Uma aplicacação de privacidade no gerenciamento de identidades em nuvem com uApprove

Daniel Ricardo dos Santos

Universidade Federal de Santa Catarina

10 de novembro de 2011

Agenda

Motivação

- Migração de serviços para as nuvens;
- Necessidade de autenticação;
- Preocupação crescente com privacidade;

Problema e Objetivo

Problema

Falta de mecanismos de proteção à privacidade em sistemas de gerenciamento de identidades.

Objetivo

Inserir o gerenciamento de identidades com proteção à privacidade em ambientes de computação em nuvem.

Agenda

O que é

Identidades digitais são coleções de dados que representam atributos ou características de uma entidade [Windley 2005].

Funcionam como um meio de autenticação e autorização e são utilizadas em diversos cenários, entre os quais podemos destacar: comércio eletrônico, governo eletrônico, redes sociais, *e-mail*, finanças e saúde online.

Sistemas de Gerenciamento de Identidades

Um serviço de gerenciamento de identidades pode ser definido como "o processo de criação, gerenciamento e utilização de identidades de usuários e a infraestrutura que suporta esse processo." [Lee et al. 2009]

Muitas vezes as informações associadas a uma identidade são sensíveis, como no caso de dados médicos e financeiros. Por causa da natureza privada e sensível dessas informações associadas os sistemas de gerenciamento de identidades devem ser seguros e confiáveis.

Papéis

Os seguintes papéis são desempenhados num sistema de gerenciamento de identidades [Bertino e Takahashi 2011]:

Usuário Possui uma identidade e utiliza os serviços do IdP e do SP;

Provedor de Identidades (IdP) Fornece os serviços de gerenciamento de identidades;

Provedor de Serviços (SP) Fornece os serviços que o usuário efetivamente deseja utilizar, como *e-mail*, *e-commerce* e outros. Delega a autenticação e autorização dos usuários a um IdP.

Agenda

Conceitos Básicos

Privacidade relaciona-se com a capacidade de um indivíduo proteger informações sobre si [Mather et al. 2009].

O Fair Information Practice Principles (FIPS) é um conjunto de regras para manipulação de informações com proteção à privacidade que regula o uso de informações privadas nos Estados Unidos e serve de base para regras de outros países [Federal Trade Comission 2011]. Os FIPs definem cinco princípios básicos.

Princípios

Advertência/Consciência Os usuários devem ser avisados das práticas de uma entidade que irá manipular informações sensíveis antes que qualquer informação seja coletada;

Escolha/Consentimento Dar aos usuários opções sobre como quaisquer dados coletados serão utilizados;

Acesso/Participação Possibilidade de um usuário acessar as informações coletadas sobre si e poder alterar esses valores;

Integridade/Segurança Coleta de dados a partir de fontes confiáveis e armazenamento seguro;

Cumprimento/Reparação Garantias de que os princípios serão respeitados.

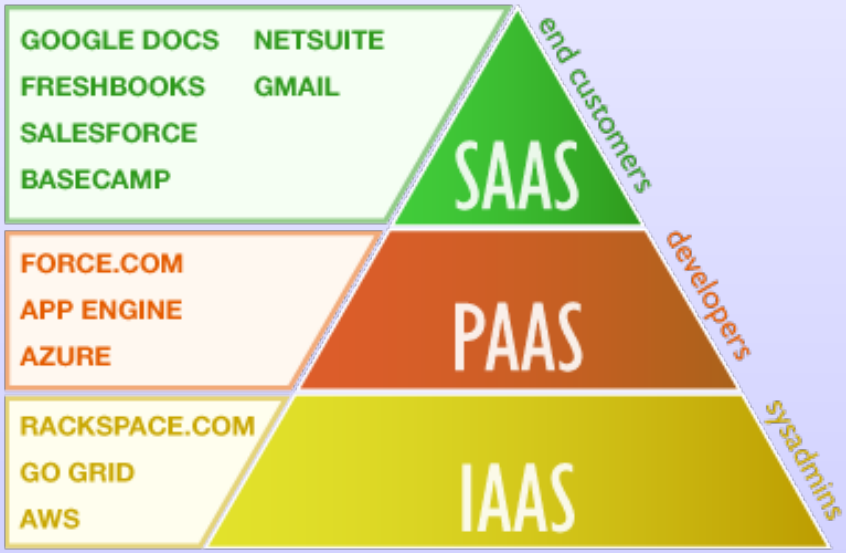
Agenda

Definição

O trabalho de [Marston et al. 2011] define computação em nuvem da seguinte forma: "É um modelo de serviço de tecnologia da informação onde os serviçs computacionais (ambos hardware e software) são entregues sob demanda para os usuários através de uma rede na forma de **auto-atendimento**, independente de dispositivo e de localização. Os recursos necessários para fornecer os diferentes níveis de qualidade de serviçoo são **compartilhados**, dinamicamente **escaláveis**, alocados rapidamente, **virtualizados** e liberados com **interação mínima com o provedor de serviço**".

