# Chapter 76
# Digital Identity Management in Cloud

**Vladimir Vujin**
*University of Belgrade, Serbia*

**Konstantin Simić**
*University of Belgrade, Serbia*

**Borko Kovačević**
*Microsoft, Serbia*

## ABSTRACT

*Existing approaches for management of digital identities within e-learning ecosystems imply defining different access parameters for each service or application. However, this can reduce system security and lead to insufficient usage of the services by end-users. This chapter investigates various approaches for identity management, particulary in a cloud computing environment. Several complex issues are discussed, such as cross-domain authentication, provisioning, multi-tenancy, delegation, and security. The main goal of the research is to provide a highly effective, scalable identity management for end-users in an educational private cloud. A federated identity concept was introduced as a solution that enables organizations to implement secure identity management and to share information on the identities of users in the cloud environment. As a proof of concept, the identity management system was implemented in the e-learning system of Faculty of Organizational Sciences, University of Belgrade.*

## INTRODUCTION

The growing complexity of modern educational ecosystems requires new approaches in access control (Dong, Zheng, Yang, Haifei, & Qiao, 2009). Cloud computing environments are multi domain environments in which each domain can use different security, privacy, and trust requirements and potentially employ various mechanisms, interfaces, and semantics. Such domains could represent individually enabled services or other infrastructural or application components (Takabi, Joshi, & Ahn, 2010). In order to provide seamless user experience, technologies such as: cloud-based services, social Web, and rapidly expanding mobile platforms will depend on identity management.

DOI: 10.4018/978-1-4666-6539-2.ch076

Development and exploitation of the applications in cloud computing environment, both private and public, requires defining and implementation of efficient strategy and tools for user's identities management. Identity Management (hereinafter: IDM) is key issue for cloud privacy and security. IDM in educational cloud is more complex than in traditional Web-based systems since the users hold multiple accounts with different educational services. The traditional model of application-centric access control, where each application keeps track of its collection of users and manages them, is not acceptable in educational cloud-based architectures.

This chapter describes existing open standards, such as: SAML2, OpenID, OAuth authentication and authorization, SCIM and XACML. These standards aim to solve problems related to maintaining interoperability and enabling easy identity management in cloud environment. Several complex questions, such as: cross-domain authentication, provisioning, multi-tenancy, delegation and security are discussed as well.

The main goal of the research is to provide a highly effective, scalable identity management for end-users in an educational private cloud. The research context of this chapter is focused on the e-learning processes in the private cloud within the Laboratory for e-business at Faculty of Organizational Sciences, University of Belgrade.

## THEORETICAL BACKGROUND

### Digital Identities

Issue of digital identities is presented since the beginning of the world wide using of the Internet. Problem has appeared because of the initial architecture of Internet. Namely, identity layer didn't exist and access to Web resources was not clearly defined. Therefore, each user has multiple different digital identities. Accordingly, managing these types of digital identities is fairly complex task.

In development of e-education system, problem of digital identity of users become significantly important. Concepts of anonymity and privacy are in confrontation with processes that require assessment, communication and access to services for learning, where exposure of information about identities is necessary. Digital identity can be observed from the different points of view. One perspective analyzes software solutions for digital identities management. Another one discusses organizations that implement these solutions. Third perspective is related to persons whose digital identities are managed.

Term digital identity refers to aspect of digital technology that deals with relations between human of identity and identity of other people and things. In the context of ICT, a digital identity is digital set of asserts a subject has about itself and other subjects. Identity is tightly coupled with terms of security and privacy. Information security is an area that deals with protecting integrity, privacy and confidentiality of information. Privacy refers to protection of attributes, affinities and characteristics of entities.

An identity is unique set of characteristics that uniquely identify a person or service. There are many different forms of personal identification in modern society. These forms of identification usually contain information that are unique, as well as information about authority that has issued the identification. Although, the term identity is well understood in physical world, defining digital identity is quite complex issue. An identity is set of data that describes attributes, characteristics and properties of a subject. Digital identity presents a set of information about particular entity. A subject or entity is person, group of people, organization, software tool or service that requires access to particular resource.

A digital identity is described through following elements: