**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 um guia de codificação "coding guidelines"para o desenvolvimento do código do portal objetivando o reaproveitamento de código e o fomento à formação de comunidades em torno dos módulos, bem como tutoriais para implementação local das soluções.

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 de software relacionados, mas independentes. Com esta propriedade o usuário loga apenas uma vez e ganha acesso a outros sistemas que façam parte do mesmo ambiente de SSO sem necessidade de fornecer usuário/senha diversas vezes. Reciprocamente, single sign-off é a propriedade do usuário deslogar e automaticamente deslogar de 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 usuário/senha 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 usuário/senha, 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 deste serviço, uma vez que sua queda implica em indisponibilidade dos serviços que fazem parte do ambiente de SSO.

[1] http://en.wikipedia.org/wiki/Single_sign-on
[2] http://en.wikipedia.org/wiki/Authentication_server

## 2.2 SSO no Noosfero

O Noosfero não implementa mecanismos de SSO, nem há referências na comunidade de utilização dele num ambiente de SSO. 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 armazenado 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.

Este problema é resultado de 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 outro domínio, isso previne, por exemplo, ataques de cross-site scripting.

Inúmeras soluções foram propostas para contornar esta limitação, 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 compartilar dados. A maioria dos Navegadores Web atuais implementam Web Messaging [6].

[3] https://en.wikipedia.org/wiki/Same-origin_policy
[4] http://stackoverflow.com/questions/7094967/single-sign-on-with-ajax-in-same-origin-policy-world-effective-solutions
[5] http://www.w3.org/TR/webmessaging/
[6] http://en.wikipedia.org/wiki/Web_Messaging

## 2.4 Como funciona?

Existem várias tecnologias para implementar SSO: Kerberos, Smart card, OTP, entre outras. Dependendo da solução as seguintes estratégias podem ser utilizadas [7]:

- As credenciais do usuário são passadas para um segundo domínio quando este acessa o segundo domínio.
- As credencias do usuário são obtidas de uma base de informação de gerenciamento de single sign-on.
- São estabelecidas várias sessões de login com todas as aplicações no momento em que se estabelece a primeira sessão.
- Armazenar temporariamente no cache e usar ao fazer requisição num segundo domínio.

A solução SiteMinder [8] da "ca technologies", por exemplo, implementa SSO da seguinte forma [9]:

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

A Figura 1 traz um diagrama exemplificando esta solução.

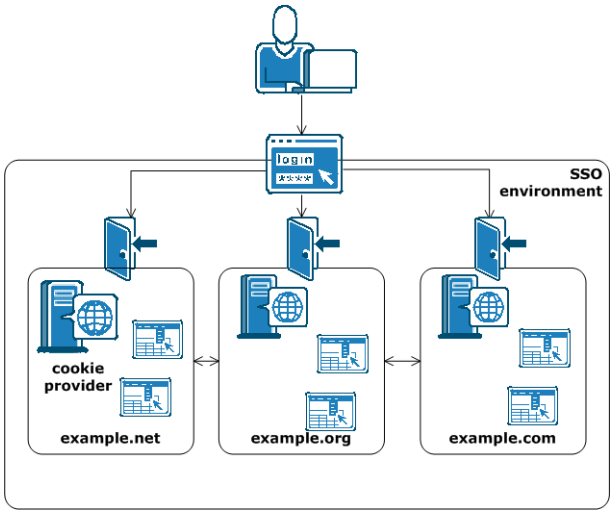


Figura 1: Exemplo de implementação de SSO do SiteMinder

[7] http://www.opengroup.org/security/sso/sso_intro.htm
[8] http://www.ca.com/br/products/detail/ca-siteminder.aspx
[9] http://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%205-ENU/Bookshelf_Files/HTML/idocs/256655.html

Este é apenas um exemplo de implementação, a solução SiteMinder é um sistema centralizado de gerenciamento de acesso Web da empresa CA Tecnologies, que implementa uma série de soluções e SSO.

## 2.5 Quais soluções existem?

Quais soluções estão disponíveis para quem quer implementar SSO? Segue uma lista baseada no artigo da Wikipedia [10] com soluções em software livre para SSO:

### 2.5.1 Accounts & SSO

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

Mais em:

- http://en.wikipedia.org/wiki/Accounts_&_SSO

### 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 que ocorre durante a autenticação é o seguinte:

- Cliente visita uma aplicação requisitando 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, CAS retorna o cliente para a aplicação, passando um ticket de segurança
- A aplicação valida o ticket contactando CASC
- AS then gives the application trusted information about whether a particular user has successfully authenticated

A implementação oficial do CAS é em Java e mantido pelo grupo JASIG [11], existem implementações oficiais do lado cliente em várias linguagens, .NET, PHP, Perl, Apache, etc.

Mais em:

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

[10] http://en.wikipedia.org/wiki/List_of_single_sign-on_implementations
[11] http://www.jasig.org

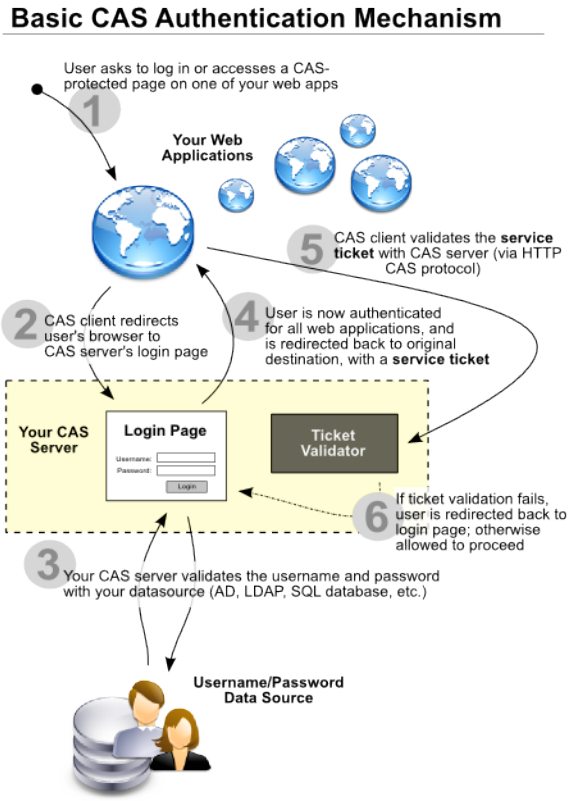


Figura 2: Diagrama do RubyCAS, implementação do protocolo CAS em Ruby

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

### 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 para os desenvolvedores do projeto, ver mais em:

Mais em:

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

### 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 [12].

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

Mais em:

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

### 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.

Na versão 3.0.0 usa Samba para integrar com Microsoft Active Directory.

Mais em:

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

### 2.5.6 IBM Enterprise Identity Mapping

Framework para mapear identidades de usuários em várias plataformas distintas, com poucas informações na Web, aparentemente apenas para integrar as soluçoes da própria IBM.

Mais em:

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

### 2.5.7 JBoss SSO

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

[12] http://en.wikipedia.org/wiki/XACML

Dentre várias funcionalidades o JBoss SSO inclue:

- Interação 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

### 2.5.8 JOSSO

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

Mais em:

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

### 2.5.9 Kerberos

Protocolo de autenticação em rede baseado em 'tickets para permitir nós se comunicar sob uma rede não-segura para provar sua identidade para outro de forma segura. Seus designers objetivaram principalmente como um modelo cliente-servidor e isso provê autenticação tanto de usuários quanto de servidores. Veja Figura 3 para exemplo de negociação com o Kerberos.

Mais em:

- http://en.wikipedia.org/wiki/Kerberos_(protocol)

### 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 emplementa sistema de autorização baseado em XACML. Veja exemplo na Figura 4 de uso do OpenAM em um portal de viagens.

Mais em:

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

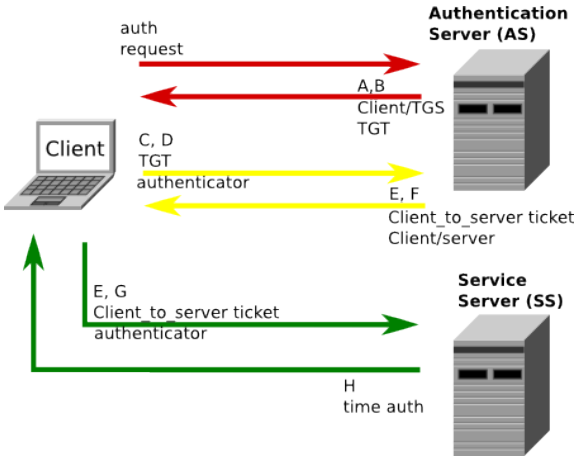


Figura 3: Diagrama de negociação do Kerberos

### 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

O ultimo release do projeto é de 2010, um pouco antigo.