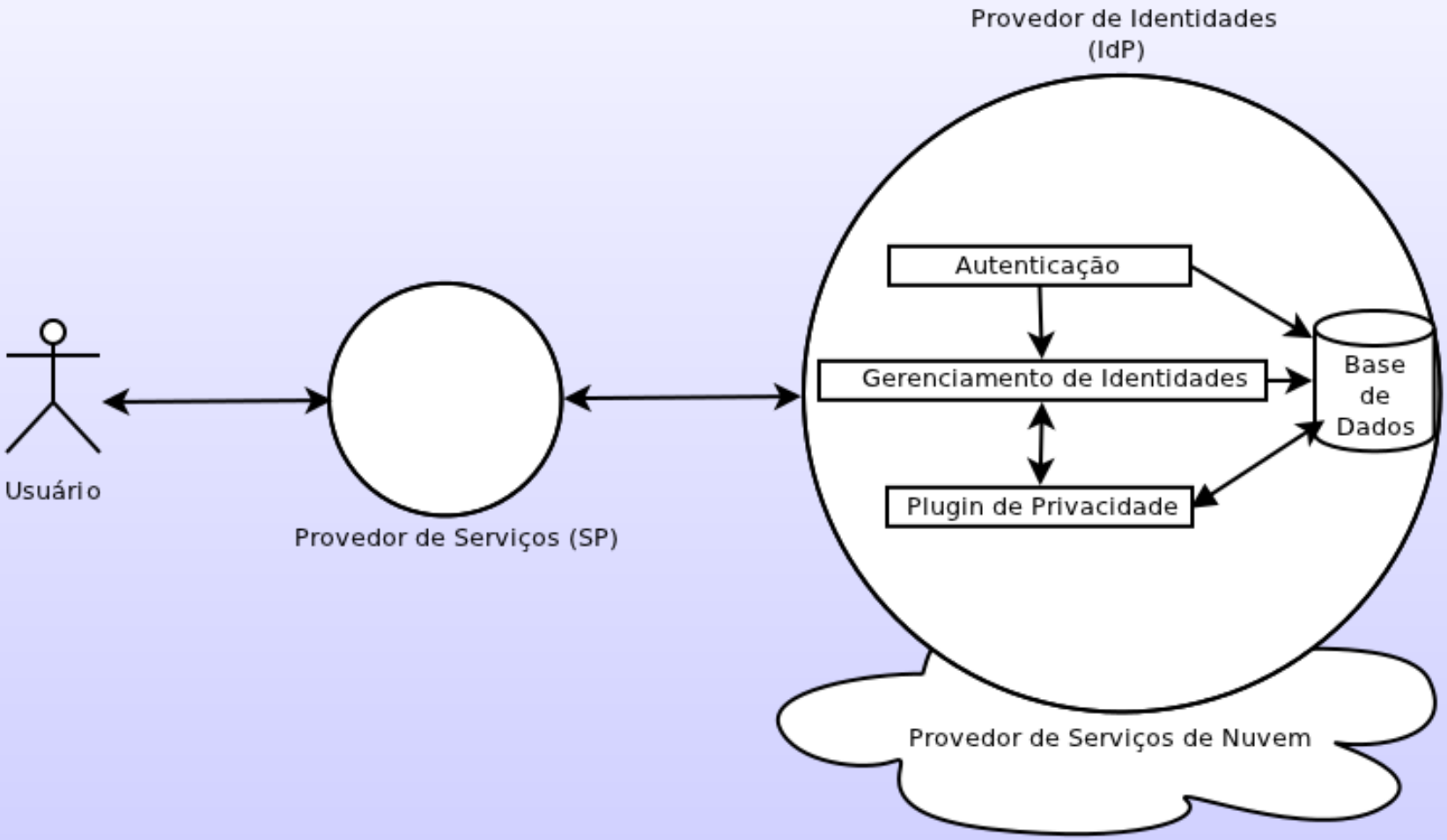
Modelos de serviço

- **IaaS** - Infrastructure as a Service.
- **PaaS** - Platform as a Service.
- **SaaS** - Software as a Service.



Agenda

Proposta


Provedor de Identidades
(IdP)
Autenticação
Gerenciamento de Identidades
Plugin de Privacidade
Base
de
Dados
Usuário
Provedor de Serviços (SP)
Provedor de Serviços de Nuvem

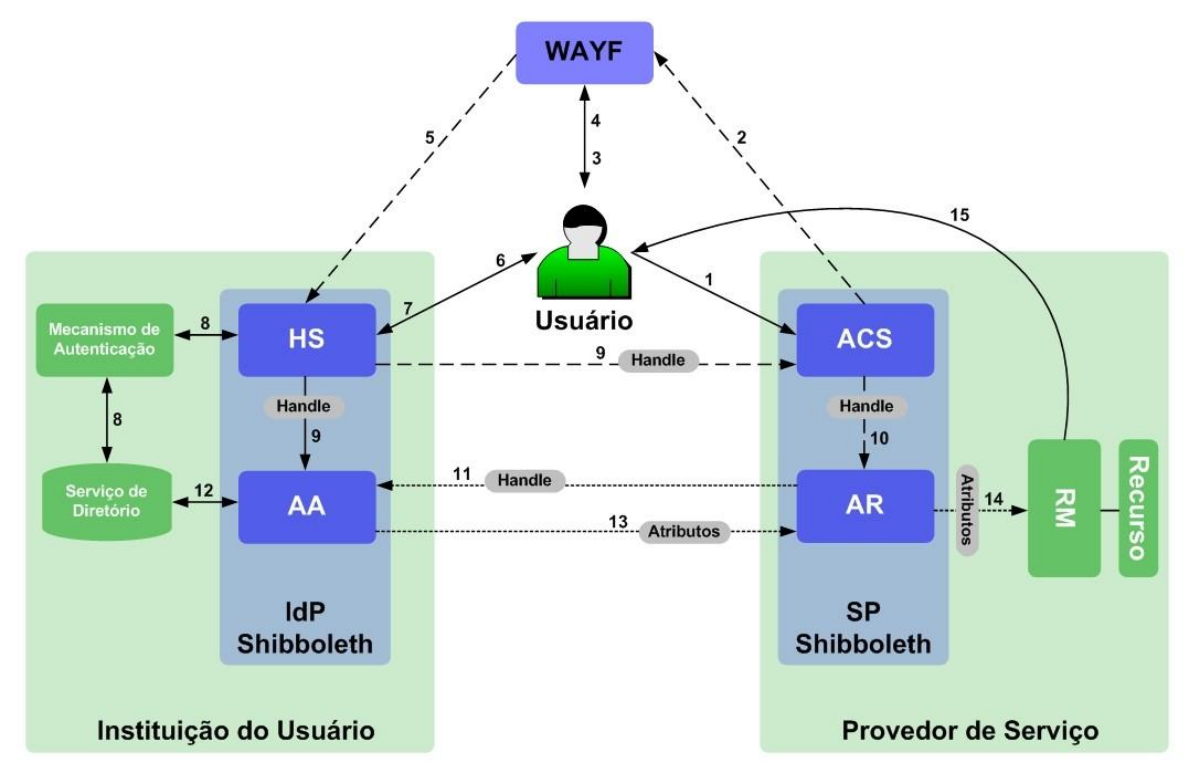
Principais ferramentas utilizadas

Amazon EC2 Provedor de serviços de nuvem (IaaS);

Shibboleth Sistema de gerenciamento de identidades;

uApprove *Plugin* de privacidade.

