Abstract—Digital identity becomes a valuable asset and protecting it becomes a requirement. Digital identity metadata XML-based scheme is proposed to reduce digital identity risks within digital memories and at information overabundance and strengthen user’s control over his identity.

Digital identity; digital memories; digital identity risks; metadata scheme.

I. INTRODUCTION

“It seems that you are me. But if you are me, then who am I?” cried Nasrudin when he awoke and found his name tag on the joker’s chest. Before going on a trip, Nasrudin’s wife put a sign around his neck with his name on it so that he would not forget his identity. In his way, he spent a night at a caravanserai; while he slept, a joker took the sign and put it around his neck. For many centuries, stories of the holy fool Nasrudin have been studied in Sufi circles for their hidden wisdom. We don’t intend here to introduce who-am-I philosophic debate over personal identity, but Nasrudin’s dilemma reflects the feelings of confusion, anger, unfairness and embarrassment when a Web user discovers that he lost control over his identity or underwent a privacy breach incident. He may find through who-am-I “ego-googling” or Spock people finder search that part of online reputation has been defamed and as a consequence his job search is hindering. Stacy’s case [1] illustrates that she was denied a teaching diploma because of a party photo she posted on her social network profile. For security reasons, Nasrudin’s wife had a good sense by reminding her husband to take care of his identity before he leaves on the journey. It is said that “elements of security in computing begin with identity” [2]. Currently, on online journeys, a web user is increasingly leaving trails that are memorized by the network, while the user, in most cases, still does not have the capabilities to delete them if he wishes. Major online service providers memorize, access, and exploit ‘Web of trails’ for their own commercial benefits, and as a result, users are losing control over their personal data. This risk is increasing in digital world and at overabundance data time, thus, this could compromise online security, privacy and trust [3-6]. In addition, Nasrudin’s story tells how easy identity theft and frauds when a Web user publicly discloses and makes identity accessible without anticipating the consequences of such actions. One hundred million worldwide Facebook users are threatened by identity theft as a repercussion of Facebook hack case [7], in which personal details have been collated and published on file-sharing service. Security threats and vulnerabilities have irrupted. Attackers are more sophisticated and focused on information that has tangible value. As a consequence many service providers are investing on security [8].

In this article, we investigate and present risks associated with digital identity within digital memories and at data overabundance age. We provide a metadata-based technical approach with XML-based implementation towards reducing such risks.

The paper is introduced in section one and structured as follows. In section two, we present a literature review about definitions, basic concepts and foundations of digital identity. In section three, we highlight salience of digital identity in economic life and major challenges within digital memories and at data overabundance time. In section four we present major digital identity risks. In section five, we investigate contributions and gains of metadata and then we propose and explain digital identity metadata scheme in order to reduce digital identity risks within digital memories and at information overabundance time. Finally, we conclude in section six.

II. DIGITAL IDENTITY: BASICS AND PRELIMINARIES

Identity is defined as a collection of attributes. Identity attributes are classified and organized into three groups or tiers. Each set maintains relationships with others, on which the perceived value is different. Tier1, or personal identity [9], 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 [9] 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