Chapter 92
Privacy Compliance Requirements in Workflow Environments

Maria N. Koukovini
National Technical University of Athens, Greece

Eugenia I. Papagiannakopoulou
National Technical University of Athens, Greece

Georgios V. Lioudakis
National Technical University of Athens, Greece

Nikolaos L. Dellas
SingularLogic S.A., Greece

Dimitra I. Kaklamani
National Technical University of Athens, Greece

Iakovos S. Venieris
National Technical University of Athens, Greece

ABSTRACT

Workflow management systems are used to run day-to-day applications in numerous domains, often including exchange and processing of sensitive data. Their native "leakage-proneness," being the consequence of their distributed and collaborative nature, calls for sophisticated mechanisms able to guarantee proper enforcement of the necessary privacy protection measures. Motivated by the principles of Privacy by Design and its potential for workflow environments, this chapter investigates the associated issues, challenges, and requirements. With the legal and regulatory provisions regarding privacy in information systems as a baseline, the chapter elaborates on the challenges and derived requirements in the context of workflow environments, taking into account the particular needs and implications of the latter. Further, it highlights important aspects that need to be considered regarding, on the one hand, the incorporation of privacy-enhancing features in the workflow models themselves and, on the other, the evaluation of the latter against privacy provisions.

DOI: 10.4018/978-1-5225-7113-1.ch092

INTRODUCTION

Workflows, that is, well-defined sequences of tasks coordinated in order to achieve a variety of business, scientific and engineering goals, have emerged as a prominent technology in current distributed and dynamic environments, fuelled also by the proliferation of Service Oriented Architectures (SOA) (Papazoglou & van den Heuvel, 2007) and their loose-coupling nature. However, workflow systems are in many cases characterised by serious privacy implications due to their nature, which natively relies to a large extent on access to and exchange of data. Besides, they are often based on and foster collaboration within heterogeneous environments and among many stakeholders, something that significantly complicates the direct and effective use of already existing solutions to privacy protection. Indeed, in such systems, balancing the competing goals of collaboration and security aspects in general is a difficult, multidimensional problem: on the one hand, establishing useful connections among people, tools, and information is a prerequisite, while, on the other, the availability, confidentiality, and integrity of these same elements must also be ensured. The key challenge arising in such context is that the various activities must no longer be considered only "in isolation" but also with respect to operational and data flows, resulting in a holistic view across the corresponding procedures; in other words, required mechanisms (e.g., access control) must be effectively enforced regarding not only individual actions but also large-scale interrelations thereof at the workflow level.

At the same time, the privacy domain is increasingly becoming a legislated area. Data protection laws have been enacted worldwide in order to regulate personal information collection, processing and dissemination (Solove, 2006; Portela & Cruz-Cunha, 2010; Greenleaf, in press). The legal and regulatory framework naturally impacts workflow systems, since business processes implemented as workflows should comply with the associated requirements.

In light of the above, this chapter investigates the issues, challenges and specific requirements related with privacy compliance in workflow environments. In this direction, after some background on workflow technologies is provided, the core legal and regulatory requirements are highlighted in order for the associated challenges for workflow systems to be identified. Thereupon, the main limitations of current technologies with respect to these challenges are outlined. Finally, the fulfilment of the underlying requirements is investigated from a dual perspective: first, the need for the inclusion, at the workflow model level, of structures able to support the in-design specification of privacy policies, leading to targeted privacy configurations enforceable at run-time, and, second, the basic compliance patterns that need to be considered, in order to enable the automatic verification of workflow models against privacy provisions and their automatic transformation in the case of detected violations.

BACKGROUND

In general terms, a workflow is a collection of tasks, i.e., well-specified steps to be completed by available resources towards performing a more complex operational procedure, along with their various interrelations, that denote the order in which tasks are executed and process the information exchanged among them, if any. A workflow is typically abstracted as a directed graph $<T, E>$, with the set of tasks T constituting its vertices and its edges E representing inter-task relations and associated parameters.

Emanating from the first office automation systems, when variants of Petri Nets (Petri, 1962) have been used in order to model related procedures, workflows originally had a purely business orientation