Processes View Modeling of Identity-related Privacy Business Interoperability

Considering User-Supremacy Federated Identity Technical Model and Identity Contract Negotiation

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

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

Abstract—Federated identity is a distributed system that is deployed across multiple parties. Service providers still hold the absolute power over people identities. So, identity-related privacy is considered as a mean to entrench subjects’ control over identities and foster trust among multiple involved parties. Thus, identity-related privacy should interoperable, which can be guaranteed through the capture of requirements from different polices related to identity. In this article, we provide and explain a BPMN processes view of the requirements allowing them to be ready to-implement, clear, easy to-understand by each party wishing to collaborate within or across federated identity systems. We highlight that present-day practitioners should be able to translate requirements with user-supremacy federated identity technical model concepts into a set of rules and take into consideration details of identity contract negotiation in order to successfully deliver processes view. BPMN collaboration and choreography diagrams are used to describe seven processes and a sub-process, which would provide a useful way to gain alignment between requirements and IT.

BPMN; federated identity; privacy processes; user-centric; user-supremacy.

I. INTRODUCTION

The word ‘user’ has been coined in computing referring to an ‘un-experienced participant’. Narrowly, in the context of software engineering, the ‘user’ is considered as “the least flexible component of any system” [1]. We recognize that new IT products are to be designed on the basis of the least intelligent user’s experience, but this is also clearly applicable in the security context. Security today is intimately linked to privacy, which could strengthen user’s power position. IT products require awareness of, and compliance with, numerous privacy laws and regulations in order to secure users from identity related crimes and personal information misuse.

Identity is defined as a as a unique set of attributes [2]. Attributes could be hair color, preferences, identifiers and credentials. Various combinations of these attributes form multiple identities related to the same user or subject. A subject could have many identities such as citizen, family member, worker, and customer [3]. Digital identity is an intersection of identity and technology and represents identity in the digital world [4–7]. Wherever we go, we leave traces of fragmented information about our identity. We leave a comment in a forum, fill out a form, maintain a blog, create full profile that comprises a photo, name, phone number, and other information in a social network, and conduct a parallel existence. As a consequence, a growing amount of scattered and unordered fragments of digital identities are distributed over different environments [8]. People feel concerned and worried about the digital world, security and loss of control [9]. We believe that identity cannot be split, thus, we don’t distinguish here between identity, digital identity, online identity, virtual identity and other designations because we are convinced that all of them are integrated and unseparated parts of the subject’s overall identity.

The dramatic increase in identity theft is unlikely to end soon [10]. Theft could be 1) identity attributes loss that can cause companies’ embarrassment and a bruised reputation; 2) hijacking existing accounts: most of phishing attacks are against financial services and 3) concocting new accounts: the fraudulent opening of new accounts using another’s identity is dangerous. When identity credentials are given to the wrong person, the strength of identity technology becomes powerless. Controlling the exposure of sensitive identity attributes could be possible through privacy protection. Thus, privacy best practices and policies can contribute to secure identity and reduce the organization’s exposure to embarrassing data loss [3].

We aim in this article to promote that identity-related privacy should be considered as a set of requirements from the start. We provide also a process view of identity-related privacy requirements to make them easy to understand by IT professionals in interconnected and inter-organizational information systems initiatives. We end up to explain that in order to provide more users’ control and higher security level over identity, privacy implementation should be based on user-supremacy federated identity technical and business negotiation between the involved parties in federated identity system. The process view provides a clear description of the negotiation operations and possible agreements or disagreements.

The remainder of the paper is structured as follows. In section 2, we present basic foundations of federated identity and we define user-supremacy technical model against the user-centric one. We explain how the adoption of user-supremacy federated identity technical model, which is a user’s control-enriched derive of user-centricity, could provide user’s power and control over identity. In section 3, we describe identity-related privacy business interoperability as a set of eleven rules that are already identified through the translation of identity-related privacy requirements [11] with the foundations of user-supremacy federated identity technical model. In section 4, we describe seven processes