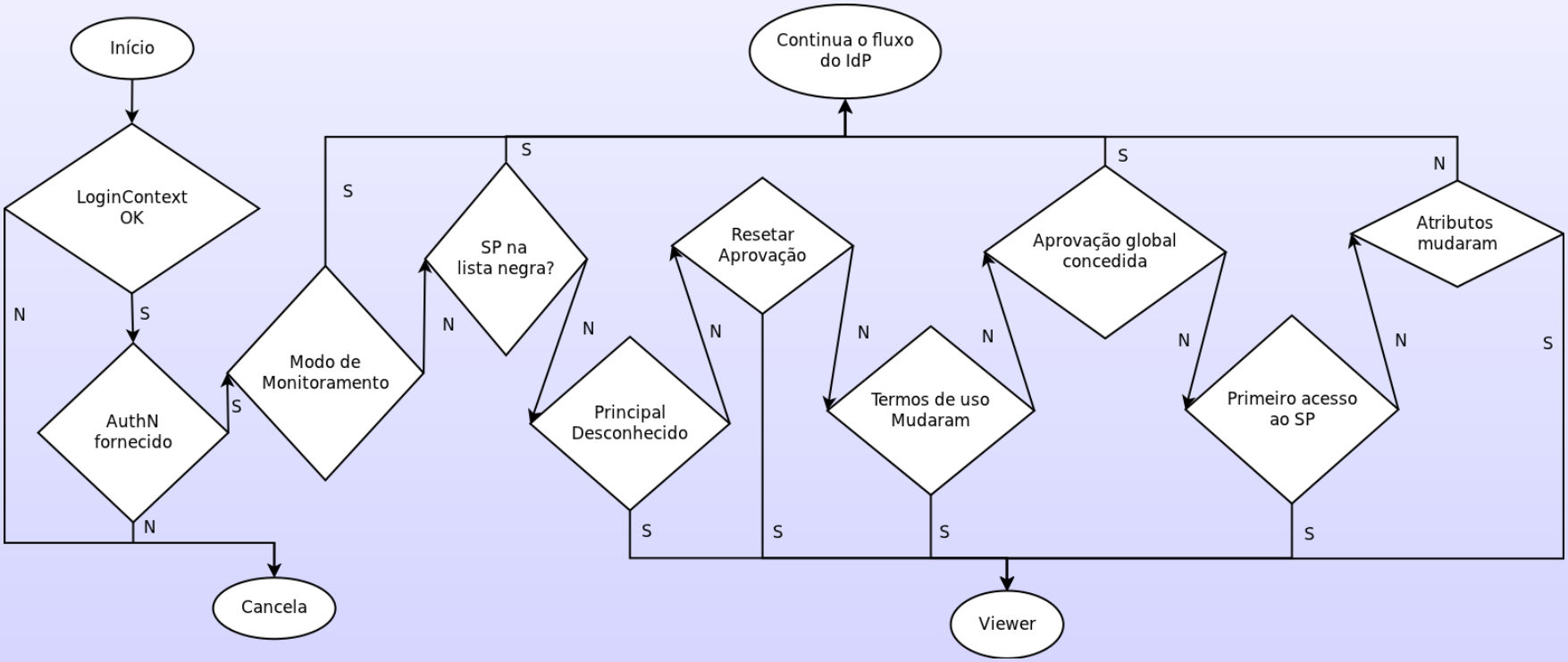
Shibboleth


WAYF
Usuário
HS
ACS
Mecanismo de Autenticação
Serviço de Diretório
AA
AR
Handle
Atributos
RM
Recurso
IdP Shibboleth
SP Shibboleth
Instituição do Usuário
Provedor de Serviço

uApprove

- *Plugin* de privacidade para o Shibboleth desenvolvido pela rede de universidades suíças SWITCH.
- Objetivo de garantir que o usuário saiba quais dados seus são liberados e para quem são liberados, além disso o usuário deve concordar com os termos de uso do provedor de serviços.
- Dividido em três componentes principais: *IdP plugin*, *Viewer* e *Reset approvals*.

uApprove


Início
LoginContext OK
AuthN fornecido
Cancela
Modo de Monitoramento
SP na lista negra?
Principal Desconhecido
Resetar Aprovação
Termos de uso Mudaram
Aprovação global concedida
Primeiro acesso ao SP
Atributos mudaram
Continua o fluxo do IdP
Viewer
S
N

Desenvolvimento - Infra-estrutura básica

- Instanciação da máquina virtual;
  - High-CPU;
  - Windows Server 2008;
  - Armazenamento EBS 30GB.
- Configuração de IP estático e regras de *firewall*;
  - IP: 50.19.108.64
  - Firewall: liberação das portas 80 (HTTP), 443 (HTTPS), 3389 (RDP), 8080 (Tomcat)
- Instalação do servidor web Apache e servidor de aplicações Tomcat;
- Configurações de SSL e proxy;

