Chapter 2
User-Centric Privacy Management in Future Network Infrastructure

Antonio F. Gomez-Skarmeta
University of Murcia, Spain

Alejandro Perez Mendez
University of Murcia, Spain

Elena Torroglosa Garcia
University of Murcia, Spain

Gabriel Lopez Millán
University of Murcia, Spain

ABSTRACT

Identity management is becoming more and more important every day. Users need a way to centralize the management of their identity information, such as simplifying the access to services with mechanisms like Single Sign-On. Organizations need a means of obtaining reliable information about users of their services. While this is the main concern for service providers, users are more worried about how their information is treated, what information is provided to what entity, and how privacy is assured in general. IdM provides the means for adequate privacy protection.

While several IdM (Identity Management) solutions that work at Web layer exist, they usually lack integration with network layer services. Future network infrastructures must integrate IdM functionality, in such a way that the user is provided with a unified and simplified vision of his identity, which results in an improved privacy and security protection. The IdM framework defined in the SWIFT (Secure Widespread Identities for Federated Telecommunications) project provides the means for cross-layer identity management as well as a set of advanced identity management concepts allowing improved privacy protection, simplification of user interactions, and extensible architecture.

Finally, it is analyzed how the inclusion of IdM in business organizations can provide economical benefits. These benefits range from a reduction in resource requirements to the increment of potential clients

DOI: 10.4018/978-1-61350-501-4.ch002

thanks to the incorporation of the organization in an identity federation. Special attention is placed on the case where the telecommunications operator is established as the main point of identity providing, as a straightforward result of its already established trust relationships with a wide range of parties (clients and service providers).

INTRODUCTION

The number of users that interact with digital services, as well as the number of services offered, has drastically increased in recent times. Different organizations have found in the Internet a good business opportunity due to the benefits it provides to the user (immediacy, 24/7 availability, access to other countries' companies…) and for the organization itself (easy deployment, low maintenance cost…).

Generally users have one account or profile for each one of the services they use. This presents several drawbacks that limit the usability of this approach. Users need to remember lots of different user names and passwords, especially if they want to preserve their privacy and to prevent their activities being traced. Users are also requested to fill out registration forms for each service they register for, so having to insert again and again their identity information. This may lead to inconsistencies and to out-of-date information.

Thus, for both users and services it is very important to deploy an identity management (IdM) system that allows the same identity information to be shared among the different services. Like this, users only need to remember a small number of credentials, while services will be provided with reliable and up-to-date information. Identity management should be applied in two different planes: horizontal (across domains and services) and vertical (across network layers).

Once identity information is shared among services, it is of paramount importance for the user to control the access to this information, determining by whom, when and how information about himself can be retrieved. So the user has a high control over how his privacy is being preserved. In addition, a user may want to access a service anonymously, just by providing a little information about himself (i.e. he is authenticated and is over 18 years old).

Network connectivity is a primary service that is required for access to this digital world. Therefore, network operators are usually the first place where users have to authenticate prior to accessing any other service. The integration of IdM into network operators is a step that can be done in order to anticipate the user requirements in terms of usability and privacy. Information should be accessed and provided by the network operator from and to other services and providers in a safe, controlled way, with special care with sensitive information (Attribute release policies - ARPs defined by the user in the different information providers will dictate how information is distributed, along with providers' local policies).

This chapter will present the analysis performed within the European research project *SWIFT*, which has its continuity in the *INS* standardization group of ETSI (European Telecommunications Standards Institute). It is divided into the following subsections. The chapter starts with a background where essential identity management terminology and concepts are introduced and some of the most relevant state-of-the-art technologies are briefly introduced. The chapter continues by describing identity management and privacy protection, and what mechanisms the former uses to achieve the latter. Then the chapter provides an overview of the main aspect of the SWIFT identity management framework, including identity aggregation, cross-layer identity management, distributed policies, integration with smart card technology and integration with legacy systems. The chapter goes on to discusses the advantages and business