Mais em:

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

### 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:

- o principal (tipicamente um usuário)
- o provedor de identidade (IdP)

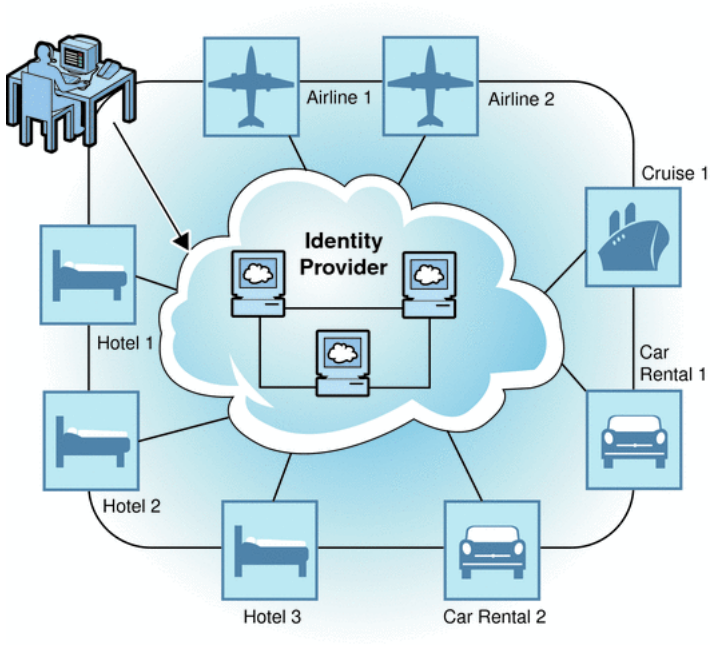


Figura 4: Exemplo de federação com OpenAM para um portal de viagens

- o provedor de serviço (SP)

A interação entre eles está representada na Figura 5.

Mais em:

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

#### 2.5.13 Shibboleth

Middleware para SSO e autenticação baseado em SAML.

Mais em:

- http://en.wikipedia.org/wiki/Shibboleth_(Internet2)

#### 2.5.14 ZXID

kit de gerenciamento de identidade SAML 2.0

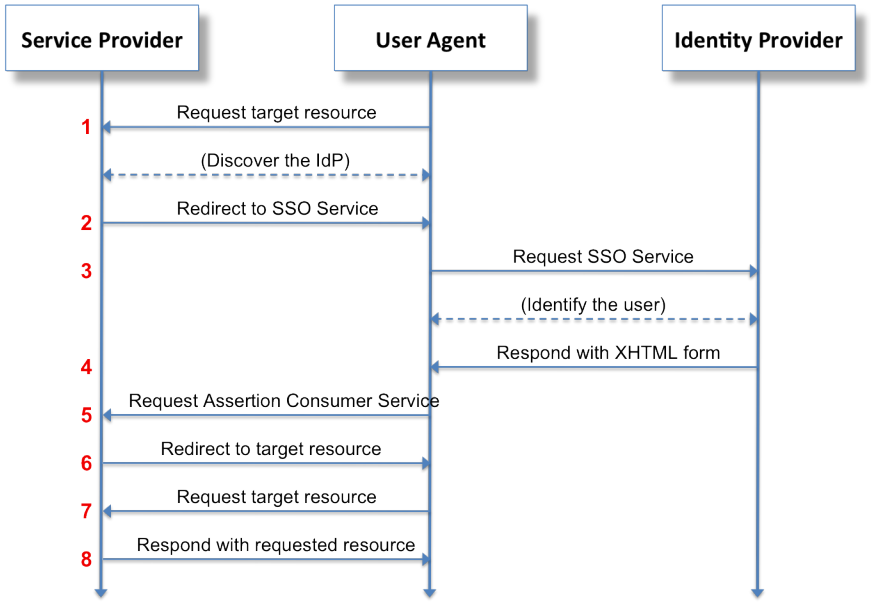


Figura 5: Single Sign-on com SAML2

Compatícel co SAML 2.0, Liberty ID-WSF 2.0 e XACML 2.0. Implementado em C com poucas dependencias externas, com bibliotecas para PHP, Perl e Java via SWIG.

Mais em:

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

# 3 IdP - Identity Provider

## 3.1 O que é IdP?

Identity Provider, ou Provedor de Identidade, é um 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 dos atores, normalmente usuários.

