The Eleventh International Conference on Networks - ICN 2012
February 29 - March 5, 2012 - Saint Gilles, Reunion Island

Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth

Marcos A. P. Leandro, Tiago J. Nascimento, Daniel R. dos Santos,
Carla M. Westphall, Carlos B. Westphall
Post Graduation Program in Computer Science
Federal University of Santa Catarina

Content at a Glance

- Introduction and Related Works
- Cloud Computing
- Identity Management
- Shibboleth
- Federated Multi-Tenancy Authorization System on Cloud
  - Scenario
  - Implementation of the Proposed Scenario
  - Analysis and Test Results within Scenario
- Conclusions and Future Works

Introduction

- Cloud computing systems: reduced upfront investment, expected performance, high availability, infinite scalability, fault-tolerance.
- IAM (Identity and Access Management) plays an important role in controlling and billing user access to the shared resources in the cloud.

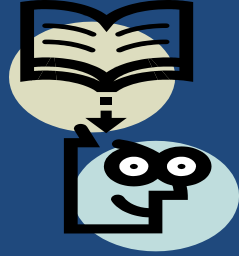
Introduction

- IAM systems need to be protected by federations.
- Some technologies implement federated identity, such as the SAML (Security Assertion Markup Language) and Shibboleth system.
- The aim of this paper is to propose a multi-tenancy authorization system using Shibboleth for cloud-based environments.

Related Work

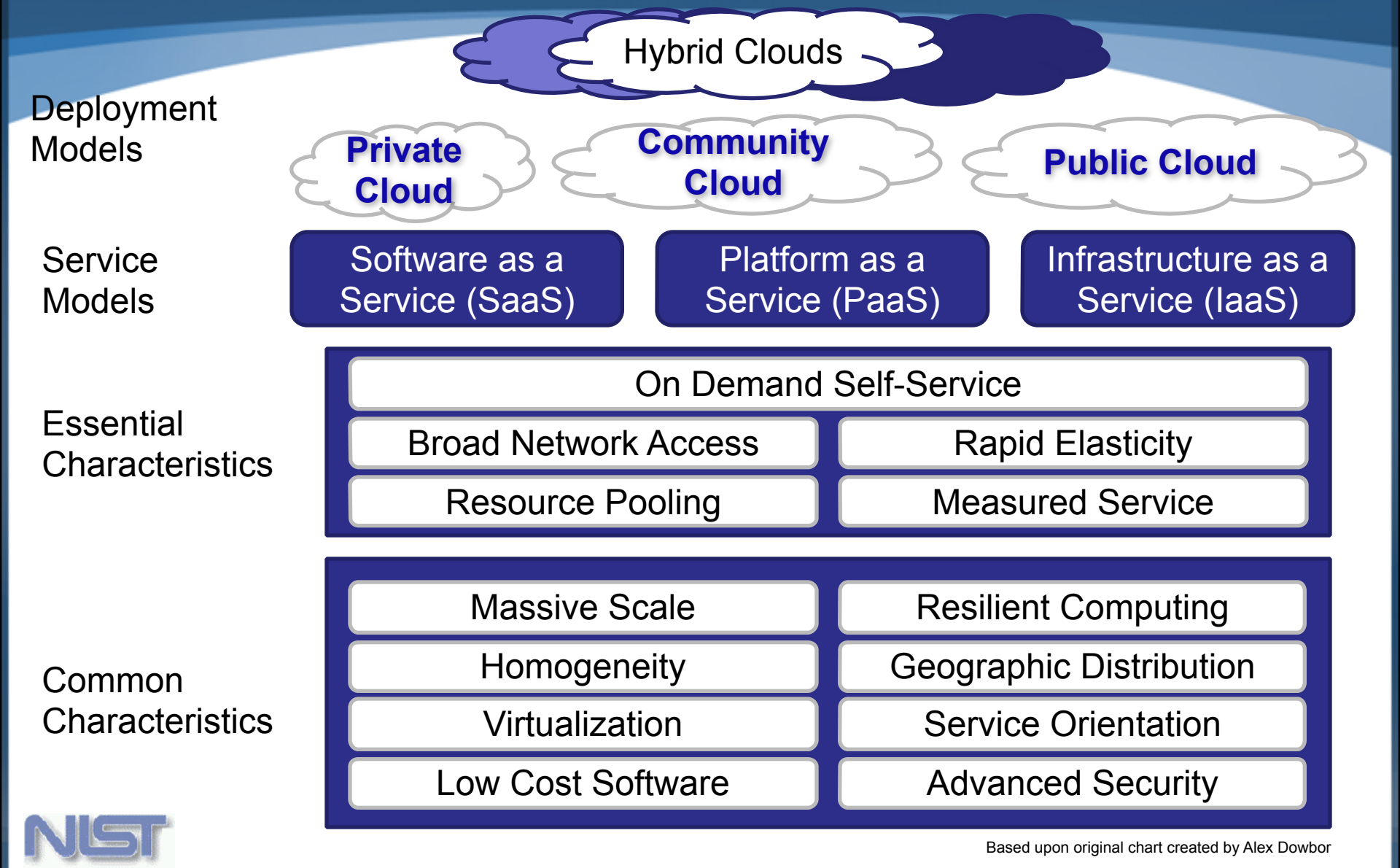
- R. Ranchal et al. 2010 - an approach for IDM is proposed, which is independent of Trusted Third Party (TTP) and has the ability to use identity data on untrusted hosts.
- P. Angin et al. 2010 - an entity-centric approach for IDM in the cloud is proposed. They proposed the cryptographic mechanisms used in R. Ranchal et al. without any kind of implementation or validation.

