lidar com uma política segurança e privacidade implementada nos Navegadores Web, esta política, chamada Same Origin Policy<sup>3</sup> é uma recomendação do W3C e previne que documentos em diferentes domínios afetem e compartilhem dados com outros domínios, isso previne, por exemplo, ataques de cross-site scripting.

Inúmeras soluções foram propostas para contornar esta política, JSONP, CORS, easyXDM, entre outras<sup>4</sup>, todas elas se tornaram obsoletas após a recomendação do W3C chamada "Web Messaging"<sup>5</sup>, uma técnica que permite documentos em diferentes domínios compartilhar dados. A maioria dos Navegadores Web atuais implementam Web Messaging<sup>6</sup>.

---

<sup>3</sup>[https://en.wikipedia.org/wiki/Same-origin\\_policy](https://en.wikipedia.org/wiki/Same-origin_policy)

<sup>4</sup><http://stackoverflow.com/questions/7094967/single-sign-on-with-ajax-in-same-origin-policy-world-effective-solutions>

<sup>5</sup><http://www.w3.org/TR/webmessaging/>

<sup>6</sup>[http://en.wikipedia.org/wiki/Web\\_Messaging](http://en.wikipedia.org/wiki/Web_Messaging)



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

## 2.4 Como SSO funciona?

Existem muitas formas de implementar SSO: Kerberos, Smart card, CAS, OTP, entre outras, cada uma com sua própria estratégia<sup>7</sup>. A solução SiteMinder<sup>8</sup> da "CA Technologies", por exemplo, implementa SSO da seguinte forma<sup>9</sup>:

- Usuário autentica uma vez
- O navegador faz cache da autenticação e seta um cookie com informações de single sign-on
- O cookie fornece informações de sessão, assim o usuário pode acessar outros sites sem necessidade de re-autenticar

A Figura 1 traz um diagrama exemplificando esta solução. A solução SiteMinder é um sistema centralizado de gerenciamento de acesso Web da empresa "CA Technologies", que implementa uma série de soluções, além de SSO.

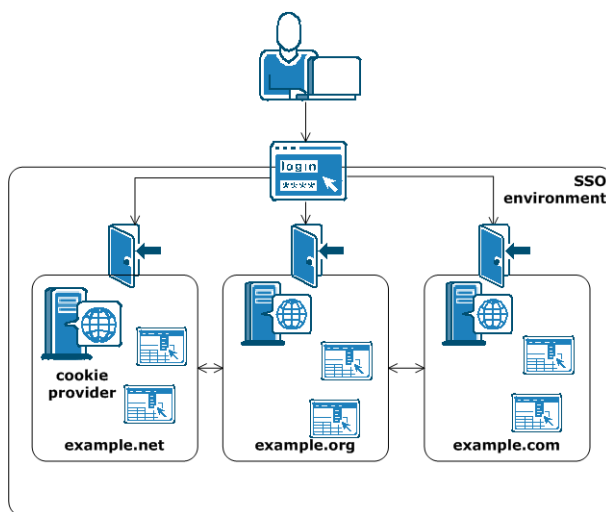


Figura 1: Exemplo de implementação de SSO do SiteMinder

## 2.5 Quais soluções de SSO existem?

A seguir é apresentada uma lista de soluções em software livre para SSO elaborada com base no artigo da Wikipedia em:

<sup>7</sup>[http://www.opengroup.org/security/sso/sso\\_intro.htm](http://www.opengroup.org/security/sso/sso_intro.htm)

<sup>8</sup><http://www.ca.com/br/products/detail/ca-siteminder.aspx>

<sup>9</sup>[http://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%205-ENU/Bookshelf\\_Files/HTML/idos/256655.html](http://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%205-ENU/Bookshelf_Files/HTML/idos/256655.html)





**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

- [http://en.wikipedia.org/wiki/List\\_of\\_single\\_sign-on\\_implementations](http://en.wikipedia.org/wiki/List_of_single_sign-on_implementations)

### 2.5.1 Accounts & SSO

Framework contendo um conjunto de componentes e bibliotecas para autenticação de contas de usuários online para clientes Desktops, sistemas Linux e POSIX.

