Chapter 26
Interoperability in Identity Management

Martin Wolf
University of Potsdam, Germany

ABSTRACT
Identity management systems are used by companies to ensure that only authorised people can access confidential information and internal applications. The interoperability of such systems is necessary due to the increasing need for companies to support interactions with partners, suppliers and customers on a technical level, which requires the exchange of identity information, rather than hiding it behind a firewall. Several initiatives have been formed to develop standard protocols for this purpose, with the goals of avoiding redundancy in user management, minimising security risks and facilitating collaboration set-up. These efforts have led to the evolution of several specifications, with each providing the means to exchange identity information in a homogenous environment with all collaboration partners using that standard.

This chapter investigates the requirements for enabling interoperability between systems independent of the standard they support. After providing an overview of current industry and research initiatives in this area, the chapter discusses the main challenges involved and presents a real world scenario from the financial industry as a motivating example. Based on an analysis of two major standards, several theoretical concepts are introduced, including a message meta model, to address the interoperability issue on an abstract level, thereby laying the foundation to support collaborations utilising multiple different standards as well as proprietary solutions. Finally, the chapter describes the implementation of a prototype supporting such a scenario based on the concepts presented in the chapter.

DOI: 10.4018/978-1-60960-485-1.ch026
INTRODUCTION

Identity information is required whenever a secured resource is to be accessed or used. Based on this information, authorisation decisions can be enforced. For example, when you want to enter a country, you need to provide a passport that proves your identity. The immigration officer can then use this information to make an informed decision about whether to let you into the country, thereby enforcing the country’s authorisation rules.

The same concept applies in a business environment. Companies need to protect their assets (such as confidential information and access to internal systems) to prevent financial loss and maintain their competitive advantage. Therefore, they use identity management systems and security mechanisms to ensure that only authorised people can access the resources. As a consequence, employees usually get several credentials, e.g. for an email account and for their workstation. The more systems they need to access, the more credentials they need to maintain, the more complex the set-up and elimination of their user accounts become (‘de-/provisioning’), and the higher the potential security risks are.

Many companies have therefore invested in Single Sign-On (SSO) solutions that centralise the user management and allow employees to access everything with just one set of credentials. The general idea of SSO is to create one holistic view of the user’s identity. Such a solution releases employees from remembering a multitude of credentials, facilitates the deprovisioning of user accounts and therefore increases the security of the overall system. However, despite these advantages, this approach has several limitations. First, centralising user management results in a single point of failure. In some cases, none of the connected systems are accessible when the SSO solution fails. Furthermore, a SSO solution is only possible if all connected systems are located in one administration domain, for example, under the control of one company.

With the increasing popularity of service-oriented architectures (SOA), this is no longer possible since interacting systems are generally no longer located within a single security domain. Companies externalise their systems into the ‘cloud’ or to a third party provider offering that particular functionality as a service. They cooperate with partners, suppliers and customers, which often requires them to share confidential information and access to internal systems.

If two companies intend to cooperate in a way that requires the exchange of confidential information or the interaction of their business processes, they could create user accounts in their domains for the employees or services that need to access internal systems or information. Unfortunately, this would result in redundant user management similar to getting an additional passport for every country you wish to enter. A second option is to agree on a secure mechanism to exchange identity information. This can be compared to a bilateral agreement between two countries to accept each other’s passports if exchanged in a certain way. However, with a large number of partners this gets rather tedious, error prone and complex, as a new mechanism must usually be introduced and maintained for each new partner.

Many companies were facing these problems and they realised that industry-wide standardisation of the exchange of identity information was necessary. Several initiatives were thus formed to specify standard security protocols and mechanisms. Their goal was to facilitate collaboration set-up, avoid redundancy in user management and minimise security risks. They achieved this by adopting the SOA concept and loosely coupling identity information from different security domains. This concept is known as identity federation.

To date, two major standards have emerged for Business-to-Business scenarios: The Web Services Specifications (WS-*) and the Security Assertion Markup Language (SAML). The WS-* specifications were initially developed by Microsoft and