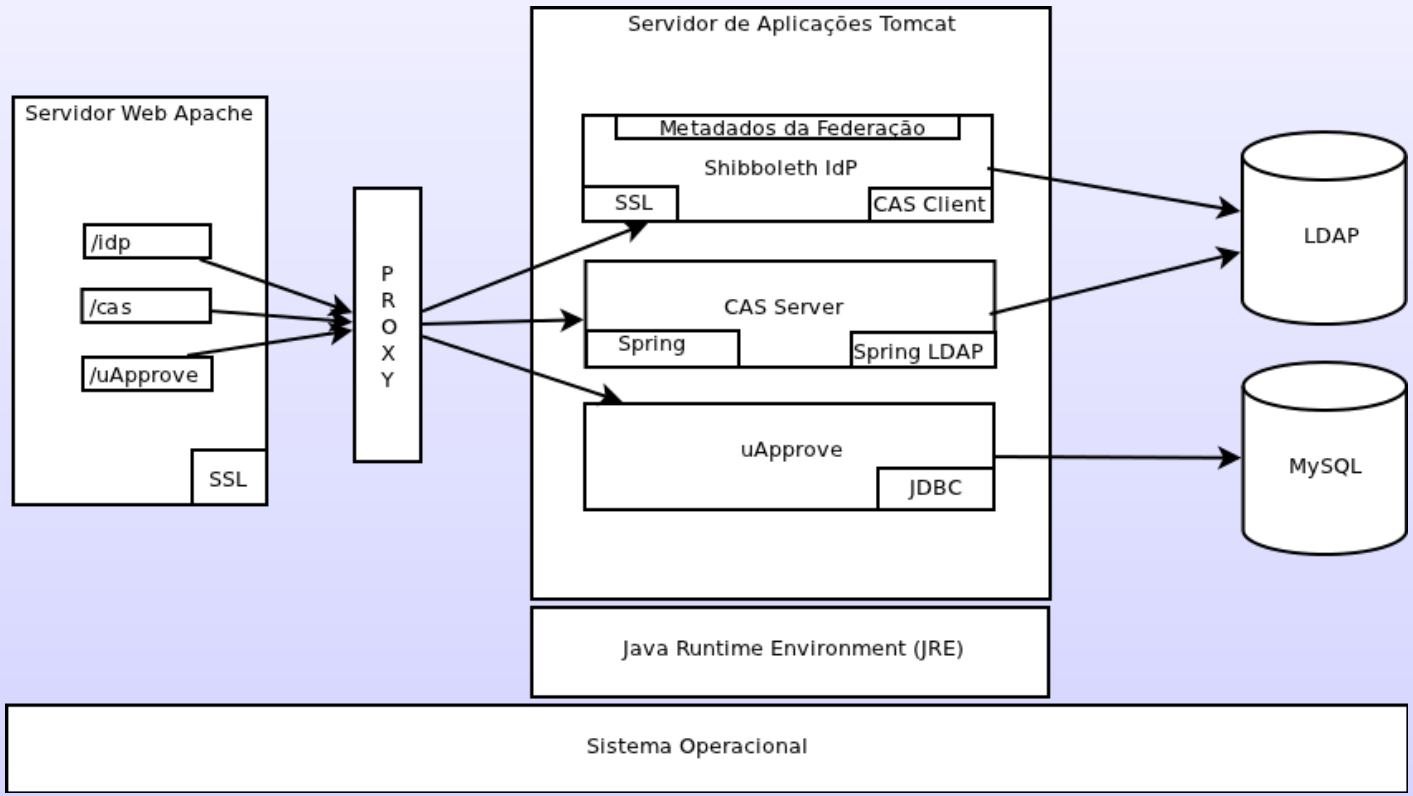
Desenvolvimento - Shibboleth

- Instalação do serviço de autenticação CAS;
  - Configuração de pesquisa dos usuários em diretório LDAP;
- Cadastro na federação TestShib;
- Instalação do Shibboleth;
  - Configuração de utilização da TestShib;
  - Configuração de autenticação através do CAS;
  - Configuração dos atributos;
  - Configuração da liberação de atributos;

Desenvolvimento - uApprove

- Instalação do MySQL;
  - Criação do banco de dados e das tabelas usadas pelo uApprove;
- Instalação do uApprove;
  - Criação dos termos de uso;
  - Configuração do filtro no Shibboleth;