Mais em:

- [http://en.wikipedia.org/wiki/Accounts\\_&\\_SSO](http://en.wikipedia.org/wiki/Accounts_&_SSO)

**Avaliação:** *Não é uma opção válida para ser implantado no portal de participação social Participa.br pois é voltado para clientes desktop.*

### 2.5.2 Central Authentication Service (CAS)

Protocolo de Single Sign-on para a Web. O nome CAS refere-se também a uma implementação deste mesmo protocolo. O fluxo durante a autenticação é o seguinte:

- Cliente visita uma aplicação que requisita autenticação
- A aplicação redireciona o Cliente para o CAS
- CAS valida autenticidade do Cliente (geralmente contra um banco, Kerberos, Active Directory, etc)
- Se a autenticação tem sucesso, o CAS retorna o cliente para a aplicação, passando um ticket de segurança
- A aplicação valida o ticket contactando o CAS
- O CAS dá a informação com segurança à aplicação que o usuário foi autenticado com sucesso

A implementação oficial do CAS é em Java e é mantido, hoje, pelo grupo JASIG<sup>10</sup>, existem implementações oficiais de cliente em várias linguagens, como: .NET, PHP, Perl, Apache, etc.

O artigo *Approaches and challenges for a single sign-on enabled extranet using Jasig CAS* descreve a experiência em configurar single sign-on em um ambiente de intranet usando o CAS e outros software livres, e faz uma boa avaliação das tecnologias envolvidas, como OpenID, OAuth, etc.

- [http://openidentity.eu/2013/media/09\\_Holzschuher\\_Peinkl\\_2013\\_SSO\\_extranet\\_CAS\\_LNI.pdf](http://openidentity.eu/2013/media/09_Holzschuher_Peinkl_2013_SSO_extranet_CAS_LNI.pdf)

Mais em:

- [http://en.wikipedia.org/wiki/Central\\_Authentication\\_Service](http://en.wikipedia.org/wiki/Central_Authentication_Service)

---

<sup>10</sup><http://www.jasig.org>



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

### Basic CAS Authentication Mechanism

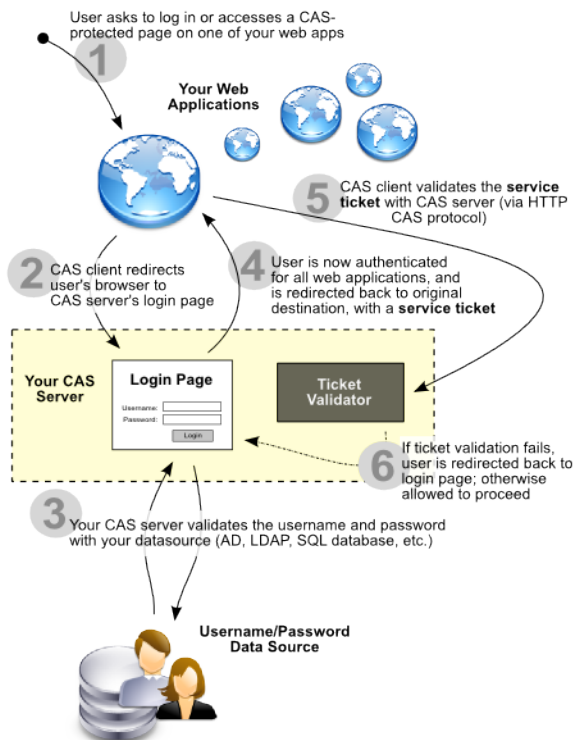


Figura 2: Diagrama do RubyCAS, implementação do protocolo CAS em Ruby

- <http://www.jasig.org/cas/protocol>

**Avaliação:** Implementação madura contendo um bom conjunto de técnicas para implementação de SSO, incluindo suporte a OAuth, OpenID, SAML, LDAP, etc. É uma opção recomendada.

#### 2.5.3 Distributed Access Control System (DACS)

DACS é um sistema de SSO leve combinado com mecanismos de autenticação e controle de acesso para Web escrito em C/C++. Possui suporte para integrar com diversos mecanismos de autenticação, como X.509, PAM, LDAP, etc. Possui módulo de autenticação para servidor Web Apache.

O Debian utiliza DACS para prover SSO entre alguns dos seus servidores de desenvolvimento do projeto.



