Chapter 3

Identity Assurance in Open Networks

Ivonne Thomas
Hasso-Plattner-Institute, Germany

Christoph Meinel
Hasso-Plattner-Institute, Germany

ABSTRACT

Identity assurance is the degree of confidence another party, such as a service provider, can have in the belief that identity in the digital world actually matches with “real-life” identity. In open networks, establishing this confidence is not an easy task as participants are often located in different trust domains. Moreover, with the spread of open identity management systems, identity information is often held by designated identity provisioning services, so called identity providers. If another party shall be enabled to rely on received information, it ought to know how much confidence it can put into the assertions of the sender. In the intent to create a global standard, governments, commercial organizations, and academia alike have published common guidelines for identity assurance as part of so-called identity assurance frameworks. This chapter provides a state-of-the-art overview of identity assurance frameworks and describes them along important trust factors of identity providers. Furthermore, limitations of identity assurance frameworks are identified and highlighted as potential fields for further research. As an outlook to future developments, a small case study is presented that introduces trust levels for attributes in order to enable a service provider to distinguish between different qualities of trust, thus providing more flexibility in the way identity assurance is achieved in open networks.

INTRODUCTION

Today, many transactions in the online world require the sharing of identity information. Consider an online shop that requires our name, address and payment information to process an order. This sharing comes along with substantial trust demands for both, the party releasing identity information, such as the user, and the party that is receiving and using this identity information, such as the online shop. Users need to trust that their personal data is kept private and that it is not disclosed to unauthorized parties. Service
providers on the other side need to trust that the information received from a foreign source is accurate and does not pose a risk on the intended transaction.

In the traditional isolated or application-centric identity management model (cf. (Jøsang, Fabre, Hay, Dalziel, & Pope, 2005)), service providers gain this confidence by setting up reasonable technical, operational and legal safeguards that ensure that a user is who he claims to be and he can be held liable in case anything bad happens. However, when applied in the open environment of the web, this approach comes along with the creation of identity islands (Jøsang, Zomai, & Suriadi, 2007). Every service provider forms a separate “island” in which its users’ identity information is stored. For users, this usually results in a multitude of user accounts, each holding duplicate identity information and requiring authentication.

To overcome the limitations of the isolated approach, so called open identity management models (Jøsang & Pope, 2005) emerged in recent years to explicitly address the open nature of the Internet. Open identity management models add an additional entity to the process of sharing identity information. So called identity providers (IPs) take the role of managing digital identities of users for the purpose of provisioning this data to parties willing to rely on it. Identity provider services can be operated by an independent service organization or can be a functional unit that is part of a larger organization such as a commercial entity or university. Figure 1 illustrates the three parties that are usually involved in the exchange of identity information when applying open identity management models (Maler, Nadalin, Reed, Rundle, & Thibeau, 2010).

Identity providers are the entities holding identity data and relying parties are the entities using this data. The user is in the middle of all transactions and controls the flow of his private data ((Rieger, 2009), (Ahn, Ko, & Shehab, 2009)). The benefit of this approach is a reduced number of user accounts, as users register with an identity provider of their choice once and use the resulting account to log in to various service providers.

However, open identity management also adds a new dimension to the trust issue as the identity provider, as an additional party, needs to be trusted by both the user and the service provider. If a service provider has to rely on the information received from another trust domain such as the identity provider’s domain, it requires

![Figure 1. The traditional triangle of parties involved in an exchange of identity information](image-url)