Chapter 2
A Secure and Dynamic Mobile Identity Wallet Authorization Architecture Based on a XMPP Messaging Infrastructure

Alexandre B. Augusto
University of Porto, Portugal

Manuel E. Correia
University of Porto, Portugal

ABSTRACT

In this chapter, the authors propose and describe an identity management framework that allows users to asynchronously control and effectively share sensitive dynamic data, thus guaranteeing security and privacy in a simple and transparent way. Their approach is realised by a fully secure mobile identity digital wallet, running on mobile devices (Android devices), where users can exercise discretionary control over the access to sensitive dynamic attributes, disclosing their value only to pre-authenticated and authorised users for determined periods of time. For that, the authors rely on an adaptation of the OAuth protocol to authorise and secure the disclosure of personal-private user data by the usage of token exchange and new XML Schemas to establish secure authorisation and disclosure of a set of supported dynamic data types that are being maintained by the personal mobile digital wallet. The communication infrastructure is fully implemented over the XMPP instant messaging protocol and is completely compatible with the public XMPP large messaging infrastructures already deployed on the Internet for real time XML document interchange.

DOI: 10.4018/978-1-4666-2669-0.ch002

INTRODUCTION

The massive aggregation of personal identity attributes is currently one of the most important structural and strategic endeavors currently being carried out all over the Internet. Global Internet companies like *Microsoft, Google,* and *Facebook* are ever more competing over personal user data due to its high strategic commercial value on the market (Gollmann, 2010), making user digital identity a strategic asset that is going to help to redefine what kind of new innovative services are going to be developed and how they are going to be deployed all over the cloud in an interoperable way. This is well illustrated by the current fierce competition being fought by *Google* and *Facebook* about digital identity and their associated authentication, authorization, and data exchange protocols like OpenID (Recordon & Reed, 2006) and OAuth (Hammer-Lahav, 2010).

Currently, identity attributes are normally composed by static values held in the identity management system running in the cloud, which can be a bad idea according to Meiko Jensen (Jensen, Schwenk, Gruschka, & Iacono, 2009). What we intend to do with the work described in this chapter is to expand the universe of managed static identity attributes with dynamic identity attributes that by their very nature are more intimately associated with their owner and therefore can only reside, not in the cloud, but in mobile personal smart devices that follow their owner everywhere and can therefore keep those values up to date on real time. One good example of a dynamic attribute is the GPS coordinates (Lahlou, 2008) of a person that owns a mobile device with GPS.

What we are proposing is to expand the set of current static attributes being managed and held by Internet identity management systems (Tracy, 2008) with a new set of highly dynamic changing attributes. These new identity attributes can be instantiated in classical Identity management systems as symbolic link names that can act as pointers to their real location in the Internet allowing the Relying Party (RP) to locate the digital attribute storage wallets where those dynamic attributes are being maintained and protected.

In this highly dynamic identity infrastructure we are currently developing (Open Federated Environment for the Leveraging of Identity and Authorisation – OFELIA), every time a RP wants to consult the real time value of a certain dynamic attribute it has first to locate the attribute storage wallet where it resides and then ask its owner for permission to access its updated value for a certain period of time, the attribute owner then has the discretionary power to allow or deny that request and provide the RP an OAuth authorisation token, that the RP will present it as proof of previous authorization, every time RP wants to monitor the dynamic attribute during the previously authorised period of time. The attribute owner maintains revocation rights by being able to revoke access at any given moment, thus shifting the balance of power once again to the user, the legitimate owner of the values being monitored and used by cloud services. This is a necessary paradigm shift idea. Highly sensitive dynamic attributes like GPS positioning have high commercial value and therefore access to their updated values should be always put at their owner discretion.

This way privacy is greatly improved by the tools being developed by OFELIA and at the same time users are put into an improved position for bargaining for better services from giant Internet user profiling companies like *Google* and *Facebook* that are constantly taking advantages of users profiles.

It is important to realise that dynamic identity attributes constitute a whole new concept of digital identity because their values are constantly being updated due data owner interactions, the RP has to constantly be able to monitor it as requested. This is easily illustrated by the GPS location scenario, where users usually are in constant movement and their locations are constantly being changed, so only with a dynamic identity attributes the RP can obtain the real near current time position of an individual and not the last time the user or application remembered to update it.