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

Mais em:

- [http://en.wikipedia.org/wiki/Distributed\\_Access\\_Control\\_System\\_\(DACS\)](http://en.wikipedia.org/wiki/Distributed_Access_Control_System_(DACS))
- <https://wiki.debian.org/DebianSingleSignOn>

**Avaliação:** ?????.

#### **2.5.4 Enterprise Sign On Engine**

Plataforma de SSO, controle de acesso e federação compatível com SAML 2.0 e parcialmente compatível com XACML<sup>11</sup>.

Desenvolvido em Java, possui suporte a Tomcat, Apache e IIS.

Mais em:

- [http://en.wikipedia.org/wiki/Enterprise\\_Sign\\_On\\_Engine](http://en.wikipedia.org/wiki/Enterprise_Sign_On_Engine)

**Avaliação:** *Nenhuma referência encontrada sobre seu uso em produção, não recomendado para o portal de participação social Participa.br.*

#### **2.5.5 FreeIPA**

Solução da RedHat para SSO e "Policy and Audit". É comparável a solução "Novell's Identity Manager" ou "Microsoft's Active Directory" pois tem objetivos e mecanismos similares.

Usa as soluções 389 Directory Server, MIT Kerberos 5, Apache HTTP e Python. A partir da versão 3.0.0 adicionou suporte a Samba para integração com Microsoft Active Directory.

Mais em:

- <http://en.wikipedia.org/wiki/FreeIPA>

**Avaliação:** *Esta solução é inicialmente voltada para ambientes de rede desktop e não atende aos requisitos do Participa.br.*

#### **2.5.6 IBM Enterprise Identity Mapping**

Framework para mapear identidades de usuários em várias plataformas distintas, pouca informação disponível na Web.

Mais em:

---

<sup>11</sup><http://en.wikipedia.org/wiki/XACML>



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

- [http://en.wikipedia.org/wiki/IBM\\_Enterprise\\_Identity\\_Mapping](http://en.wikipedia.org/wiki/IBM_Enterprise_Identity_Mapping)

**Avaliação:** *Voltado apenas para integrar soluções da própria IBM.*

### **2.5.7 JBoss SSO**

Faz parte da suíte de soluções JBoss SOA, permite single sign-on, sign-off e acesso federado a múltiplas aplicações e recursos computacionais em rede.

Dentre várias funcionalidades o JBoss SSO inclui:

- Integração entre aplicações e módulos baseados no padrão SAML
- Abordagem descentralizada
- Habilidade de conectar a diferentes sistemas de armazenamento

Mais em:

- [http://en.wikipedia.org/wiki/JBoss\\_SSO](http://en.wikipedia.org/wiki/JBoss_SSO)

**Avaliação:** *Solução madura, possível alternativa a ser utilizada.*

### **2.5.8 JOSSO**

Java Open Single Sign On (JOSSO) é uma solução de SSO para aplicações Web. Baseado em Java EE, permite múltiplos servidores web autenticar usuários através de suas credenciais. JOSSO se comunica com o armazenamento das credenciais por LDAP ou JDBC e fornece interface via SOAP sob o protocolo HTTP para permitir fácil integração com aplicações não-Java.

Mais em:

- <http://en.wikipedia.org/wiki/JOSSO>

**Avaliação:** *Solução madura, possível alternativa a ser utilizada.*

### **2.5.9 Kerberos**

Protocolo de autenticação em rede baseado em 'tickets', permite comunicação entre nós sob uma rede não-segura de forma segura. Foi projetado principalmente com um modelo cliente-servidor, isso provê autenticação tanto de usuários quanto de servidores. Veja na Figura 3 um exemplo de negociação com o Kerberos.

