Chapter 19
A Mobile-Based Attribute Aggregation Architecture for User-Centric Identity Management

Alexandre B. Augusto
University of Porto, Portugal

Manuel E. Correia
University of Porto, Portugal

ABSTRACT

The massive growth of the Internet and its services is currently being sustained by the mercantilization of users' identities and private data. Traditional services on the Web require the user to disclose many unnecessary sensitive identity attributes like bankcards, geographic position, or even personal health records in order to provide a service. In essence, the services are presented as free and constitute a means by which the user is mercantilized, often without realizing the real value of its data to the market. In this chapter the auhors describe OFELIA (Open Federated Environment for Leveraging of Identity and Authorization), a digital identity architecture designed from the ground up to be user centric. OFELIA is an identity/authorization versatile infrastructure that does not depend upon the massive aggregation of users' identity attributes to offer a highly versatile set of identity services but relies instead on having those attributes distributed among and protected by several otherwise unrelated Attribute Authorities. Only the end user, with his smartphone, knows how to aggregate these scattered Attribute Authorities' identity attributes back into some useful identifiable and authenticated entity identity that can then be used by Internet services in a secure and interoperable way.

1. INTRODUCTION

The explosive growth of the Internet is accelerating the migration of essential real world and monetary infrastructures to the virtual world, with digital identity playing a central catalyzing role for this societal transformative process. Arguably, the digital world is radically different from the real world, but

DOI: 10.4018/978-1-5225-0159-6.ch019

Copyright © 2016, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

there are some essential concepts that are readily transposed. Very much like in the physical world, in the Internet we have people interacting with other people and non-human computerised entities, under highly diverse situations. In the real world, people behave rather differently when they are at work, in the grocery store or at the gym, where they assume different roles in the face of different contextual situations. This essential social ability to contextually change the way we relate with others is what must be transposed from the physical world to the Internet every time we try to dematerialise societal real world processes to the virtual world.

A digital Identity can thus be readily defined has the "set of characteristics that uniquely describes a digital subject or entity and its relations with other entities or digital subjects in a virtual world." A digital subject, or entity, is therefore something, not necessarily human, that makes a request in order to access a particular resource (a Web page, an item from a database…) and is composed by a set of personal data attributes that in some sense characterizes that person or entity, usually referred to as a "user." The subset of personal data attributes needed for a specific role (or "user") depends on the situation and context at hand and is usually referred to as an identity persona (Baden, Bender, Spring, Bhattacharjee, & Starin, 2009). The association between an identity persona and a user is done by the means of an authentication process that can also be conducted by an Identity Management System (IdMS) (Hai-Binh & Bouzefrane, 2008).

Digital identity management systems, like their real world analogues, are essential in ensuring that a network infrastructure is capable to scale and meet the basic interoperable expectations and functionalities concerning security, privacy and reliability that emerge every time there is a need to plan and deploy a well engineered Internet service.

1.1. Digital Identity Management

Digital identity is maintained by identity Management Systems (IdMS). These are composed by governing organization policies, economic model, business processes and technologies that implement and manage the personal identity users attributes that are needed to establish and manage access rights to organizational digital assets (Chadwick, 2009). Moreover Identity management systems are also responsible for the digital identity lifecycle management within organizations, as they provide the flexible and scalable means by which it is possible to validate and exchange the digital personal data attributes that one needs in order to establish and promote interoperability among different systems, in accordance with some set of pre-established organizational security and legal policies. According to Kim Cameron, every useful IdMS should follow the seven "Laws of Identity" (Cameron, 2005) that can be observed on Table 1.

Identity management systems are employed by Identity Providers (IdP) (Clauß & Köhntopp, 2001) to manage digital identity within an organization, group of organizations or even the whole Internet. Depending on the scale, their interim structure and the social and/or financial benefits accrued by their deployment; IdPs can be further classified as:

- **Traditional (digital silo):** Where each service domain deploys its own IdP, thus forcing the user to create multiple independent accounts in order to access different services.
- **Centralized:** Bringing the concept of single sign-on (David, 2006), later extended with the usage of information cards (Cameron & Jones, 2007) in order to establish a way to dismiss the typical login/password scenario. In this model only one centralized IdP is needed to provides the neces-

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/a-mobile-based-attribute-aggregation-architecture-for-user-centric-identity-management/153411

Related Content

A Review of Internet Addiction on the Basis of Different Countries (2007–2017)
Ruya Samli (2018). *Psychological, Social, and Cultural Aspects of Internet Addiction (pp. 200-220).*
www.irma-international.org/chapter/a-review-of-internet-addiction-on-the-basis-of-different-countries-20072017/193104

Violence Against Healthcare Workers
Raleigh Blasdell, Michelle Kilburn, Laura Krieger-Sampleand Rhiannon Oakes (2023). *Research Anthology on Modern Violence and Its Impact on Society (pp. 1075-1108).*
www.irma-international.org/chapter/violence-against-healthcare-workers/311317

Scepticism and Seduction
Cesar Kiraly (2017). *Seduction in Popular Culture, Psychology, and Philosophy (pp. 259-296).*
www.irma-international.org/chapter/scepticism-and-seduction/162994

Cybersecurity and Business Continuity: An Essential Partnership in an Era of Digital Interactions
Nelson Russo (2023). *Internet of Behaviors Implementation in Organizational Contexts (pp. 68-99).*
www.irma-international.org/chapter/cybersecurity-and-business-continuity/333552

Educator Experiences as Victims of School Violence: Emerging Perspectives and Research
Kailyn Bare, Susan D. McMahon, Elena Gonzalez Molina, Cori Tergesenand Kayleigh E. Zinter (2022). *Research Anthology on Interventions in Student Behavior and Misconduct (pp. 755-779).*
www.irma-international.org/chapter/educator-experiences-as-victims-of-school-violence/308249