Chapter IV
Identity Management

Kumbesan Sandrasegaran
University of Technology, Sydney, Australia

Mo Li
University of Technology, Sydney, Australia

ABSTRACT

The broad aim of identity management (IdM) is to manage the resources of an organization (such as files, records, data, and communication infrastructure and services) and to control and manage access to those resources in an efficient and accurate way. Consequently, identity management is both a technical and process-orientated concept. The concept of IdM has begun to be applied in identities-related applications in enterprises, governments, and Web services since 2002. As the integration of heterogeneous wireless networks becomes a key issue in towards the next generation (NG) networks, IdM will be crucial to the success of NG wireless networks. A number of issues, such as mobility management, multi-provider and securities require the corresponding solutions in terms of user authentication, access control, and so forth. IdM in NG wireless networks is about managing the digital identity of a user and ensuring that users have fast, reliable, and secure access to distributed resources and services of an next generation network (NGN) and the associated service providers, across multiple systems and business contexts.

INTRODUCTION

The broad aim of identity management (IdM) is to manage the resources of an organisation (such as files, records, data, and communication infrastructure and services) and to control and manage access to those resources in an efficient and accurate way (which in part usually involves a degree of automation). Consequently, IdM is both a technical and process-orientated concept.

The concept of IdM has begun to be applied in identities-related applications in enterprise, governments, and Web services since 2002. As the integration of heterogeneous wireless networks becomes a key issue in the fourth generation (4G) wireless networks, IdM will become crucial to the success of next generation (NG) wireless networks. A number of issues, such as mobility management, multi-provider, and securities require the corresponding solutions in terms of user authentication, access control, and so forth. Although IdM processes require the integration into existing business processes at several levels (Titterington, 2005), it remains an opportunity for NG wireless networks.

IdM in NG wireless networks is about managing the digital identity of a user and ensuring that users have fast, reliable, and secure access to distributed resources and services of NG wireless networks and associated service providers across multiple systems and business contexts.

Definition

Given the open and currently non-standardised nature of IdM, there are varying views as to the exact definition of IdM. These include:

By HP (Clercq & Rouault, 2004)
Identity Management can be defined as the set of processes, tools and social contracts surrounding the creation, maintenance, utilization and termination of a digital identity for people or, more generally, for systems and services to enable secure access to an expanding set of systems and applications.

By Reed (2002)
The essence of Identity Management as a solution is to provide a combination of processes and technologies to manage and secure access to the information and resources of an organisation while also protecting users' profiles.

By Cisco Systems (2005)
Businesses need to effectively and securely manage who and what can access the network, as well as when, where, and how that access can occur...lets enterprises secure network access and admission at any point in the network, and it isolates and controls infected or unpatched (sic) devices that attempt to access the network.

Objectives

As IdM can be used in different areas such as enterprise, government, Web services, telecommunication networks and so forth, its objectives diversity in different contexts. Generally, the IdM system is expected to satisfy the following objectives (Reed, 2002):

- It should define the identity of an entity (a person, place, or thing).
- It should store relevant information about entities, such as names and credentials, in a secure, flexible, customisable store.
- It should make the information accessible through a set of standard interfaces.
- It should provide a resilient, distributed, and high performance infrastructure for identity management.
- It should help to manage relationships between the enterprise and the resources and other entities in a defined context.

Main Aspects

Authentication

Authentication is the process by which an entity provides its identity to another party, for example, by showing photo ID to a bank teller or entering a password on a computer system. This process is broken down into several methods which may involve something the user knows (e.g., password), something the user has (e.g., card), or something the user is (e.g., fingerprint, iris, etc.). Authentication can take many forms, and may even utilise combinations of these methods.

Authorisation

Authorisation is the process of granting access to a service or information based on a user's role in an organisation. Once a user is authenticated, the system then must ensure that a particular user has access to a particular resource.

Access Control

Access control is used to determine what a user can or cannot do in a particular context (e.g., a user may have access to a particular resource/file, but only during a certain time of day, e.g., work hours, or only from a certain device, e.g., desktop in the office).