Mais em:

- [http://en.wikipedia.org/wiki/Kerberos\\_\(protocol\)](http://en.wikipedia.org/wiki/Kerberos_(protocol))



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

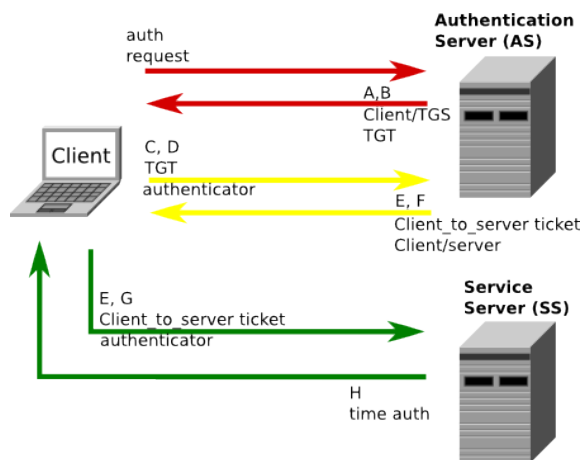


Figura 3: Diagrama de negociação do Kerberos

**Avaliação:** *Protocolo de autenticação, não é uma solução para SSO.*

### 2.5.10 OpenAM

Provê single sign-on de forma transparente em infraestrutura de redes. Escrito em Java, suporte a mais de 20 tipos de autenticação, possui suporte a SAML e implementa sistema de autorização baseado em XACML. Veja um exemplo na Figura 4 de uso do OpenAM em um portal de viagens.

Mais em:

- <http://en.wikipedia.org/wiki/OpenAM>

**Avaliação:** *Possível alternativa de ser utilizada, madura, bem documentada e bastante utilizada, suporta: OAuth, SAML, Kerberos, LDAP, etc.*

### 2.5.11 Pubcookie

Protocolo (e software) de SSO, o processo de autenticação se dá da seguinte forma:

- Quando usuário acessa a aplicação, Pubcookie seta 2 cookies, pré-sessão e concessão de requisição
- Redireciona usuário para página de login
- Usuário fornece login e senha, se o login for com sucesso, seta 2 cookies, login e concessão

Mais em:



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

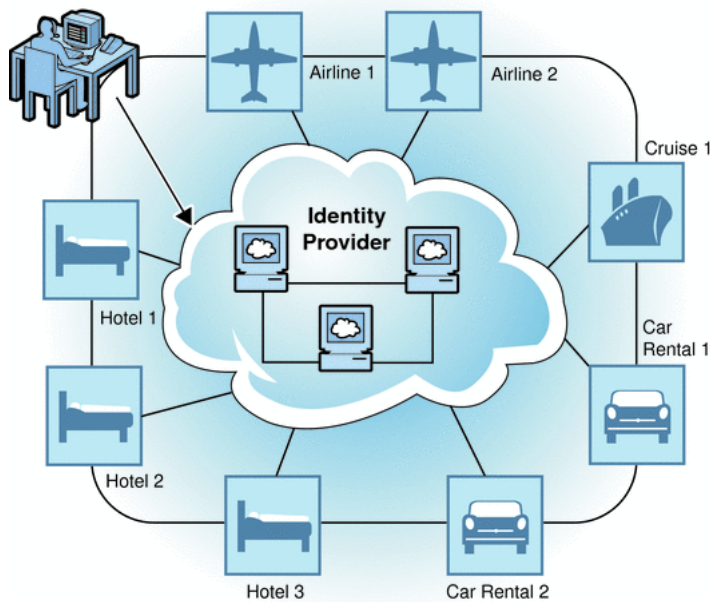


Figura 4: Exemplo de federação com OpenAM para um portal de viagens

- <http://en.wikipedia.org/wiki/Pubcookie>

**Avaliação:** O último release do projeto é de 2010, não recomendado como possível solução de SSO para o portal Participa.br

## 2.5.12 SAML

Linguagem de marcação para definir comunicação sobre autenticação e autorização

Security Assertion Markup Language (SAML) é uma linguagem de marcação baseada em XML para troca de dados de autenticação e autorização definido pelo OASIS Security Services Technical Committee. O SAML é principalmente desenvolvido para ser aplicado em Web Browser Single Sign-on.

A especificação SAML define 3 papéis:

- Principal (geralmente um usuário)
- Provedor de identidade (IdP)
- Provedor de serviço (SP)

A interação entre eles está representada na Figura 5.