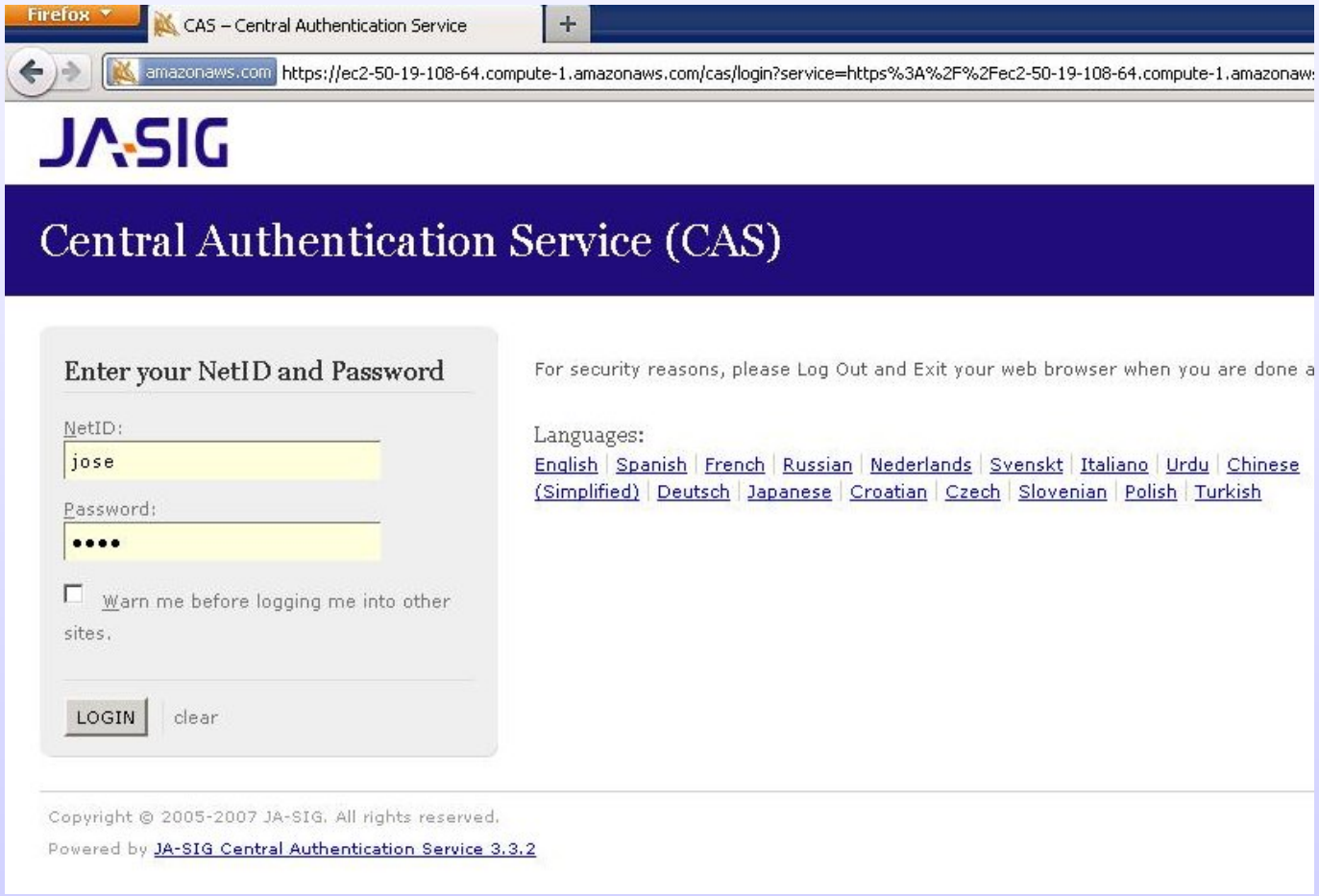
Desenvolvimento



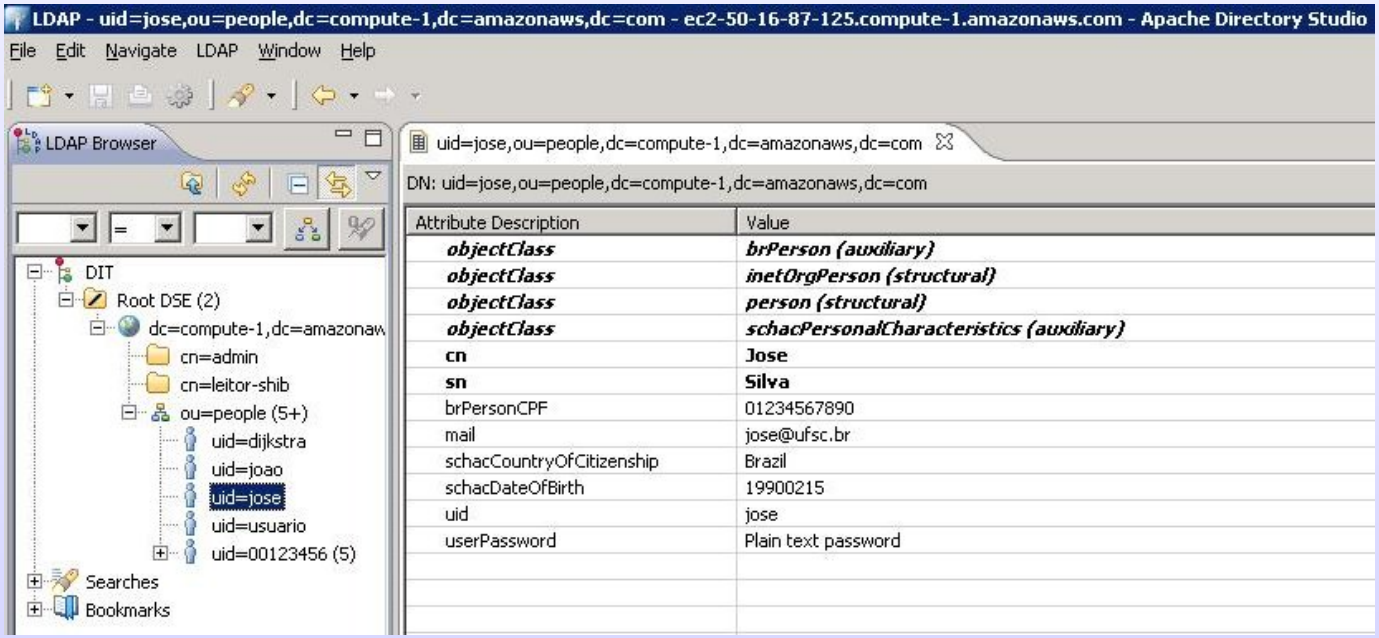
Resultados


TESTSHIB
Welcome to the TestShib Service Provider! Hopefully, you won't be here too long. Make sure you've already joined TestShib and configured your IdP. You can also test against other TestShib members later.
If you don't make it back successfully, first check the Shibboleth Wiki (1.3). If that doesn't solve it, send a detailed description of the error, your configuration, and log information to shibboleth-users@internet2.edu.
To start, you'll need to enter the entityID of your IdP in the box below. You'll be redirected to your IdP, where you'll use credentials such as myself/myself or others you've added to authenticate. Afterwards, you'll bounce back and see some results. If you enter your entityID incorrectly, you'll see a Session Creation Failure.
https://ec2-50-19-108-64.compute-1.amazonaws.com/idp/shibboleth
Go!
© Copyright 2006-2009 Internet2.