This Work



- Provide identity management and access control and aims to: (1) be an independent third party; (2) authenticate cloud services using the user's privacy policies, providing minimal information to the Service Proveder (SP); (3) ensure mutual protection of both clients and providers.
- This paper highlights the use of a specific tool, Shibboleth, which provides support to the tasks of authentication, authorization and identity federation.
- The main contribution of our work is the implementation in cloud and the scenario presented.

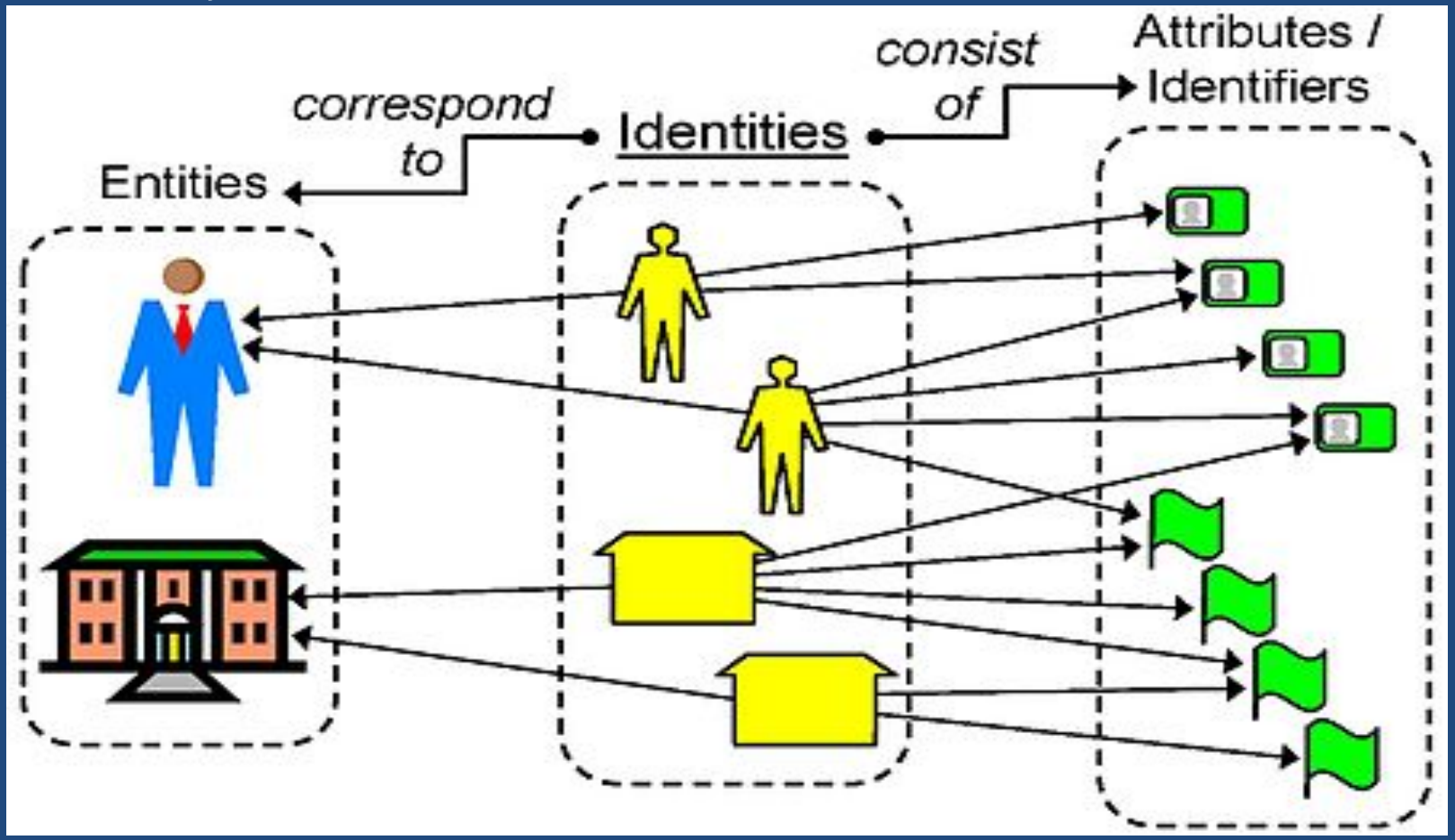
The NIST Cloud Definition Framework



Based upon original chart created by Alex Dowbor

Identity Management

- Digital identity is the representation of an entity in the form of attributes.