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

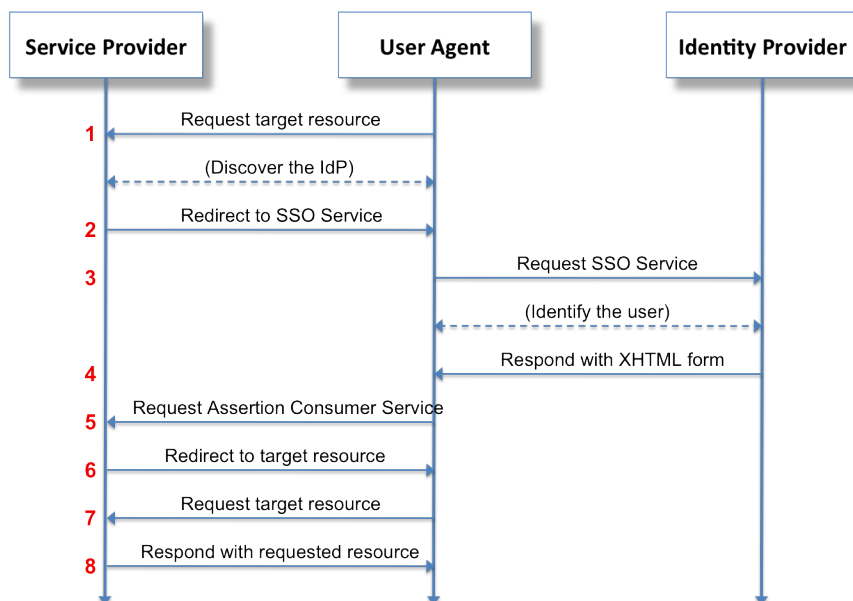


Figura 5: Single Sign-on com SAML2

Mais em:

- [http://en.wikipedia.org/wiki/Security\\_Assertion\\_Markup\\_Language](http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language)

**Avaliação:** Não uma solução de SSO em si, é suportado por várias soluções, é altamente recomendado que a solução adotada no Participa.br suporte este padrão.

### 2.5.13 Shibboleth

Middleware para SSO e autenticação baseado em SAML.

Mais em:

- [http://en.wikipedia.org/wiki/Shibboleth\\_\(Internet2\)](http://en.wikipedia.org/wiki/Shibboleth_(Internet2))

**Avaliação:** É uma possível alternativa a ser utilizada no Participa.br, tem boas referências de uso na prática como por exemplo a iniciativa das universidades do Reino Unido chamada OpenAthens.



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

#### **2.5.14 ZXID**

Kit de gerenciamento de identidade SAML 2.0. Compatível com SAML 2.0, Liberty ID-WSF 2.0 e XACML 2.0. Implementado em C com, possui poucas dependências externas, fornece bibliotecas para PHP, Perl e Java via SWIG.

Mais em:

- <http://en.wikipedia.org/wiki/ZXID>

**Avaliação:** *Não recomendado.*

### **3 IdP - Identity Provider**

#### **3.1 O que é IdP?**

Identity Provider, ou Provedor de Identidade, é o serviço responsável por gerenciar informações de identidade entre sistemas, usuários ou outros atores, provendo através de um módulo interno ou externo serviço de autenticação e autorização, de forma segura, a fim de verificar a autenticidade.

Um provedor de identidade fornece uma alternativa para que vários serviços web distintos autenticem seus usuários através dele, de forma que um usuário pode ter apenas um login/senha e autenticar em vários serviços com este mesmo login/senha. Isto não implica em Single Sign-on, pois com um provedor de identidade apenas o usuário ainda precisa passar por uma etapa de autenticação, num ambiente de SSO isto fica transparente e o usuário ao logar num sistema Web não precisa passar pela etapa de autenticação ao acessar um segundo serviço.

Uma solução de SSO é composta usualmente de ao menos 3 componentes:

- Usuário/cliente, geralmente usa-se o termo *Principal*
- Provedor de identidade, *IdP - Identity Provider*
- Provedor de serviço, *SP - Service Provider*

Neste cenário o usuário autentica apenas uma vez e um token de segurança é passado entre os sistemas participantes do ambiente de SSO. Normalmente suportam os tipos de token de segurança mais comuns, como: SAML, SPNEGO, X.509.

Um sistema de provedor de identidade (IdP) é normalmente parte de um ambiente de SSO, usualmente é um primeiro passo para se ter Single Sign-on.

