Digital Identity Management within Networked Information Systems
From Vertical Silos View into Horizontal User-Supremacy Processes Management

Ghazi Ben Ayed
Faculty of Business and Economics, University of Lausanne, Switzerland
ghazi.benayed@unil.ch

Solangne Ghermaouti-Hélie
Faculty of Business and Economics, University of Lausanne, Switzerland
sgh@unil.ch

Abstract—Users count on digital identities to make everyday’s tasks, therefore digital identities become valuable assets. Within networked and interconnected information systems arena, where digital identity related risks arise, effective digital identity management is required in order to secure and protect them. We provide from the literature and discuss taxonomy of digital identity management based on definition-focus. While, user-supremacy processes guarantee user control over attributes and privacy but they should be integrated and aligned to common networked information systems’ security policies and business strategy. We argument that digital identity management should change from being vertical or functional into inter-information systems and horizontal integrated business processes with service orientations. We point out that SoaML-based methodology would help to decompose and reduce digital identity management requirements into a set of collaborative services.

Digital identity management taxonomy; user-supremacy; horizontal processes management; service orientation.

I. INTRODUCTION

User’s information security has been one of the most sensitive areas of concern discussed at different organizational levels for a majority of the world’s leading organizations across all industries [1]. In order to achieve organizational competitive advantage, information systems are moving away from a closed perimeter business model into a networked, an interconnected and an open perimeter-less mode. The new reality has posed new research challenges when dealing with security and particularly in managing users’ identities due to the multiple risks that have been raised within such open and unreliable nature of the environment. Digital identity management (DigIdM) has evolved as a discipline of its own and it is considered as one of the security pillar, which should provide information security, privacy, policies compliance, and trust in order to support information systems’ boundaries expansion and openness [2-5]. In addition, DigIdM has been and is still by far one of the most critical yet very complex and challenging requirement for establishing better business strategies to benefit the economy on a global scale [6].

Abundant research tracks indicate multiple definitions of digital identity management and how such management is a critical component that organizations should be aware of. In this article, we provide and discuss major definitions of DigIdM in literature review and we highlight that intra-information system DigIdM has vertical silos-focus and that of networked information systems requires horizontal end-to-end and processes-focus.

The remainder of the paper is structured as follows. In section 2, we present basic foundations of digital identity and we explain that we don’t distinguish between identity, digital identity, online identity, virtual identity and other designations because all of them are being part of the user’s overall identity. In section 3, we provide and discuss a taxonomy, in which DigIdM definitions are classified based definition-focus perspectives. In section 4, we explain the need of horizontal process view instead of vertical one. In section 5, we discuss how horizontal user-supremacy DigIdM processes and services orientations are becoming requirements of open and interconnected information systems context. Finally, we conclude in section 6.

II. DIGITAL IDENTITY

A. Identity and Digital Identity

Identity is defined as a collection of attributes. Identity attributes are classified and organized into three related groups, called tiers [7]. Tier1 derives from attributes and traits associated with a person that makes him unique such as personal characteristics, special interests, favorite activities, and hair color. Tier2 consists of context-specific attributes that are assigned to a person by others in the sake of identifying him temporarily within that context and based on some kind of relationship. Driver’s license, credit card, health insurance card, library card are all examples that hold tier2 attributes. Once the relationship that defines the identity is terminated, the context changes, the attributes associated with it are no more useful. The author [7] stresses the social side of tier2 identity and calls it social identity, which is constructed in response to those with whom a person came into contact of such as family members, friends, and neighbors, regarding the way he portrayed himself to them in person. Tier3 deals with the identity of a group and profiling. Marketing companies classify a person as a male over 50, a Swiss Air frequent flyer, and a Geneva resident. A person perceives the value and benefits of tier2 identity relationship, which is usually established with his consent to meet a real need, however, tier3 relationships are usually forced on us and rarely meet a real need. Unsolicited commercial email or spam is tier3 identity issue [3]. Digital identity is seen as an intersection of identity and technology in the digital age [3, 8, 9].