http://en.wikipedia.org/wiki/Identity_management

Identity Management

- Identity Management (IdM) is a set of functions and capabilities used to ensure identity information, thus assuring security.
- An identity management system (IMS) provides tools for managing individual identities.
- An IMS involves:
  - User
  - Identity Provider (IdP)
  - Service Provider (SP)

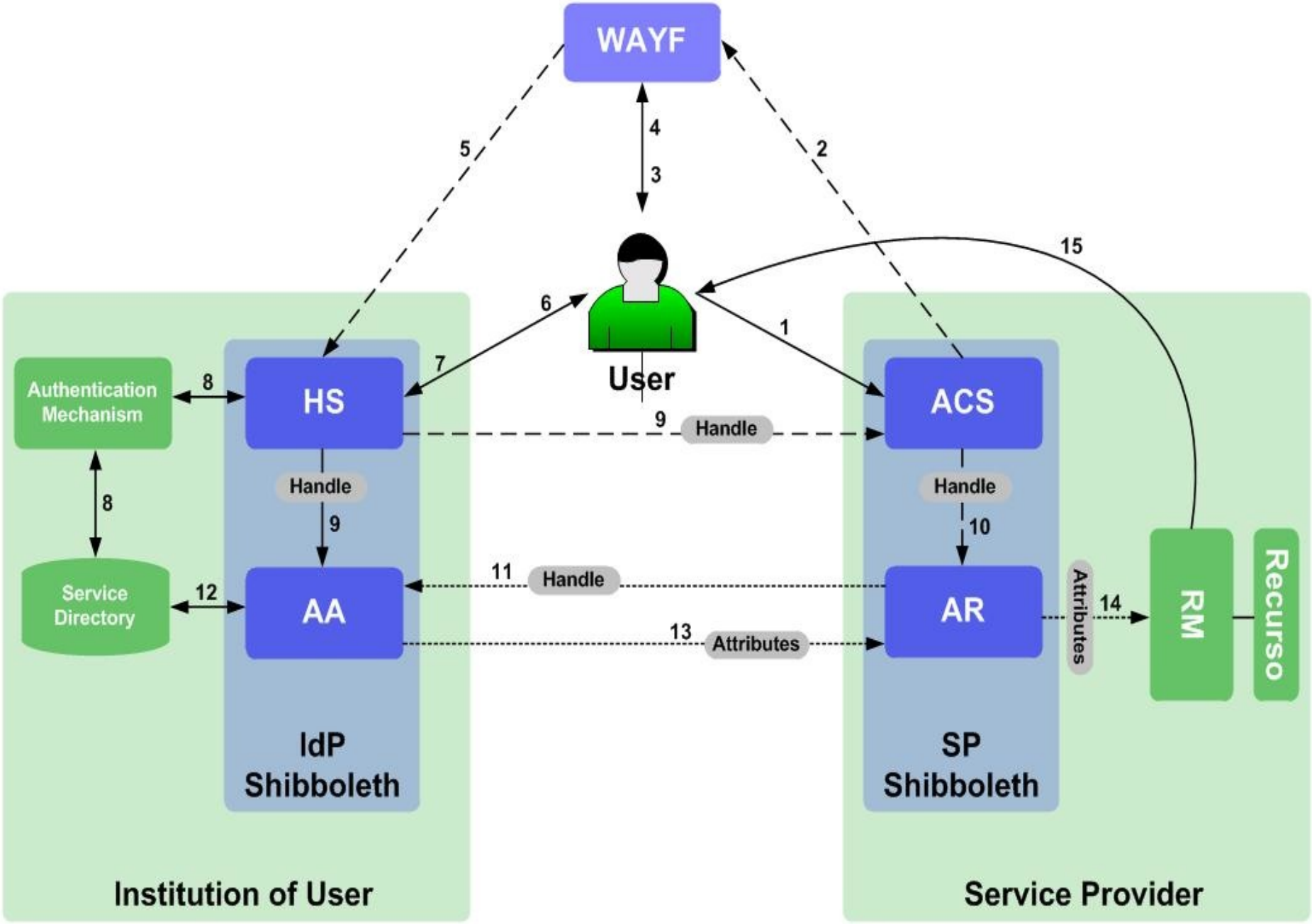
IMS

- *Provisioning:* addresses the provisioning and deprovisioning of several types of user accounts.
- *Authentication:* ensures that the individual is who he/she claims to be.
- *Authorization:* provide different access levels for different parts or operations within a computing system.
- *Federation:* it is a group of organizations or SPs that establish a circle of trust.

- The OASIS SAML standard defines precise syntax and rules for requesting, creating, communicating, and using SAML assertions.
- The Shibboleth is an authentication and authorization infrastructure based on SAML that uses the concept of federated identity. The Shibboleth system is divided into two entities: the IdP and SP.

Shibboleth

- The IdP is the element responsible for authenticating users: Handle Service (HS), Attribute Authority (AA), Directory Service, Authentication Mechanism.
- The SP Shibboleth is where the resources are stored: Assertion Consumer Service (ACS), Attribute Requester (AR), Resource Manager (RM).
- The WAYF ("Where Are You From", also called the Discovery Service) is responsible for allowing an association between a user and organization.

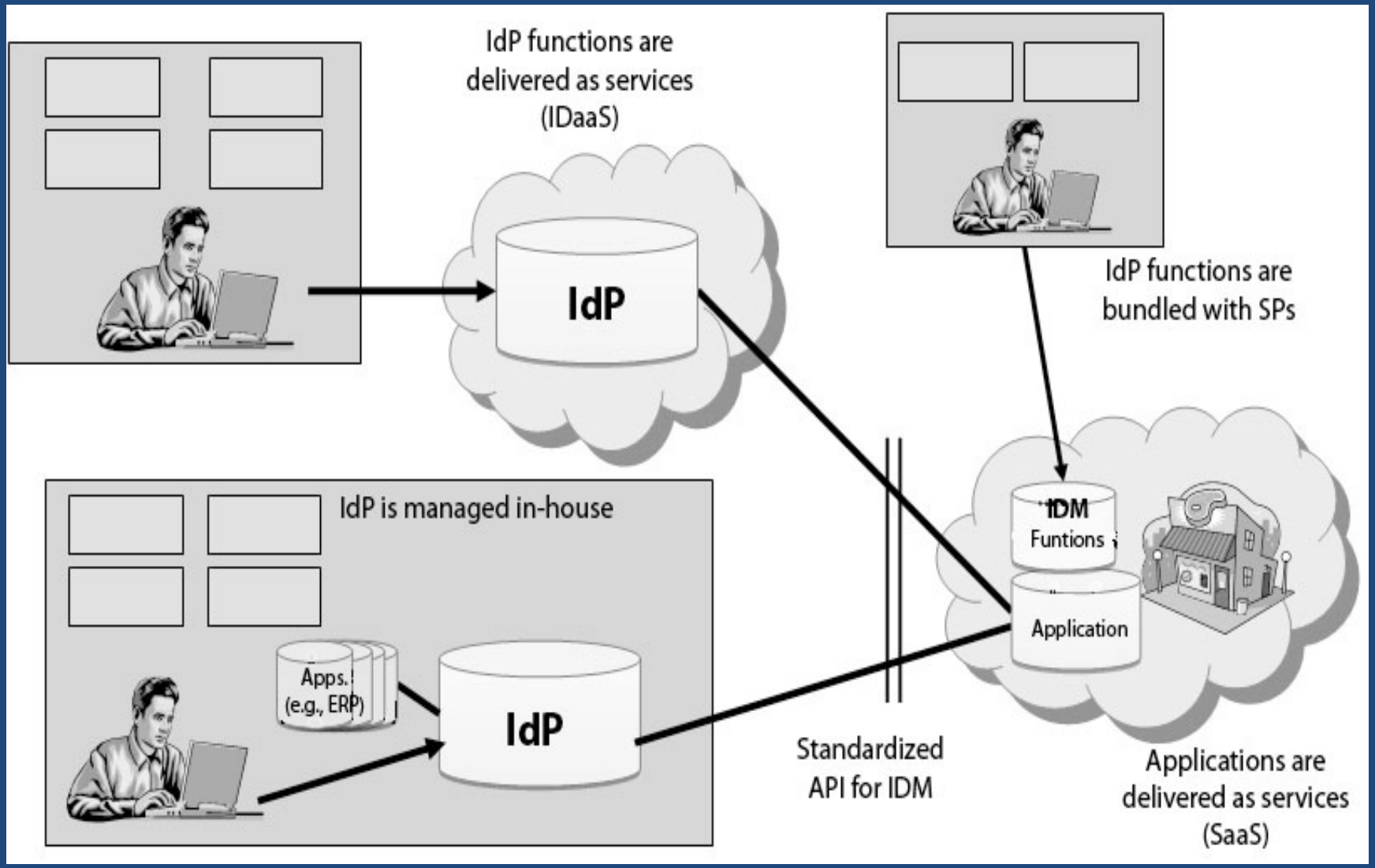

WAYF
5
4
3
2
15
6
1
User
Authentication Mechanism
8
HS
7
9
Handle
ACS
Handle
8
9
Handle
10
Service Directory
12
AA
11
Handle
AR
Attributes
14
RM
Recurso
13
Attributes
IdP Shibboleth
SP Shibboleth
Institution of User
Service Provider

In Step 1, the user navigates to the SP to access a protected resource. In Steps 2 and 3, Shibboleth redirects the user to the WAYF page, where he should inform his IdP. In Step 4, the user enters his IdP, and Step 5 redirects the user to the site, which is the component HS of the IdP. In Steps 6 and 7, the user enters his authentication data and in Step 8 the HS authenticate the user. The HS creates a handle to identify the user and sends it also to the AA. Step 9 sends that user authentication handle to AA and to ACS. The handle is checked by the ACS and transferred to the AR, and in Step 10 a session is established. In Step 11 the AR uses the handle to request user attributes to the IdP. Step 12 checks whether the IdP can release the attributes and in Step 13 the AA responds with the attribute values. In Step 14 the SP receives the attributes and passes them to the RM, which loads the resource in Step 15 to present to the user.

Federated Multi-Tenancy Authorization System on Cloud

- IdM can be implemented in several different types of configuration:
  - IdM can be implemented in-house;
  - IdM itself can be delivered as an outsourced service. This is called Identity as a Service (IDaaS);
  - Each cloud SP may independently implement a set of IdM functions.
- In this work, it was decided to use the first case configuration: in-house.

Configurations of IDM systems on cloud computing environments



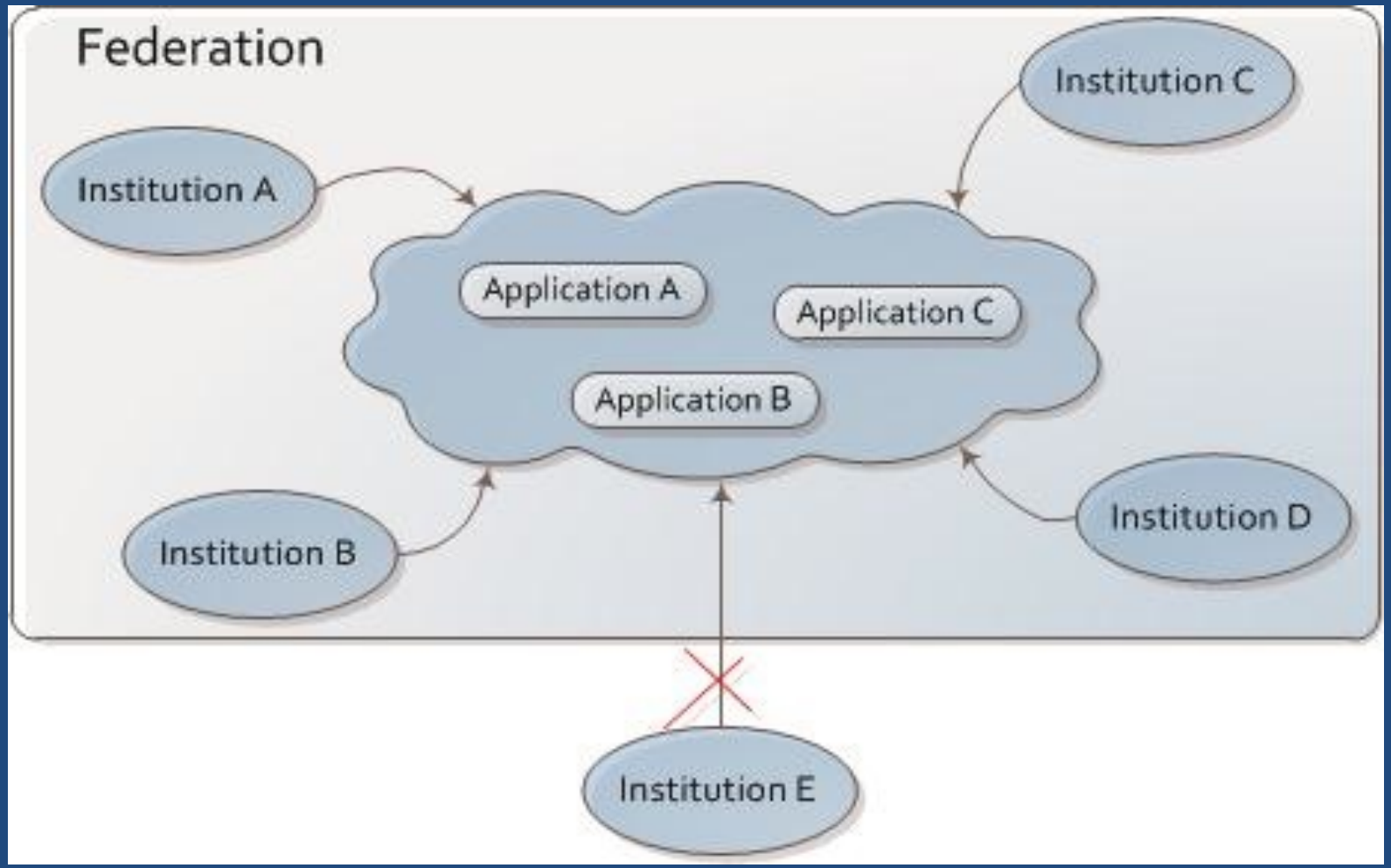
Federated Multi-Tenancy Authorization System on Cloud

- This work presents an authorization mechanism to be used by an academic institution to offer and use the services offered in the cloud.
- The part of the management system responsible for the authentication of identity will be located in the client organization.
- The communication with the SP in the cloud (Cloud Service Provider, CSP) will be made through identity federation.
- The access system performs authorization or access control in the environment.
- The institution has a responsibility to provide the user attributes for the deployed application SP in the cloud.
- The authorization system should be able to accept multiple clients, such as a multi-tenancy.

Scenario

- A service is provided by an academic institution in a CSP, and shared with other institutions. In order to share services is necessary that an institution is affiliated to the federation.
- For an institution to join the federation it must have configured an IdP that meets the requirements imposed by the federation.
- Once affiliated with the federation, the institution will be able to authenticate its own users, since authorization is the responsibility of the SP.

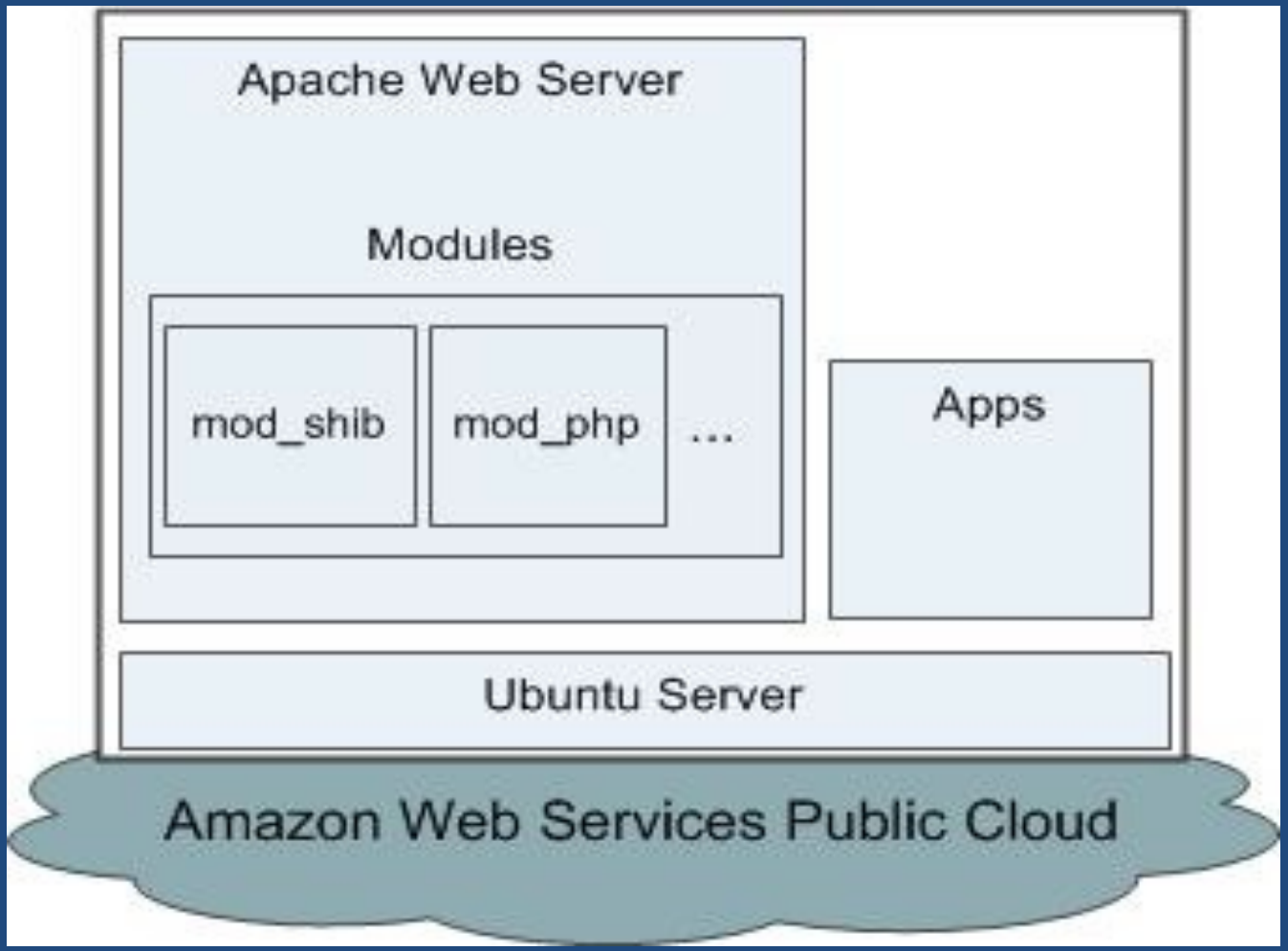
Scenario - Academic Federation sharing services in the cloud