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 autentique 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

Em um ambiente SSO um 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 provedor de identidade (IdP) sozinho não garante Single Sign-on (SSO), um IdP é normalmente parte de um ambiente de SSO, normalmente um primeiro passo para ter um ambiente SSO é implantar um serviço de IdP.

Definição de IdP segundo a OASIS:

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

Mais sobre esses termos pode ser encontrado em:

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

Mais sobre Identity Provider em:

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

## 3.2 IdP no Noosfero

O Noosfero não implementa oficialmente integração de nenhum protocolo ou tecnologia de provedor de identidade, no entando existe uma implementação não-oficial em uso na rede Cirandas.net [13] de uso do OAuth e do Mozilla Persona, o código fonte desta implementação não-oficial, ainda não integrada ao repositório oficial do Noosfero na seguinte URL:

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

[13] http://cirandas.net

## 3.3 Resolve qual problema?

Um usuário criar 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, isso facilita por exemplo quando o usuário precisa alterar sua senha, pois em apenas um único ponto ele altera a senha de acesso a diversos sistemas, de uma só vez.

## 3.4 Quais soluções 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

A motivação pela privacidade está no fato de que um provedor de identidade não deve saber quais sites o usuário está se identificando.

Mais em:

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

Thread sobre SSO com Persona: * https://groups.google.com/forum/#!topic/mozilla.dev.identity/oNseXZxbVUQ

Baseado no protocolo BrowserID prototipado pela Mozilla. * http://identity.mozilla.com/post/7616727542/introducing-browserid-a-better-way-to-sign-in

A Mozilla disponibiliza uma instancia do Persona rodando em:

- https://login.persona.org

Mas é possível rodar um proprio servidor Persona seguindo a seguinte instruções:

- https://developer.mozilla.org/en-US/Persona/Implementing_a_Persona_IdP

### 3.4.2 OAuth

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

A maioria dos grandes serviços para Web implementam ele, como: Google, Facebook, Yahoo, AOL, Microsoft, PayPal, MySpace, and Flickr entre outros. Ainda, a maioria dos serviços de email provêem serviço de autorização via OAuth.

Mais em:

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

Existem algumas preocupações com o OAuth como descrito no link abaixo, alguns dos autores iniciais do protocolo saíram do projeto apontando uma série de falhas no protocolo, mas não chegam a recomendar o desuso dele, apenas apontam para um novo e melhor caminho que não é possível incluir no OAuth por força das organizações que fazem partem do comitê que define o padrão, um deles é o Eran Hammer que propôs duas novas soluções, Oz e o Hawk.

- http://hueniverse.com/2012/07/26/oauth-2-0-and-the-road-to-hell
- https://github.com/hueniverse/oz
- https://github.com/hueniverse/hawk

### 3.4.3 OpenID

Sistema de identificação baseado em URL. Permite autenticação de usuários usando parceiros para autenticação, usuários podem criar seu acesso onde desejar e logar onde quer que OpenID seja suportado.

Usuários podem criar contas com seu provedor de identidade OpenID preferido e então usar sua conta para logar em qualquer outro sistema Web que aceite autenticação com OpenID. Alguns provedores de OpenID hoje são: Google, Yahoo!, PayPal, BBC, AOL, LiveJournal, MySpace, IBM, etc.

O sistema que influenciou identificação baseado em URL no OpenID foi o LID:

- http://en.wikipedia.org/wiki/Light-Weight_Identity

Mais em:

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

### 3.4.4 OpenID Connect

Camada de autenticação em cima do OAuth 2.0, um framework de autorização, promovido pelo OpenID Foundation.

Mais em:

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

# 4 Outras iniciativas

## 4.1 OpenAthens - Reino Unido

Athens, iniciativa do 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

Mais em:

- 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 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 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 séries 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
- https://en.wikipedia.org/wiki/Kantara_Initiative

# 5 Discussão

Discussao 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 entando.

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 [14].

CASE: OpenSSO foi utilizado pela CPqD para implantas SSO entre diversar aplicações da empresa https://blogs.oracle.com/s

CAS é geralmente a escolhe preferida para grande 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

Discussao na visao do pessoal do DACS sobre o porque SSO é pouco adotado no geral: * http://dacs.dss.ca/about.html

## 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 rodandm 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 Fisl15 apresentando a palestra "Login Cidadão: Uma conta. Tudo o que o governo oferece", o vídeo está disponível através do link abaixo:

[14] https://wiki.jasig.org/display/CASUM/OAuth

- 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 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)
- Cultura Educa (cc/org)

Assim que implementado conectaríamos:

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

# 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