Πρακτικές και μεθοδολογίες ελέγχου διαλειτουργικότητας και ιδιωτικότητας: εφαρμογές σε προηγμένες και ασφαλείς ηλεκτρονικές και κινητές υπηρεσίες

ΠΕΡΙΛΗΨΗ Δ.Δ ΠΑΠΑΣΤΕΡΓΙΟΥ

The design, development and implementation of electronic and mobile (e/m-) services relying on XML and Web Service (WS)-based standards and technologies which are the main components of Service Oriented Architectures (SOAs) is the current trend in the modern era. Due to the nature of these services several issues pertaining to security, privacy, identity management and interoperability have been raised. Initially, the thesis identifies the need for targeted methodologies and frameworks that check and guarantee the end-to-end application interaction capabilities of common services. The thesis proposes a well-formed grey box testing methodology entitled ICoM, able to test whether various services achieve communication effectively based on the adopted standards. ICoM has been applied in order to evaluate the interoperability of the existing autonomous SELIS e-invoicing service and the SWEB e-invoicing service embedded in a SOA-based platform. In addition, the need for privacy aware transactions raises specific problems that aforementioned services need to solve including the privacy-aware managing of identities. The research in this thesis has identified several identity management solutions that implement complete identity handling frameworks. In this diversity of solutions, a SOA designer faces the problem of identifying which framework or specific solution better suites the needs of the SOA he is building, without introducing additional complexity to the design on one hand or leaving out important aspects of privacy management on the other. In this context, this thesis proposes a specific classification of SOAs-designs with respect to the way that the trust relationship among the involved entities, users and SOAs, is established enabling the user to access the provided services. Although, the last decade, the provided e/m-services have been increased, the level of trust and confidence remain low, preventing their adoption and prevalence. Nowadays, despite the formulation of Federations, where a trust relationship among the involved parties is established and monitored by Identity Management System (IMS), has been considered as the most appropriate solution to build Trust, the notion of Trust is still very vague. The accumulation of behavior (reputation) of the parties involved in an e/m-transaction has been already used as a quantitative measure of trust. In this context, this thesis includes an overview and an evaluation of existing reputation systems. The thesis acknowledging the need for a more privacy-respecting design of reputation systems, contributes towards this direction proposing an Identity Management Reputation Service (IMRS) which operates in the IMSs in order to preserve and enhance trust. Finally, the Phd thesis acknowledging the significance of connection anonymity, includes a review of the existing network-based approaches to anonymity and proposes an anonymity SOA framework built upon widely used standards and technologies such as the WS-Addressing and deploys the Tor anonymizing network, taking advantage of the benefits that it offers.