Mais sobre Identity Provider e os diversos conceitos envolvidos podem ser encontrados em:

- [http://en.wikipedia.org/wiki/Identity\\_provider](http://en.wikipedia.org/wiki/Identity_provider)





**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

- <http://www.empowerid.com/learningcenter/technologies/service-identity-providers>

### **3.2 IdP no Noosfero**

O Noosfero não implementa oficialmente integração com nenhum protocolo ou tecnologia de provedor de identidade, no entanto existe uma implementação não-oficial em uso na rede Cirandas.net<sup>12</sup> de uso do OAuth e Mozilla Persona, o código fonte desta implementação, ainda não integrada ao repositório oficial do Noosfero, encontra-se em:

- <https://github.com/CIRANDAS/noosfero-ecosol/tree/master/plugins/oauth>

### **3.3 Qual problema IdP resolve?**

Um usuário cria apenas um registro login/senha e acessa múltiplos serviços através deste mesmo login/senha, sem necessidade de ter várias senhas em cada serviço Web que deseje acessar.

### **3.4 Quais soluções de IdP existem?**

#### **3.4.1 Mozilla Persona**

O Mozilla Persona é um sistema de autenticação descentralizado, projeto iniciado em 2011 e compartilha alguns dos objetivos de sistemas similares como OpenID ou Facebook Connect, mas com algumas diferenças:

- Usa endereços de email como identificador
- Foco na privacidade do usuário
- Forte integração com navegadores web

É baseado no protocolo BrowserID, proposto pela própria Mozilla<sup>13</sup>. A privacidade é um ponto central de preocupação neste protocolo, ele propõe que nem o provedor de identidade nem o outros servidores saibam quais sites o usuário está acessando.

Mais em:

- [http://en.wikipedia.org/wiki/Mozilla\\_Persona](http://en.wikipedia.org/wiki/Mozilla_Persona)
- <https://login.persona.org>
- [https://developer.mozilla.org/en-US/Persona/Implementing\\_a\\_Persona\\_IdP](https://developer.mozilla.org/en-US/Persona/Implementing_a_Persona_IdP)

---

<sup>12</sup><http://cirandas.net>

<sup>13</sup><http://identity.mozilla.com/post/7616727542/introducing-browserid-a-better-way-to-sign-in>



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

**Avaliação:** *Altamente recomendado.*

### 3.4.2 OAuth

OAuth é um padrão aberto para autorização, desenhado especialmente para funcionar sob o protocolo HTTP, essencialmente permite acesso a tokens gerados por servidores de autorização, o cliente usa tal token para acessar serviços protegidos. Ele é complementar, apesar de distinto, ao OpenID.

A maioria dos grandes serviços para Web implementam OAuth, como: Google, Facebook, Yahoo, AOL, Microsoft, PayPal, MySpace, Flickr, entre outros.

Mais em:

- <http://en.wikipedia.org/wiki/OAuth>

Existem algumas preocupações com o OAuth, alguns dos autores iniciais, como o Eran Hammer por exemplo, saíram do projeto apontando<sup>14</sup> uma série de falhas e apontam um novo caminho, como o Oz<sup>15</sup> e Hawk<sup>16</sup> por exemplo, um protocolo de autorização e um esquema de autenticação HTTP, respectivamente.

**Avaliação:** *Apesar dos problemas apontados por alguns desenvolvedores do projeto, OAuth é praticamente um padrão e seu uso é altamente recomendado no portal de participação Participa.br.*

### 3.4.3 OpenID

Sistema de identificação baseado em URL, permite autenticação de usuários a partir de sistemas de autenticação parceiros, usuários podem criar seu acesso onde desejar e logar onde quer que OpenID seja suportado. Alguns exemplos de provedores OpenID: Google, Yahoo!, PayPal, BBC, AOL, LiveJournal e MySpace.

No OpenID os usuários são identificados através de URLs, isto foi fortemente influenciado pelo sistema LID<sup>17</sup>, um sistema online de gerenciamento de identidade digital desenvolvido como parte do NetMesh.

Mais em:

- <http://en.wikipedia.org/wiki/OpenID>

**Avaliação:** *Recomendado.*

---

<sup>14</sup><http://hueniverse.com/2012/07/26/oauth-2-0-and-the-road-to-hell>

<sup>15</sup><https://github.com/hueniverse/oz>

<sup>16</sup><https://github.com/hueniverse/hawk>

<sup>17</sup>[http://en.wikipedia.org/wiki/Light-Weight\\_Identity](http://en.wikipedia.org/wiki/Light-Weight_Identity)



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

### **3.4.4 OpenID Connect**

Camada de autenticação em cima do OAuth 2.0 promovido pelo OpenID Foundation.

