**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

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

# Sumário

# Lista de Figuras

# 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[1]. 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[2] 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 redobradas. 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.

## 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[3] 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[4], todas elas se tornaram obsoletas após a recomendação do W3C chamada "Web Messaging"[5], uma técnica que permite documentos em diferentes domínios compartilhar dados. A maioria dos Navegadores Web atuais implementam Web Messaging[6] [7] [8].

## 2.4 Como SSO funciona?

Existem muitas formas de implementar SSO: Kerberos, Smart card, CAS, OTP, entre outras, cada uma com sua própria estratégia[9]. A solução SiteMinder[10] da "CA Technologies", por exemplo, implementa SSO da seguinte forma[11]:

- 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.

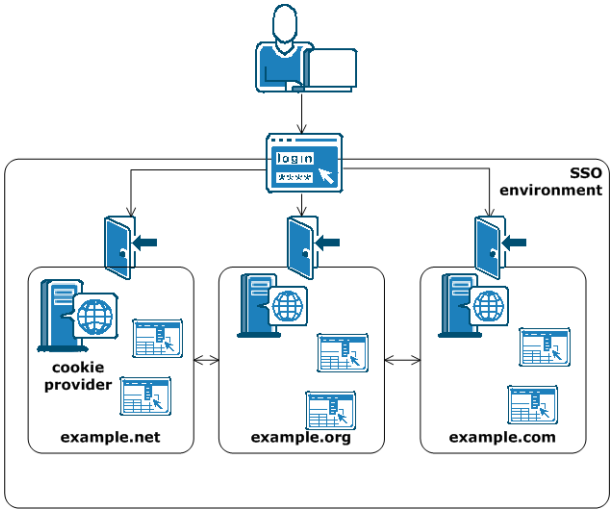


Figura 1: Exemplo de implementação de SSO do SiteMinder

## 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:

- 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

**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 atenticidade 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[12], existem implementações oficiais de cliente em várias linguagens, como: .NET, PHP, Perl, Apache, etc. A partir da versão 3.5 adicionou suporte a OAuth[13], tanto cliente quanto servidor.

O artigo *Approaches and challenges for a single sign-on enabled extranet using Jasig CAS*[14] 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.

CAS centraliza a autenticação e é recomendável de ser utilizado quando todas as aplicações autenticam numa mesma base de credenciais de autenticação. É geralmente a melhor escolha para grandes organizações, onde se quer centralizar a base de usuários, como universidades por exemplo.

Mais em:

- http://en.wikipedia.org/wiki/Central_Authentication_Service
- 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.*

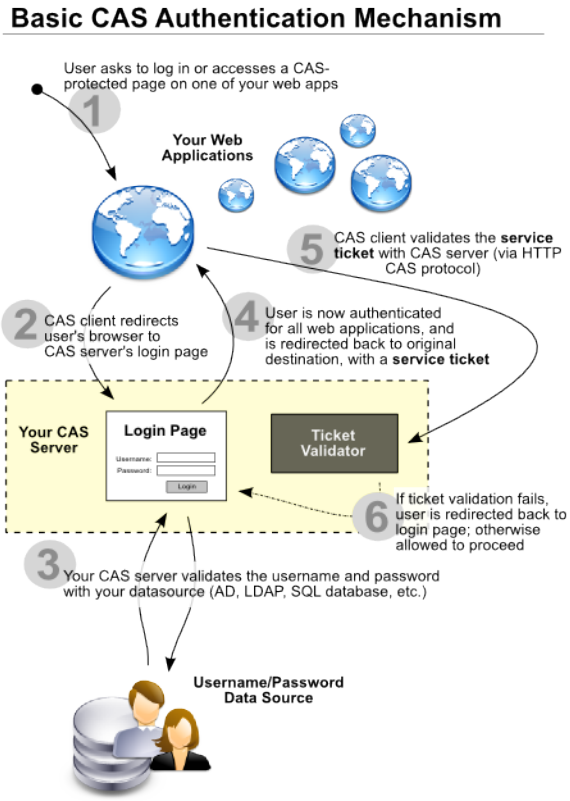


Figura 2: Diagrama do RubyCAS, implementação do protocolo CAS em Ruby

### 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[15].

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

Mais em:

