# Chapter 16
# Privacy in Identity and Access Management Systems

**Andreas Pashalidis**
*Katholieke Universiteit Leuven, Belgium*

**Chris J. Mitchell**
*Royal Holloway, University of London, UK*

## ABSTRACT

*This chapter surveys the approaches for addressing privacy in open identity and access management systems that have been taken by a number of current systems. The chapter begins by listing important privacy requirements and discusses how three systems that are being incrementally deployed in the Internet, namely SAML 2.0, CardSpace, and eID, address these requirements. Subsequently, the findings of recent European research projects in the area of privacy for I&AM systems are discussed. Finally, the approach taken to address the identified privacy requirements by ongoing projects is described at a high level. The overall goal of this chapter is to provide the reader with an overview of the diversity of privacy issues and techniques in the context of I&AM.*

## INTRODUCTION

Identity and Access Management (I&AM) systems support *access control*, namely ensuring that access to certain resources is granted only if the requestor is properly authorized. For example, a company employee that accesses a company VPN (Virtual Private Network) while working from abroad is likely to be granted access by an access control system. Although I&AM systems are closely integrated with access control systems, their main function is to support the system administrators and the end users in performing maintenance procedures, such as managing access credentials, user roles, access rights, rights delegation, auditing, and relationships between organizational units, throughout the lifetime of the system.

Over the last fifty years, many I&AM systems with a wide range of functions have been devel-

DOI: 10.4018/978-1-61350-498-7.ch016

oped. Such systems are typically composed of a number of modules, each with a specific task. Some I&AM systems are as simple as a database with authorized username/password pairs, while others are complex distributed systems that could include sophisticated policy decision points, interconnection with business process engines, accounting and billing infrastructures, credential negotiation agents, customer relationship management systems, administrative interfaces for the lifetime management of comprehensive user profiles, and provisions for auditing. Many I&AM systems are *closed*, i.e. they are designed for environments where there is a single system provider, such as a company or government organization, that has a very strong relationship with the prospective users.

The focus of this chapter is *open* I&AM systems, i.e. systems that cover multiple organizations. In the context of such systems, users interact with a range of different organizations using one or more credentials. New users may be introduced into the system by multiple parties, or users may be able to independently create new accounts for themselves. In open systems there is clearly a need for interoperability, and thus standardization is probably more important than in closed systems; privacy also plays a central role. Users should, for example, be able to control the degree of dissemination of their personal information to organizations and other users. The particular focus of this chapter is the various degrees of privacy achieved by current open I&AM systems, and what issues need to be addressed in future such systems.

## PRIVACY REQUIREMENTS FOR I&AM SYSTEMS

The need for user privacy in open I&AM system arises from the need to reduce the risks of unnecessary or otherwise unwanted disclosure of personal information. In recent years, legislation in Europe, both at EU and at national levels, has become an important driver for the introduction of privacy and transparency enhancing techniques within I&AM systems. This is because many of these laws require businesses to follow the principles of data minimization, data protection, and, in some cases, data retention. The data minimization principle requires that personal data is not disclosed to a transacting partner unless that information is strictly needed in order to carry out the transaction. In order to establish such strict necessity, the purpose of disclosure must be specified for each data item to be disclosed. Data protection and retention require that users have access to, and can update, their personal information when it is stored at an organization, but also that organizations have to keep records in a way that facilitates effective investigation of past transactions. In this context, 'personal data' is any data that could potentially lead to the identification of an individual, even if this is only possible in combination with additional information.

The following more concrete requirements arise from the requirement to minimize the personal data that is transferred between parties. We say that a privacy-preserving I&AM system should enable its users to:

- selectively disclose personal data to organizations and other users;
- create multiple identities or pseudonyms;
- attach different pieces of personal information to different identities;
- review data disclosed in the past;
- maintain different identities towards different organizations;
- formulate 'sticky' policies that follow personal data and that govern under which conditions the data may be disclosed and used;
- minimize the amount of trust users are required to place in third parties and infrastructural components in general; and