Mais em:

- [http://en.wikipedia.org/wiki/OpenID\\_Connect](http://en.wikipedia.org/wiki/OpenID_Connect)
- <http://openid.net/connect>

**Avaliação:** *Recomendado.*

## **4 Outras iniciativas**

### **4.1 OpenAthens - Reino Unido**

Iniciativa de implantação de SSO no Reino Unido, iniciou em instituições de ensino universidades e então pelas instituições de saúde, adota SAML e interfaces via Shibboleth. Em funcionamento desde 1996 com mais de 4.5 milhões de contas de usuários é usado para prover acesso a mais de 300 serviços web distintos, entre universidades e serviços públicos.

Desenvolvido pela empresa Eduserv, uma empresa sem fins lucrativos sediada em Bath-UK:

- <http://www.eduserv.org.uk/services/OpenAthens>

O post no link abaixo fornece uma visão clara de como tudo funciona:

- [http://everything2.com/index.pl?node\\_id=1888399](http://everything2.com/index.pl?node_id=1888399)

Mais em:

- [http://en.wikipedia.org/wiki/Athens\\_access\\_and\\_identity\\_management](http://en.wikipedia.org/wiki/Athens_access_and_identity_management)

### **4.2 Microsoft account**

O Microsoft account, anteriormente conhecido como Windows Live ID é um provedor de identidade para os serviços da Microsoft, está sendo citado aqui apenas para exemplificar uma solução não-livre em produção, existem outras, como o próprio Facebook Connect. O Microsoft account implementa OpenID e é também um provedor de identidade OpenID.

Mais em:

- [http://en.wikipedia.org/wiki/Microsoft\\_account](http://en.wikipedia.org/wiki/Microsoft_account)



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

### **4.3 Liberty Alliance**

Iniciativa entre organizações para promover padrões de federação, IGF, serviços de identidade, etc... submeteu para o OASIS Group a especificação do SAML 2.0, propôs uma série de soluções como: OpenAz, ZXID, etc... As iniciativas deste grupo hoje estão sendo mantidas pelo Kantara Initiative.

Mais em:

- [http://en.wikipedia.org/wiki/Liberty\\_Alliance](http://en.wikipedia.org/wiki/Liberty_Alliance)
- [https://en.wikipedia.org/wiki/Kantara\\_Initiative](https://en.wikipedia.org/wiki/Kantara_Initiative)

## **5 Discussão**

Discussão sobre CAS x OAuth: \* <http://stackoverflow.com/questions/2033026/sso-with-cas-or-oauth/3181557#3181557>

CAS centraliza a autenticação, deve ser usado quando todas as aplicações autenticam numa mesma base de credenciais usuário/senha de usuários.

OpenID decentraliza a autenticação, deve ser usado para aceitar login de qualquer provedor OpenID, mas a aplicação pode restringir quais provedores OpenID aceitar no entanto.

Nem CAS nem OpenID lidam com autorização nativamente.

OAuth lida com autorização, autoriza por exemplo que um site X possa efetuar autenticação a partir de um serviço de autenticação de terceiros Y. OAuth é sobre permitir usuário controlar como seus recursos serão acessados por terceiros.

CAS a partir da versão 3.5 suporta OAuth cliente e servidor<sup>18</sup>.

CASE: OpenSSO foi utilizado pela CPqD para implantar SSO entre diversas aplicações da empresa <https://blogs.oracle.com/s>

CAS é geralmente a escolha preferida para grandes organizações, onde se quer centralizar a base de usuários, exemplo universidades.

Falha grave de segurança: \* <http://research.microsoft.com/apps/pubs/default.aspx?id=160659>

Discussão na visão do pessoal do DACS sobre o porque SSO é pouco adotado no geral: \* <http://dacs.dss.ca/about.html>

---

<sup>18</sup><https://wiki.jasig.org/display/CASUM/OAuth>



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

## **5.1 Iniciativas (Governo e Comunidade)**

### **5.1.1 Login Cidadão**

Projeto piloto desenvolvido pela PROCERGS de um provedor de identidade com base em OAuth para os serviços do governo do estado do Rio Grande do Sul.