- http://en.wikipedia.org/wiki/Distributed_Access_Control_System_(DACS)
- https://wiki.debian.org/DebianSingleSignOn

**Avaliação:** *Recomendado.*

### 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[16].

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

Mais em:

- 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 incialmente 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:

- http://en.wikipedia.org/wiki/IBM_Enterprise_Identity_Mapping

**Avaliação:** *Voltado apenas para integrar soluçoes 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 inclue:

- 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

**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 mútiplos 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)

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

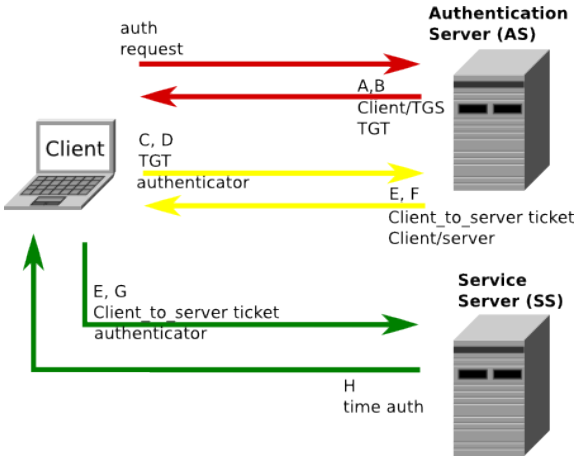


Figura 3: Diagrama de negociação do Kerberos

### 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.

O OpenSSO, projeto que deu origem ao OpenAM, foi utilizado pela CPqD para implantar Single Sign-on entre diversas aplicações e é um bom caso de uso desta plataforma em um ambiente real, mais detalhes no link abaixo:

- https://blogs.oracle.com/superpat/entry/opensso_at_cpqd

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

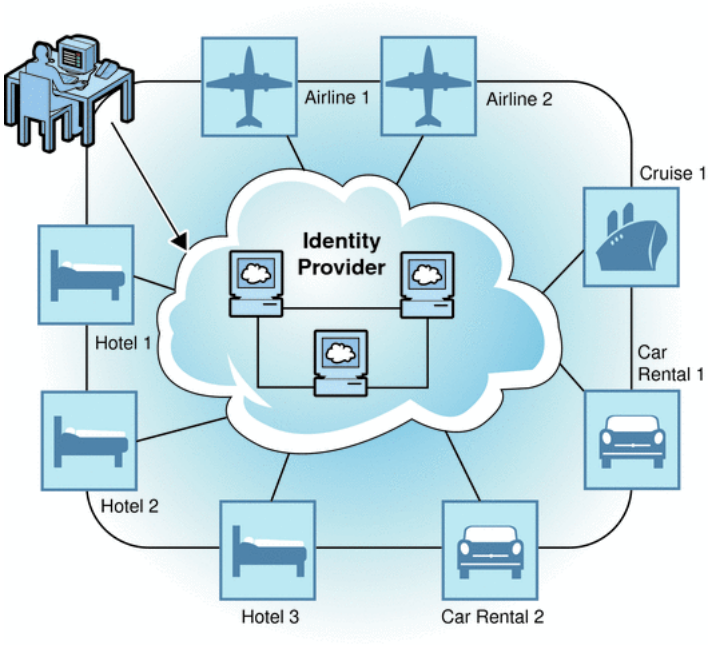


Figura 4: Exemplo de federação com OpenAM para um portal de viagens

Mais em:

- 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.

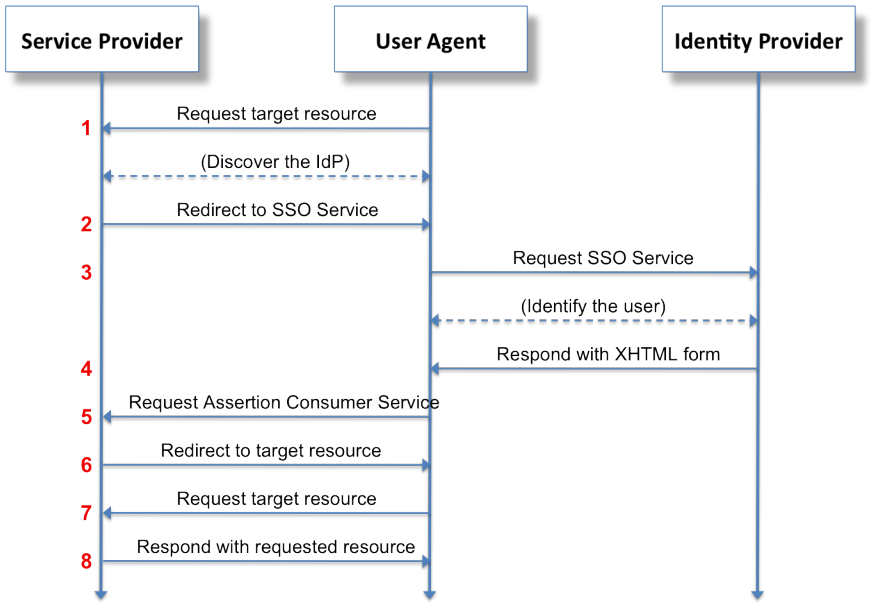


Figura 5: Single Sign-on com SAML2

Mais em:

- http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

**Avaliação:** *Não uma solução de SSO em sí, 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)

**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 Reuino Unido chamada OpenAthens.*

#### 2.5.14 ZXID

Kit de gerenciamento de identidade SAML 2.0. Compatícel co SAML 2.0, Liberty ID-WSF 2.0 e XACML 2.0. Implementado em C com, possui poucas dependencias 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, afim de verificar a autenticidade.

Um provedor de identidade fornece uma alternativa para que vários serviços web distintos autentiquem 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 os 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://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 entando existe uma implementação não-oficial em uso na rede Cirandas.net[17] 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[18]. 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
- https://login.persona.org
- https://developer.mozilla.org/en-US/Persona/Implementing_a_Persona_IdP

**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.

OAuth autoriza, por exemplo, que um site X possa efetuar autenticação a partir de um serviço de autenticação Y. Ele permite que os usuários controlem como os seus recursos serão acessados por terceiros. A maioria dos grandes serviços para Web implementam OAuth, como: Google, Facebook, Yahoo, AOL, Microsoft, PayPal, MySpace e Flickr.

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[19] uma série de falhas e apontam um novo caminho, como o Oz[20] e Hawk[21] 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 influencido pelo sistema LID[22], um sistema online de gerenciamento de identidade digital desenvolvido como parte do NetMesh.

OpenID decentraliza a autenticação, recomenda-se seu uso quando se quer aceitar login de qualquer provedor OpenID, mas esse comportamento pode ser alterado configurando a aplicação para restringir quais provedores OpenID são aceitos.

Mais em:

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

**Avaliação:** *Recomendado.*

### 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://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, 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.

Mais em:

- http://www.eduserv.org.uk/services/OpenAthens
- http://en.wikipedia.org/wiki/Athens_access_and_identity_management
- http://everything2.com/index.pl?node_id=1888399

## 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 cidado 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

## 4.3 Liberty Alliance

Iniciativa para promover padrões de federação, IGF, serviços de identidade, etc. Submeteu para o OASIS Group a especificação do SAML 2.0, propôs uma séries de soluções como OpenAz e ZXID por exemplo. As iniciativas deste grupo hoje estão sendo mantidas pelo Kantara Initiative.