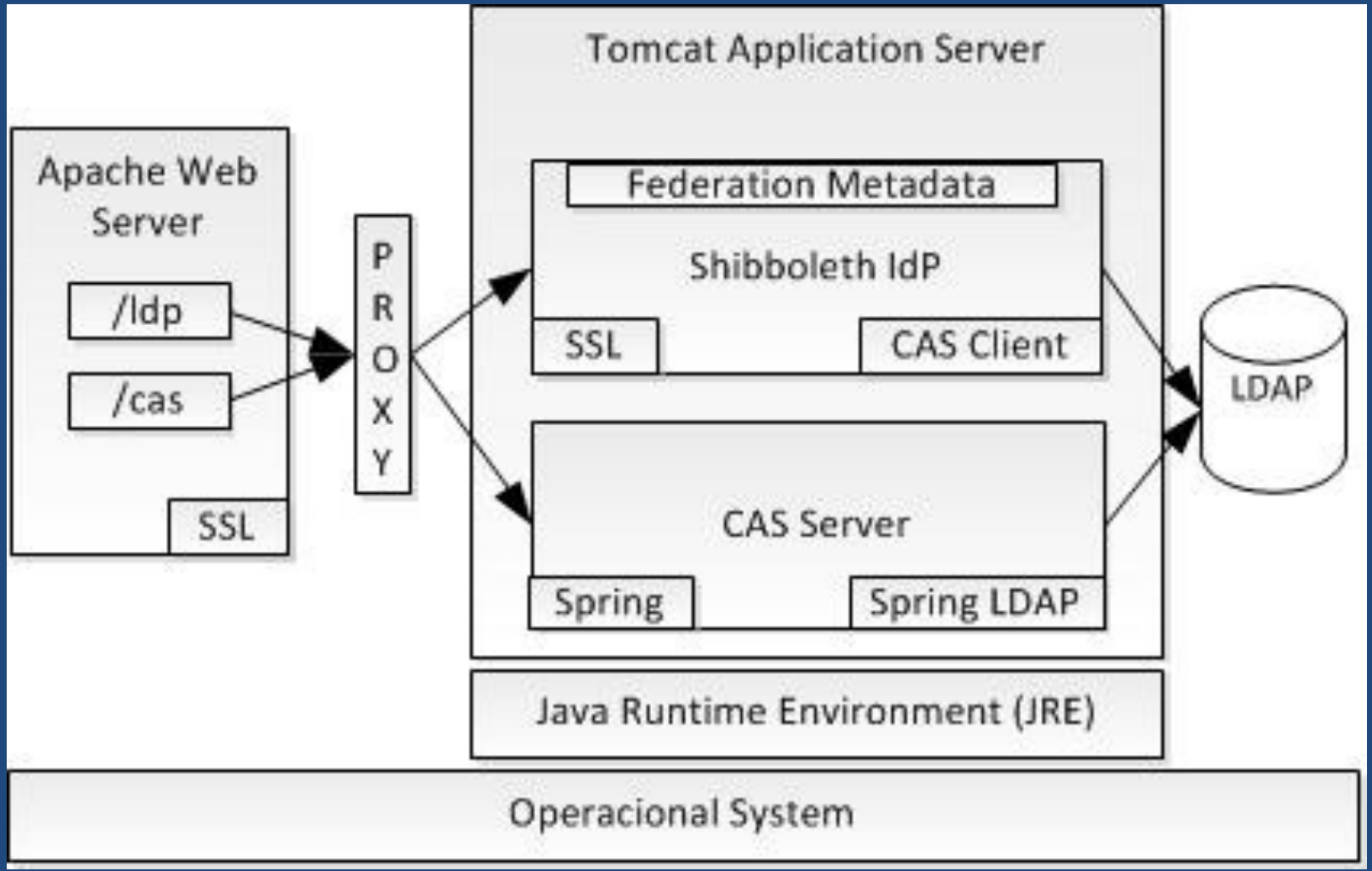
Implementation of the Proposed Scenario

- A SP was primarily implemented in the cloud:
  - an Apache server on a virtual machine hired by the Amazon Web Services cloud.
  - Installation of the Shibboleth SP.
  - Installation of DokuWiki, which is an application that allows the collaborative editing of documents.
  - The SP was configured with authorization via application, to differentiate between common users and administrators of Dokuwiki.

Implementation of the Proposed Scenario – Cloud Service Provider



Implementation of the Proposed Scenario – cloud IdP



Implementation of the Proposed Scenario

- The JASIG CAS Server was used to perform user authentication through login and password, and then passes the authenticated users to Shibboleth.
- The CAS has been configured to search for users in a Lightweight Directory Access Protocol (LDAP). To use this directory OpenLDAP was installed in another virtual machine, also running on Amazon's cloud.
- To demonstrate the use of SP for more than one client, another IdP was implemented, also in cloud, similar to the first. To support this task Shibboleth provides a WAYF component.

Analysis and Test Results within Scenario

- In this resulting structure, each IdP is represented in a private cloud, and the SP is in a public cloud.

The results highlighted two main use cases:

- *Read access to documents*
- *Access for editing documents*

Conclusions

- The use of federations in IdM plays a vital role.
- This work was aimed at an alternative solution to a IDaaS. IDaaS is controlled and maintained by a third party.
- The infrastructure obtained aims to: (1) be an independent third party, (2) authenticate cloud services using the user's privacy policies, providing minimal information to the SP, (3) ensure mutual protection of both clients and providers.

Conclusions

- This paper highlights the use of a specific tool, Shibboleth, which provides support to the tasks of authentication, authorization and identity federation.
- Shibboleth was very flexible and it is compatible with international standards.
