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:

- 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.

(daqui para baixo são informações anotadas de forma desordenada)

Fonte: http://www.opengroup.org/security/sso/sso_intro.htm

Exemplo de implementação de SSO para múltiplos domínios da solução SiteMinder (http://www.ca.com/br/products/detail/ca siteminder.aspx), solução da "ca technologies"para implantar SSO, federação, etc.

* 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

Imagem com diagrama dessa solução: http://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%205-ENU/Bookshelf_File

Fonte: http://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%205-ENU/Bookshelf_Files/HTML/idocs/256655.html

2.5 Quais soluções existem?

Lista de implementações para SSO: * http://en.wikipedia.org/wiki/List_of_single_sign-on_implementations

Abaixo apenas as soluções livres.

Accounts & SSO - Solução de SSO para computadores (apenas cliente) http://en.wikipedia.org/wiki/Accounts_%26_SSO

Central Authentication Service (CAS) - Protocolo Web (servidor) de SSO http://en.wikipedia.org/wiki/Central_Authentication

Como funciona: http://rubycas.github.io/images/basic_cas_single_signon_mechanism_diagram.png

(tem pacote Debian)

Distributed Access Control System (DACS) - SSO leve e controle de acesso basead em papéis para WEB http://en.wikipedia.org/wiki/Distributed_Access_Control_System_(DACS)

(não inclui sistema de autenticação mas suporta muitos métodos, X.509, PAM, LDAP, etc...)

Enterprise Sign On Engine - Plataforma de SSO, controle de acesso e federação http://en.wikipedia.org/wiki/Enterprise_Sign_

FreeIPA - Solução da RedHat para SSO, Policy and Audit, ... http://en.wikipedia.org/wiki/FreeIPA

IBM Enterprise Identity Mapping - http://en.wikipedia.org/wiki/IBM_Enterprise_Identity_Mapping

JBoss SSO - single sign-on, sign-off, federação http://en.wikipedia.org/wiki/JBoss_SSO

JOSSO - SSO para aplicações web, Java EE http://en.wikipedia.org/wiki/JOSSO

Kerberos - Protocolo de autenticação em rede http://en.wikipedia.org/wiki/Kerberos_(protocol)

OpenAM - controle de acesso e federação, engloba uma série de soluções http://en.wikipedia.org/wiki/OpenAM

Mozilla Persona - Não é SSO, mas sim sistema de autenticação descentralizado http://en.wikipedia.org/wiki/Mozilla_Persona

Pubcookie - Protocolo (e software) de SSO http://en.wikipedia.org/wiki/Pubcookie

SAML - Linguagem de marcação para definir comunicação sobre autenticação e autorização http://en.wikipedia.org/wiki/Secu

Shibboleth - SSO e autenticação http://en.wikipedia.org/wiki/Shibboleth_(Internet2)

ZXID - kit de gerenciamento de identidade SAML 2.0 http://en.wikipedia.org/wiki/ZXID

* Ler sobre protocolo CAS: http://www.jasig.org/cas/protocol

Existe um protocolo para implementar SSO: * http://en.wikipedia.org/wiki/Central_Authentication_Service

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

2.6 Discussão sobre vantagens desvantagens de cada solução

Riscos: * https://blog.perfectcloud.io/does-facebook-federation-have-your-best-interests-at-heart-2/

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

2. Identidade Digital / Autenticação

Uma solução de SSO não implica em serviço de identidade centralizada, ou seja, os sites envolvidos em SSO não necessariamente utilizam um sistema de autenticação em de um servidor de identidade contralizada

O que é? Resolve qual problema? Como funciona? Quais soluções existem?

OAuth OpenID OpenID Connect Etc...

Comparativo entre soluções (vantagens desvantagens)

3. Iniciativas em andamento (Governo e Comunidade)

4. Proposta de solução para o Participa.BR (qual caminho tomar)

4.1 Objetivo

Nosso objetivo é que esse arranjo de confiança do Participa.br possa ser utilizado por plataformas de participação social do governo (gov) e da sociedade (org). Assim que implementado conectaríamos:

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

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

3 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