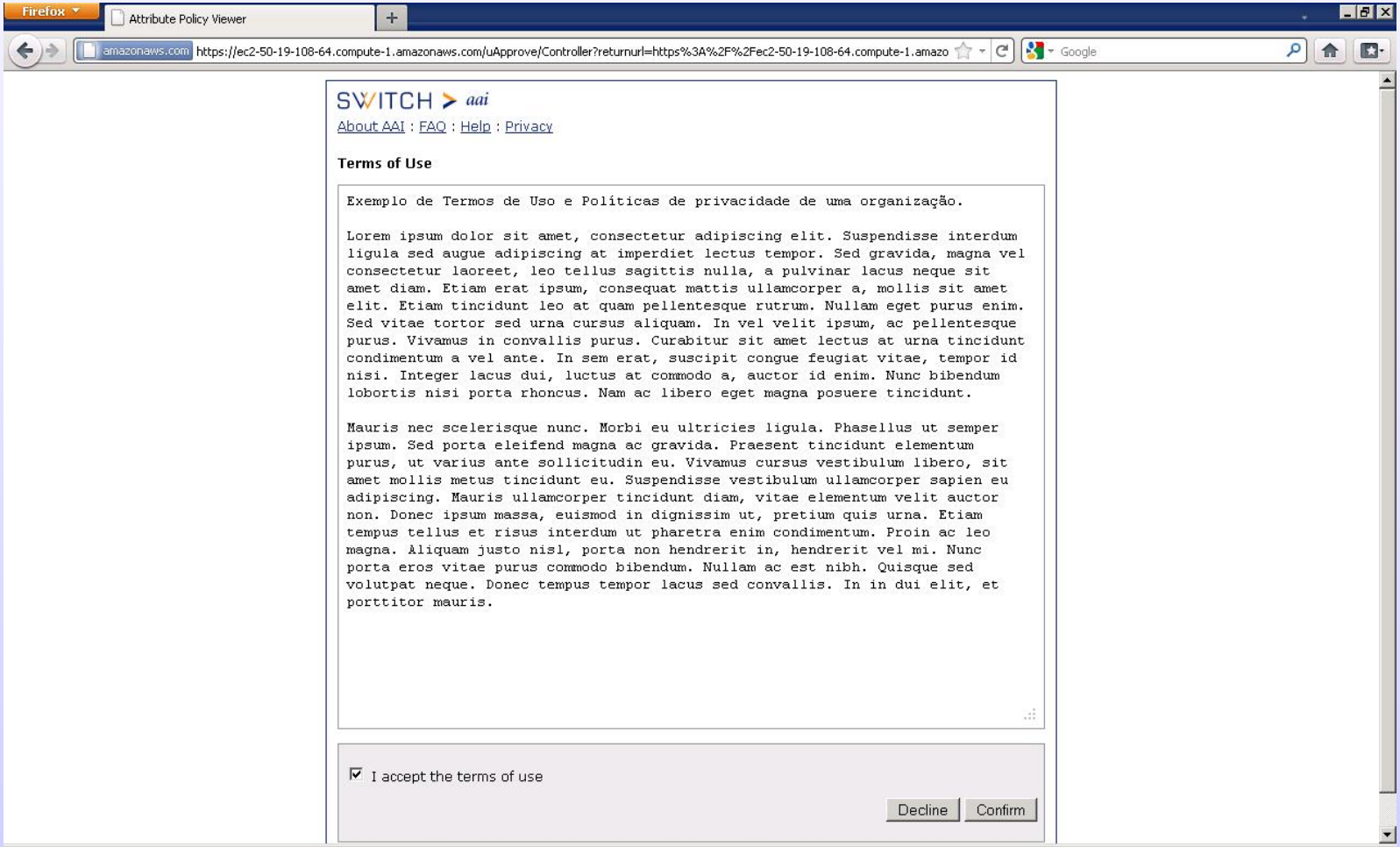
Resultados


Firefox
CAS – Central Authentication Service
amazonaws.com
https://ec2-50-19-108-64.compute-1.amazonaws.com/cas/login?service=https%3A%2F%2Fec2-50-19-108-64.compute-1.amazonaw
JA-SIG
Central Authentication Service (CAS)
Enter your NetID and Password
NetID:
jose
Password:
Warn me before logging me into other sites.
LOGIN
clear
For security reasons, please Log Out and Exit your web browser when you are done a
Languages:
English | Spanish | French | Russian | Nederlands | Svenskt | Italiano | Urdu | Chinese (Simplified) | Deutsch | Japanese | Croatian | Czech | Slovenian | Polish | Turkish
Copyright © 2005-2007 JA-SIG. All rights reserved.
Powered by JA-SIG Central Authentication Service 3.3.2

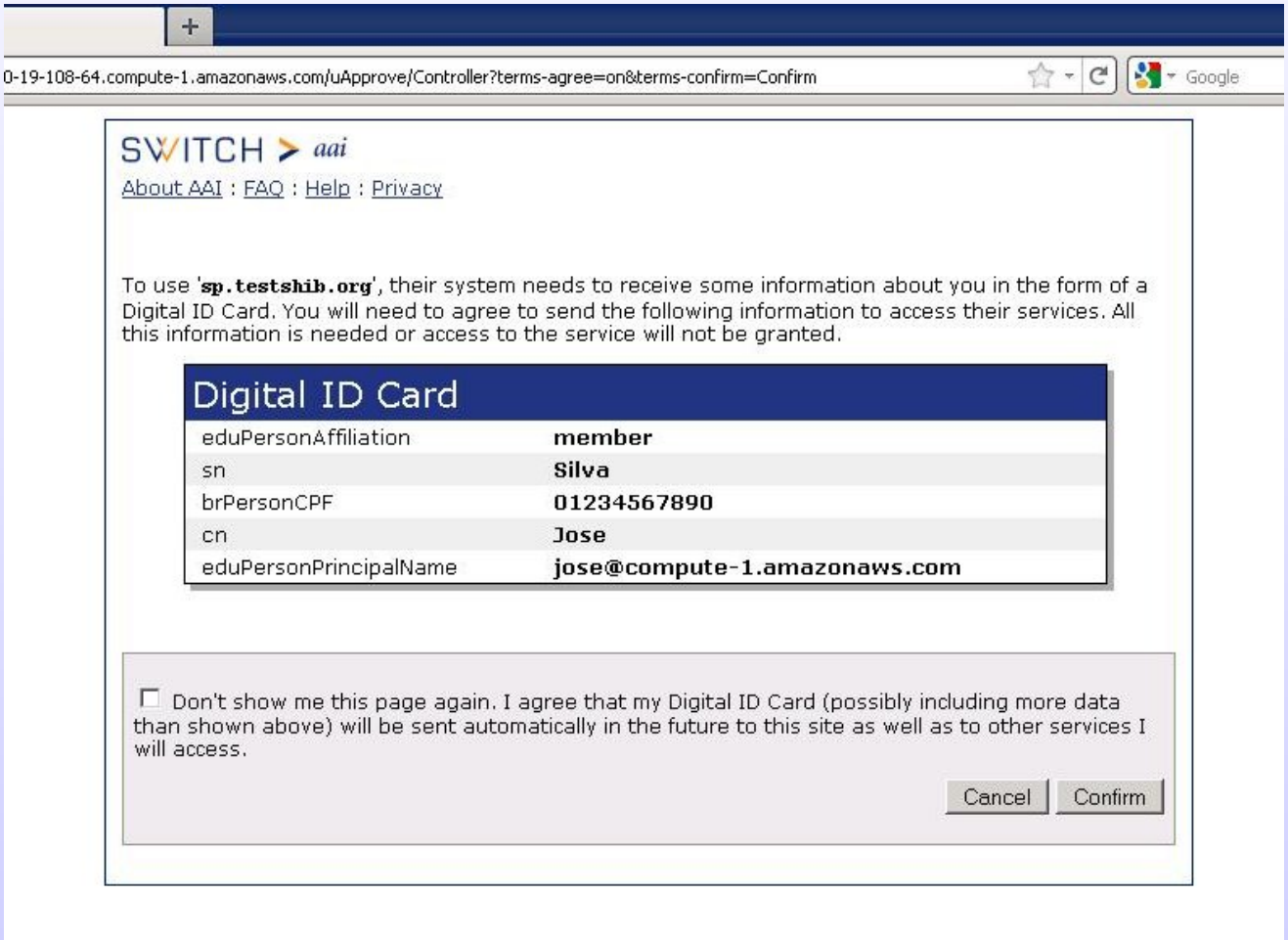
Resultados


LDAP - uid=jose,ou=people,dc=compute-1,dc=amazonaws,dc=com - ec2-50-16-87-125.compute-1.amazonaws.com - Apache Directory Studio
File Edit Navigate LDAP Window Help
LDAP Browser
DIT
Root DSE (2)
dc=compute-1,dc=amazonaw
cn=admin
cn=leitor-shib
ou=people (5+)
uid=dijkstra
uid=joao
uid=jose
uid=usuario
uid=00123456 (5)
Searches
Bookmarks
uid=jose,ou=people,dc=compute-1,dc=amazonaws,dc=com
DN: uid=jose,ou=people,dc=compute-1,dc=amazonaws,dc=com
Attribute Description
Value
objectClass
brPerson (auxiliary)
objectClass
inetOrgPerson (structural)
objectClass
person (structural)
objectClass
schacPersonalCharacteristics (auxiliary)
cn
Jose
sn
Silva
brPersonCPF
01234567890
mail
jose@ufsc.br
schacCountryOfCitizenship
Brazil
schacDateOfBirth
19900215
uid
jose
userPassword
Plain text password