- It was possible to offer a service allowing public access in the case of read-only access, while at the same time requiring credentials where the user must be logged in order to change documents.

Future Work

- We propose an alternative authorization method, where the user, once authenticated, carries the access policy, and the SP should be able to interpret these rules.
- The authorization process will no longer be performed at the application level.
- Expanding the scenario to represent new forms of communication
- Create new use cases for testing.
- Use pseudonyms in the CSP domain.

References

1. E. Bertino, and K. Takahashi, Identity Management - Concepts, Technologies, and Systems. ARTECH HOUSE, 2011.
2. "Security Guidance for Critical Areas of Focus in Cloud Computing," CSA. Online at: http://www.cloudsecurityalliance.org.
3. "Domain 12: Guidance for Identity and Access Management V2.1.," Cloud Security Alliance. - CSA. Online at: https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf.
4. D. W. Chadwick, Federated identity management. Foundations of Security Analysis and Design V, Springer-Verlag: Berlin, Heidelberg 2009 pp. 96–120, doi: 10.1007/978-3-642-03829-7_3.
5. A. Albeshri, and W. Caelli, "Mutual Protection in a Cloud Computing environment," Proc. 12th IEEE Intl. Conf. on High Performance Computing and Communications (HPCC 10), pp. 641-646, doi:10.1109/HPCC.2010.87.
6. R. Ranchal, B. Bhargava, A. Kim, M. Kang, L. B. Othmane, L. Lilien, and M. Linderman, "Protection of Identity Information in Cloud Computing without Trusted Third Party," Proc. 29th IEEE Intl. Symp. on Reliable Distributed Systems (SRDS 10), pp. 368–372, doi: 10.1109/SRDS.2010.57.
7. P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. B. Othmane, L. Lilien, and M. Linderman, "An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing," Proc. 29th IEEE Intl. Symp. on Reliable Distributed Systems (SRDS 10), pp. 177–183, doi: 10.1109/SRDS.2010.28.

Thank you!





Marcos A. P. Leandro, Tiago J. Nascimento,
Daniel R. dos Santos, Carla M. Westphall,
Carlos B. Westphall

{ marcosleandro, tiagojn, danielrs,
carlamw, westphal}@inf.ufsc.br