As more and more activities and processes such as shopping, discussion, entertainment and business collaboration are conducted in the cyber world, digital identities, be them user names, passwords, digital certificates, or biometric features and digital identity management have become fundamental to underpinning accountability in business relationships, controlling the customization of the user experience, protecting privacy, and adhering to regulatory controls. In its broadest sense, identity management revolves around the enterprise process of adding or removing (provisioning) digital identity information and managing their authentication and associated access rights (policy) to information systems and applications (“access management”). Hence, digital identity management is strictly intertwined with identification technologies, such as biometrics, and authorization and access control technologies. Moreover, digital identity management requires us to consider at the same time aspects and technologies related to usability and management. Digital identity is not a static information too. It may evolve over time, and hence digital identity management requires us to consider and apply change management techniques to digital identity representations.

Digital Identity management is an emerging research field which addresses the aspects mentioned above. Moreover, the emergence of SOA and Web services-based enterprise information systems requires us to consider not only the technical aspects of distribution but also the impact of service autonomy on identity management solutions.

This chapter covers all relevant notions related with identity management and then discusses how digital identity management can be combined with negotiation techniques to provide a more flexible but still privacy-preserving solution.

The chapter first provides an overview of the main concepts related to digital identity management, focusing on recent federated approaches, namely Liberty-Alliance initiative [166], WS-Federation [170], the Shibboleth System [138], and Microsoft CardSpace. Issues related to identity management in the context of grid computing systems are discussed, in that these systems
represent a significant application context for SOA and digital identity management. The chapter also presents the trust negotiation paradigm, its main concepts and protocols, and possible applications of it in the context of federated identity management systems. Finally, to show the advantages of the digital identity management and trust negotiation approaches, the chapter presents a federated attribute management and trust negotiation solution, which provides a truly distributed approach to the management of user identities and user attributes with negotiation capabilities.

5.1 Overview of Digital Identity Management

Digital identity management is the set of processes, tools, social contracts, and a supporting infrastructure for creating, maintaining, utilizing, and terminating a digital identity. These tools allow administrators to manage large populations of users, applications, and systems securely and efficiently. They support selective assignment of roles and privileges that makes it easier to comply with regulatory controls and contribute to privacy-sensitive access controls. Identity management systems (IdM systems, from now on) have strong links with the management of security, trust, and privacy in a given system. Traditionally, identity management has been a core component of system security environments for the maintenance of account information to control log in access to systems or to a limited set of applications. Additionally, the identity of users has been the core of many authentication and authorization systems.

Recently, however, the scope of identity management has expanded, with its becoming a key enabler for electronic business. Identity management systems are now fundamental to underpinning accountability in business relationships, controlling the customization of the user experience, protecting privacy, and adhering to regulatory controls.

In this section we discuss the main concepts related to IdM systems. We begin with a brief overview of the notion of digital identity and identifiers, and then outline the most significant identity management frameworks.

Digital identity and identifiers

Digital identity can be defined as the digital representation of the information known about a specific individual or organization. Such information can be represented and conveyed in various ways, from log in names and passwords to digital credentials and biometric features.

IdM systems, according to the typical representation in SOA architectures, define identities by profiles of attributes associated with an individual. Identity attributes are typically stored at ad hoc Identity Providers (or IdPs, for short) which disclose identifiers as dictated by the authentication or authorization protocols in place.