Mais em:

- http://en.wikipedia.org/wiki/Liberty_Alliance
- https://en.wikipedia.org/wiki/Kantara_Initiative

# 5 Discussão

## 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.

Uma instancia do Login Cidadão pode ser encontrada em:

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

Código fonte do projeto desenvolvido em PHP com base no framework symfony pode ser obtido a partir do seguinte link:

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

A equipe responsável pelo Login Cidadão esteve no Fisl15 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/fisl15/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 desde então tem sido sendo utilizada por este projeto, o código fonte pode ser encontrado em:

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

## 5.2 Proposta para o Participa.BR

O Participa.BR tem a necessidade de criar um arranjo de confiança entre alguns sites parceiros, neste arranjo de confiança um ambiente de Single Sign-on será implementado, os sites parceiros são:

- Participatório (gov)
- Cidade Democrática (org)
- Cultura Educa (cc/org)

Para isso propõe-se dividir o trabalho em duas etapas:

1. Implementar um provedor de identidade
2. Implementar SSO usando umas das soluções recomendadas

Esta estratégia permite ter com pouco investimento um provedor de identidade em produção sendo utilizado pelos sites parceiros, o que já proporciona grande parte do que se espera de um ambiente de Single Sign-on.

Lembrando que o desenvolvimento de um provedor de identidade envolve implementação tanto do lado do Participa.BR quanto do lado dos sites parceiros, então é importante lembrar que será preciso contar também com a colaboração das equipes que mantém tais sites.

Nesta proposta o Participa.BR será o provedor de identidade e os sites parceiros serão clientes. Os usuários de tais sites poderão efetuar login através de seus usuários no Participa.BR.

A melhor opção para implementar este provedor é o Mozilla Persona e o OAuth, o Mozilla Persona por ter uma grande preocupação com a privacidade do usuário onde não toma conhecimento e nem armazena quais sites o usuário visita e o OAuth por ser amplamente adotado e possuir inúmeras implementações em diversas linguagens, o que facilita bastante sua implementação. O Mozilla Persona tem uma vantagem adicional, que apesar de ser uma vantagem estética deve ser levada em consideração, a identificação de um usuário através do Mozilla Persona é no formato nome@provedor, semelhante à um endereço de email, isto é de fato a melhor forma de identificar alguém na internet, é semanticamente auto-explicativo e por sí já é um formato bastante adequado para ambientes federados.

A partir daí, já com o Participa.BR sendo um provedor de identidade, inicia-se o desenvolvimento da segunda etapa que é implementar SSO real usando uma das opções recomendadas. Dentre as opções recomendadas, destaca-se:

- CAS
- DACS
- OpenAM

A decisão de qual plataforma utilizar depende de fatores que fogem ao escopo deste documento, um deles é a experiência da equipe que irá implementar tal solução. Que poderá influenciar fortemente por uma ou outra solução.

Mas a princípio é importante destacar as vantagens de cada solução, o CAS é um protocolo extremamente maduro para federação com uma implementação de mesmo nome mantido pelo grupo Jasig, tal implementação é bastante difundida, tendo seu último release v4.0.0 lançado em Maio de 2014, portanto em desenvolvimento ativo. O projetos DACS é um sistema leve de SSO escrito em C/C++, ele é utilizado pelo projeto Debian, um projeto de desenvolvimento de um sistema operacional baseado em GNU/Linux, o Debian é um grande projeto com uma equipe altamente especializada, o uso do DACS por parte deste projeto é um sinal de maturidade do DACS e um bom caso de sucesso de uso desta ferramenta, por conta disto ele está entre as soluções recomendadas. O OpenAM é uma implementação em Java para federação com suporte a Single Sign-on, madura, amplamente utilizada, possui suporte a mais de vinte tipos de autenticação, dentre elas LDAP, suporte a autorização via OAuth, o que casa perfeitamente com a proposta de implementar no Participa.BR um provedor de OAuth.

Resumindo, a solução de SSO para o Participa.BR será composta de Mozilla Persona e OAuth como provedores de identidade. E CAS, DACS ou OpenAM como plataforma de Single Sign-on integrando com o provedor de identidade previamente implementado. Novamente destaco que qualquer das solução de SSO listadas acima atendem às necessidades do projeto Participa.BR e a escolha dependerá da experiência da equipe que desenvolverá tal solução.

# 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 pessoar 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.

Brasília/DF, 21 de Abril de 2014

**Joenio Marques da Costa**
Consultor do PNUD

## Referências

[1] "Single sign-on - wikipedia," http://en.wikipedia.org/wiki/Single_sign-on - Acessado em 22 de Maio de 2014.

[2] *Authentication server - Wikipedia*. http://en.wikipedia.org/wiki/Authentication_server - Acessado em 22 de Maio de 2014.

[3] *Same origin policy - Wikipedia*. https://en.wikipedia.org/wiki/Same-origin_policy - Acessado em 05 de Junho de 2014.

[4] *Single Sign On with Ajax in same origin policy world - effective solutions - Stackoverflow*. http://stackoverflow.com/questions/7094967/single-sign-on-with-ajax-in-same-origin-policy-world-effective-solutions - Acessado em 05 de Junho de 2014.

[5] *Web Messaging - W3C*. http://www.w3.org/TR/webmessaging/ - Acessado em 05 de Junho de 2014.

[6] *Web Messaging - Wikipedia*. http://en.wikipedia.org/wiki/Web_Messaging - Acessado em 05 de Junho de 2014.

[7] *Designing single-sign-on with JSONP/CORS? - Stackexchange*. http://security.stackexchange.com/questions/36753/designing-single-sign-on-with-jsonp-cors - Acessado em 14 de Junho de 2014.

[8] *Web Messaging API - .openBlog()*. http://openblog.github.io/2013/02/25/html5-web-messaging-api/ - Acessado em 14 de Junho de 2014.

[9] *Introduction to Single Sign-On - The Open Group*. http://www.opengroup.org/security/sso/sso_intro.htm - Acessado em 05 de Junho de 2014.

[10] *SiteMinder - CA Technologies*. http://www.ca.com/br/products/detail/ca-siteminder.aspx - Acessado em 22 de Maio de 2014.

[11] *SSO SiteMinder DOCS - CA Technologies*. http://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%205-ENU/Bookshelf_Files/HTML/idocs/256655.html - Acessado em 22 de Maio de 2014.

[12] *Jasig Group*. http://www.jasig.org - Acessado em 06 de Junho de 2014.

[13] *OAuth - CAS User Manual - Jasig Wiki*. https://wiki.jasig.org/display/CASUM/OAuth - Acessado em 06 de Junho de 2014.

[14] R. P. Florian Holzschuher, “Approaches and challenges for a single sign-on enabled extranet using jasig cas,” 2013.

[15] Y. Gershteyn, “Web services: Role based access control with single sign-on architecture,” 2008.

[16] *XACML - Wikipedia*. http://en.wikipedia.org/wiki/XACML - Acessado em 10 de Junho de 2014.

[17] *Cirandas - Rede social e econômica de empreendimentos solidários*. http://cirandas.net - Acessado em 10 de Junho de 2014.

[18] *Introducing BrowserID: A better way to sign in*. http://identity.mozilla.com/post/7616727542/introducing-browserid-a-better-way-to-sign-in - Acessado em 10 de Junho de 2014.

[19] *OAuth 2.0 and the Road to Hell*. http://hueniverse.com/2012/07/26/oauth-2-0-and-the-road-to-hell - Acessado em 10 de Junho de 2014.

[20] *OZ - Web Authorization Protocol*. https://github.com/hueniverse/oz - Acessado em 12 de Junho de 2014.

[21] *Hawk - HTTP Holk Authentication Scheme*. https://github.com/hueniverse/hawk - Acessado em 12 de Junho de 2014.

[22] *Light-Weight Identity - Wikipedia*. http://en.wikipedia.org/wiki/Light-Weight_Identity - Acessado em 12 de Junho de 2014.