Instancia do Login Cidadão rodando em:

- <https://meu.rs.gov.br>

Código fonte, projeto desenvolvido em PHP com framework symfony:

- <https://github.com/PROCERGS/login-cidadao>

A equipe responsável pelo Login Cidadão esteve no Fis15 apresentando a palestra "Login Cidadão: Uma conta. Tudo o que o governo oferece", o vídeo está disponível através do link abaixo:

- <http://hemingway.softwarelivre.org/fis15/high/41f/sala41f-high-201405081612.ogv>

### **5.1.2 Id da Cultura**

O MinC (Ministério da Cultura) iniciou um projeto de provedor OpenID para fornecer identidade centralizada para os serviços Web do MinC e parceiros, o projeto é desenvolvido em Python e o código-fonte está disponível em:

- <https://github.com/hacklabr/iddacultura-provider>

Esta implementação foi posteriormente aproveitada pelo projeto Mapas Culturais do Estado de São Paulo e hoje está sendo utilizado neste projeto, o código utilizado neste projeto está em:

- <https://github.com/hacklabr/mapasculturais-openid>

## **5.2 Proposta para o Participa.BR**

Qual caminho tomar?

Neste contexto de SSO, o Participa.BR tem a necessidade de criar um arranjo de confiança entre alguns sites relacionados ao projeto, inicialmente estes os sites que farão parte deste arranjo são, além do próprio Participa.br são:

- Participatório (gov)
- Cidade Democrática (org)



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

- Cultura Educa (cc/org)

Assim que implementado conectaríamos estes sites acima.

O caminho de implementação pode ser SLTI (gov) ou Serpro (gov/com).

Existem 2 caminhos distintos a adotar: 1) Implementar SSO logo de cara, usar OpenAM ou alguma outra solução de SSO; ou 2) Implementar apenas um provedor de identidade, com base no banco do Participa.br, e permitir que os sites do arranjo loguem através disso

A opção 2) se mostra mais interessante, uma vez que ela é inicialmente menos custosa de implementar, e parte do trabalho (senão todo o trabalho) é aproveitado ao se implementar SSO de verdade futuramente.

Dentre as opções pesquisadas, Mozilla Persona se mostra bastante interessante, uma vez que utiliza um identificador de usuário em formato de email usuario@dominio.com, ao invés de uma URL como é feito no OpenID <http://dominio.com/usuario>

O OpenAM como solução mostra por outro lado uma grande vantagem pois é uma tecnologia já adotada pelo Serpro, o que facilitaria bastante sua implantação caso a solução seja implementada por esta instituição.

OpenAM, provê uma solução completa, provedor de identidade, single sign-on, em um só pacote, seria necessário apenas implementar no Noosfero uma forma de autenticar através da base do OpenAM.

A alternativa mais apropriada é implementar inicialmente suporte a OAuth, OpenID ou Mozilla Persona no Noosfero, implementar tanto o lado cliente quando o lado servidor (provider), isto irá fornecer a infraestrutura básica para num segundo momento implementar Single Sign-on de verdade.

O OpenAM tem suporte a OAuth, OpenID Connect, então é inteiramente possível aproveitar o trabalho feito no momento que for implantar SSO de verdade usando OpenAM, caso seja esta a solução eleita.

## **6 Considerações finais**

Neste documento foi apresentado um "Documento com análise de arquiteturas de sistemas de identidade distribuída, estratégia de implantação considerando os sites parceiros e contendo propostas de códigos."

Lembramos que para tornar o Portal de Consulta Pública realmente um canal de consulta e participação popular na discussão e na definição da agenda prioritária do país, é necessário que além de documentação faça-se um esforço de movimentar as pessoas fora do ambiente virtual, para que haja um engajamento no uso e contribuição deste projeto de forma consistente e perene.

Sem mais nada a acrescentar, coloco-me à disposição.



**PRESIDÊNCIA DA REPÚBLICA**  
**SECRETARIA-GERAL**  
Secretaria-Executiva

Brasília/DF, 21 de Abril de 2014

**Joenio Marques da Costa**  
Consultor do PNUD