Federated Identity Management

David W. Chadwick

Computing Laboratory, University of Kent, Canterbury, CT2 7NF, UK
d.w.chadwick@kent.ac.uk

Abstract. This paper addresses the topic of federated identity management. It discusses in detail the following topics: what is digital identity, what is identity management, what is federated identity management, Kim Cameron's 7 Laws of Identity, how can we protect the user's privacy in a federated environment, levels of assurance, some past and present federated identity management systems, and some current research in FIM.

Keywords: Identity Management, Shibboleth, CardSpace, Federations.

1 Introduction

What is digital identity? One can find many different variants of this definition on the Internet. Perhaps the most general definition is the one from a new draft ITU-T standard (X.1250) on global identity management [2], which states that identity is the "*Representation of an entity (or group of entities) in the form of one or more information elements which allow the entity(s) to be uniquely recognised within a context to the extent that is necessary (for the relevant applications).*" This definition is so general that it lacks precision of whose identity we are talking about (who or what is an entity?) and what data are we talking about (what is an information element?). Whilst an entity can be any object, in most cases it is personal identity that we are concerned about, so we will restrict this chapter to considering identity management of people rather than of any object. In this context, the information elements are restricted to Personal Indentifying (or Personally Identifiable) Information (PII), which is "*the information pertaining to any living person which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person).*" [1] We can consider that PII is simply the attributes[1] of a person, such as: their hair colour, sound of their voice, height, name, qualifications, past actions, reputation, medical records, etc. You might think that hair colour is not PII and is not a digital identity as it is too generic, but if we had a rule that stated that ginger haired people are granted a 10% discount at Ginger's hairdressing salon, then hair colour alone would be sufficient identity information to allow a person to be *uniquely recognised within a context to the extent that is necessary (for the relevant applications).* So even something as generic as hair colour can be classed as a digital

[1] An attribute is defined in [3] as "*information of a particular type*".

A. Aldini, G. Barthe, R. Gorrieri (Eds.): FOSAD 2007/2008/2009, LNCS 5705, pp. 96–120, 2009.

identity and as PII. To summarise, we can say that a person's (digital) identity comprises a set of attributes, and only a subset of these attributes are necessary to allow the person to be sufficiently recognised within a given context.

So what is identity management? In short it is the whole process of managing a user's identity attributes. Y.2720 [1] has a more comprehensive definition which states that identity management is: *A set of functions and capabilities (e.g. administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:*

- *Assurance of identity information (e.g., identifiers, credentials, attributes);*
- *assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects); and*
- *enabling business and security applications.*

Before proceeding further, we should clarify the difference between an *identifier* and an *Identity*, and an *attribute* and a *credential*. An identifier is usually a series of digits and/or characters that is used to uniquely identify an entity within one domain or system. No two entities (or users) within the same system can have the same identifier. So an identifier is a rather special type of identity attribute, since no two users can share the same identifier, whilst they may have other identity attributes in common, such as hair colour. Furthermore, an identifier is tightly bound to the system or domain in which it is defined; it usually cannot be meaningfully moved between domains, unlike the other identity attributes. Indeed, different domains can use the same identifier to identify different users. An identifier is only one of the identity attributes that comprise that person's digital identity within a system. Different computer systems know different subset's of a person's identity attributes, but each computer system will have its own identifier which uniquely identifies this individual within this system. An individual whose identity is distributed throughout many systems will therefore have multiple identifiers such as: their passport number, login ID, social security number, email address etc., which are each unique within their own domains. Some systems may store the identifiers from remote domains as well as their own. For privacy (and other) reasons, users are typically wary about releasing their identifiers to third parties, since these can uniquely identify them, whereas their other identity attributes, such as age, typically cannot.

An *attribute assertion* is a *claim* made by someone (the asserter) that a particular person possesses a particular attribute. Usually attributes have to be conferred on individuals (or asserted) by authoritative sources. Whilst people may be trusted in some situations to assert some of their identity attributes themselves, for example, their favourite drink, they certainly wont be trusted in all situations to assert all of their identity attributes themselves, for example, their qualifications or criminal record. Thus different authoritative sources are usually responsible for assigning different attributes to individuals. For example, the university that one graduated from is the authoritative source of one's degree attribute. These authoritative sources are also known as attribute authorities (AAs). An identity provider is an attribute authority combined with an authentication service to authenticate its users. An identity provider can authenticate a user and then issue an attribute assertion about the user. Attribute