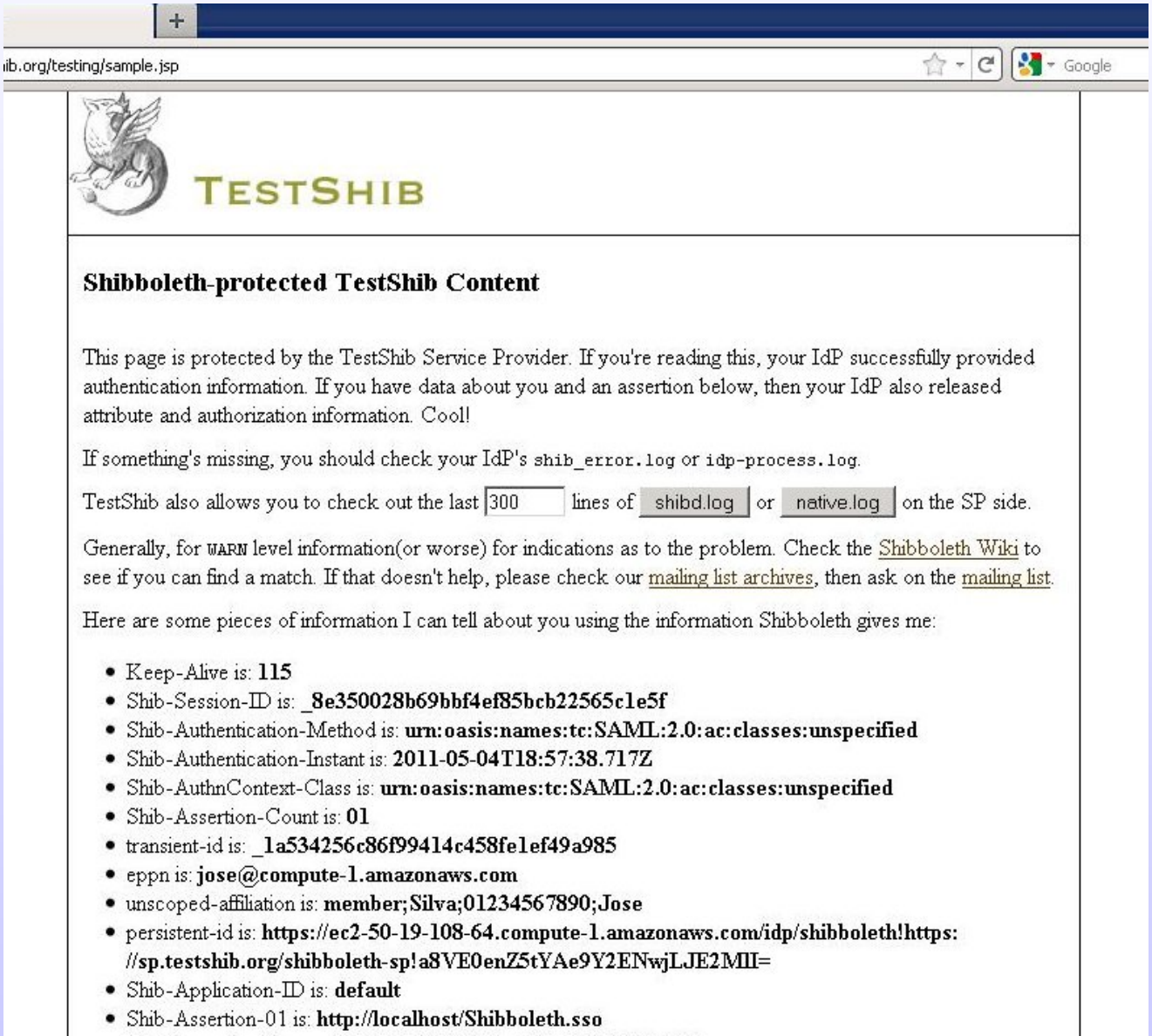
Resultados


Firefox
Attribute Policy Viewer
amazonaws.com
https://ec2-50-19-108-64.compute-1.amazonaws.com/uApprove/Controller?returnurl=https%3A%2F%2Fec2-50-19-108-64.compute-1.amazo
Google
SWITCH aai
About AAI : FAQ : Help : Privacy
Terms of Use
Exemplo de Termos de Uso e Políticas de privacidade de uma organização.
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse interdum ligula sed augue adipiscing at imperdiet lectus tempor. Sed gravida, magna vel consectetur laoreet, leo tellus sagittis nulla, a pulvinar lacus neque sit amet diam. Etiam erat ipsum, consequat mattis ullamcorper a, mollis sit amet elit. Etiam tincidunt leo at quam pellentesque rutrum. Nullam eget purus enim. Sed vitae tortor sed urna cursus aliquam. In vel velit ipsum, ac pellentesque purus. Vivamus in convallis purus. Curabitur sit amet lectus at urna tincidunt condimentum a vel ante. In sem erat, suscipit congue feugiat vitae, tempor id nisi. Integer lacus dui, luctus at commodo a, auctor id enim. Nunc bibendum lobortis nisi porta rhoncus. Nam ac libero eget magna posuere tincidunt.
Mauris nec scelerisque nunc. Morbi eu ultricies ligula. Phasellus ut semper ipsum. Sed porta eleifend magna ac gravida. Praesent tincidunt elementum purus, ut varius ante sollicitudin eu. Vivamus cursus vestibulum libero, sit amet mollis metus tincidunt eu. Suspendisse vestibulum ullamcorper sapien eu adipiscing. Mauris ullamcorper tincidunt diam, vitae elementum velit auctor non. Donec ipsum massa, euismod in dignissim ut, pretium quis urna. Etiam tempus tellus et risus interdum ut pharetra enim condimentum. Proin ac leo magna. Aliquam justo nisl, porta non hendrerit in, hendrerit vel mi. Nunc porta eros vitae purus commodo bibendum. Nullam ac est nibh. Quisque sed volutpat neque. Donec tempus tempor lacus sed convallis. In in dui elit, et porttitor mauris.
I accept the terms of use
Decline
Confirm

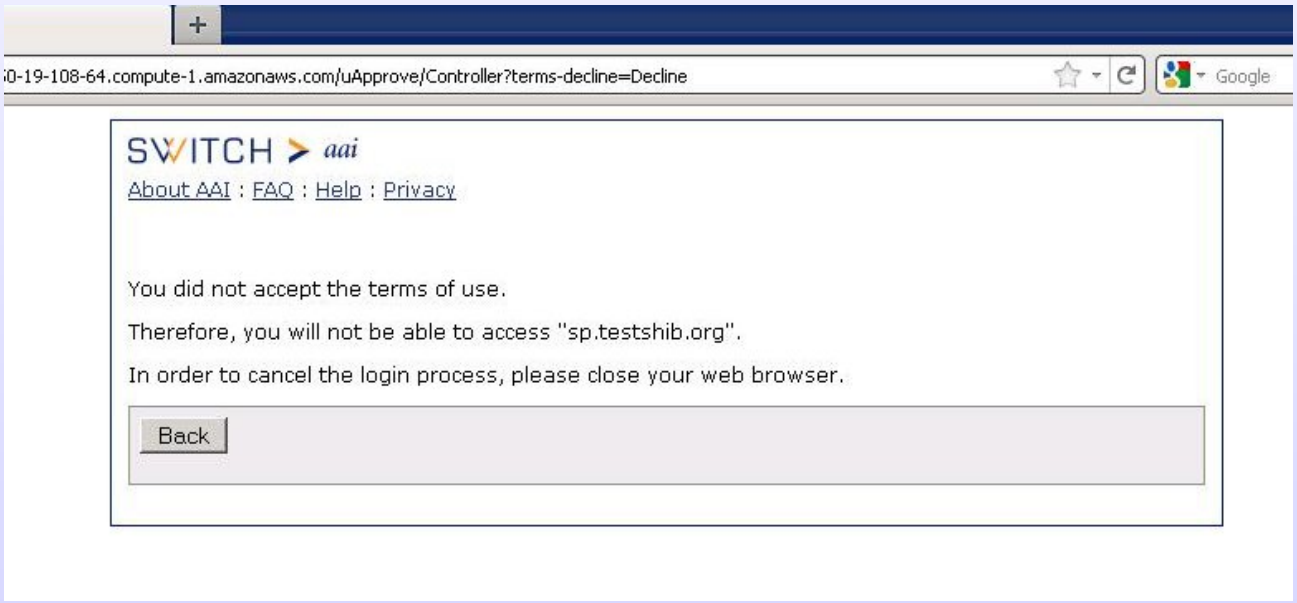
Resultados


0-19-108-64.compute-1.amazonaws.com/uApprove/Controller?terms-agree=on&terms-confirm=Confirm
Google
SWITCH aai
About AAI : FAQ : Help : Privacy
To use 'sp.testshib.org', their system needs to receive some information about you in the form of a Digital ID Card. You will need to agree to send the following information to access their services. All this information is needed or access to the service will not be granted.
Digital ID Card
eduPersonAffiliation member
sn Silva
brPersonCPF 01234567890
cn Jose
eduPersonPrincipalName jose@compute-1.amazonaws.com
Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future to this site as well as to other services I will access.
Cancel
Confirm

Resultados


ib.org/testing/sample.jsp
Google
TESTSHIB
Shibboleth-protected TestShib Content
This page is protected by the TestShib Service Provider. If you're reading this, your IdP successfully provided authentication information. If you have data about you and an assertion below, then your IdP also released attribute and authorization information. Cool!
If something's missing, you should check your IdP's shib_error.log or idp-process.log.
TestShib also allows you to check out the last 300 lines of shibd.log or native.log on the SP side.
Generally, for WARN level information(or worse) for indications as to the problem. Check the Shibboleth Wiki to see if you can find a match. If that doesn't help, please check our mailing list archives, then ask on the mailing list.
Here are some pieces of information I can tell about you using the information Shibboleth gives me:
Keep-Alive is: 115
Shib-Session-ID is: _8e350028b69bbf4ef85bcb22565c1e5f
Shib-Authentication-Method is: urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
Shib-Authentication-Instant is: 2011-05-04T18:57:38.717Z
Shib-AuthnContext-Class is: urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
Shib-Assertion-Count is: 01
transient-id is: _1a534256c86f99414c458fe1ef49a985
eppn is: jose@compute-1.amazonaws.com
unscoped-affiliation is: member;Silva;01234567890;Jose
persistent-id is: https://ec2-50-19-108-64.compute-1.amazonaws.com/idp/shibboleth!https://sp.testshib.org/shibboleth-sp!a8VE0enZ5tYAe9Y2ENwjLJE2MII=
Shib-Application-ID is: default
Shib-Assertion-01 is: http://localhost/Shibboleth.sso

Resultados


0-19-108-64.compute-1.amazonaws.com/uApprove/Controller?terms-decline=Decline
Google
SWITCH aai
About AAI : FAQ : Help : Privacy
You did not accept the terms of use.
Therefore, you will not be able to access "sp.testshib.org".
In order to cancel the login process, please close your web browser.
Back

Agenda

Conclusões

- Tratados dois problemas importantes: a falta de consciência dos usuários quanto à liberação de seus atributos para provedores de serviço e a falta de preocupação dos provedores de identidades quanto à apresentação de seus termos de uso.
- A proposta de solução, com o uso dos softwares Shibboleth e uApprove, mostrou que é possível resolver os dois problemas de maneira eficiente e sem comprometer a usabilidade da aplicação.
- A proposta se mostrou viável e pôde ser implantada em uma nuvem pública, com a possibilidade de utilização em federações consolidadas.

Trabalhos futuros

- Automatização da verificação de compatibilidade entre políticas de privacidade de provedores e de usuários pode ser considerado um trabalho futuro.

Obrigado

Obrigado!

Daniel Ricardo dos Santos

danielricardo.santos@gmail.com