Provision of Secure Policy Enforcement Between Small and Medium Governmental Organizations

Nikolaos Oikonomidis, Sergiu Tcaciuc, and Christoph Ruland

Institute for Digital Communication Systems, University of Siegen
{nikolaos.oikonomidis, sergiu.tcaciuc, christoph.ruland}@uni-siegen.de

Abstract. This paper is derived from research work conducted within eMayor project, funded by the EU committee (IST-2003-507217). Motivation of the project was the fact that small and medium sized governmental organizations (SMGOs) interact frequently with citizens and/or businesses, to offer paper-based and electronic services utilizing a limited number of resources (e.g. employees and funds). SMGOs also interact with each other, in local or cross-border transactions, to exchange information on behalf of citizens, businesses or the organization itself. Main objectives of eMayor are to build a secure, interoperable, cost-effective and open e-government platform, addressing the needs of SMGOs. The core of the eMayor platform will be built upon state-of-the-art web-services technology which enables the interoperability with existing web-services already provided by governmental organizations. However, the problem of heterogeneity of security, access control, privacy and process flow policies among the different organization remains, both on national and international level. To provide full interoperability a framework which solves the addressed issues and provides transparent coordination of different policy enforcement mechanisms is needed. Such a framework, enforcing security and access-control policies across a decentralized network of governmental organizations is discussed in this paper. First the system architecture of eMayor platform is introduced. Thereafter, general and specific security requirements that apply to an interoperable e-government platform are discussed and the trust model together with the roles which pose different authentication and authorization attributes are depicted. Results of the requirements analysis provide input for platform design. Policy enforcement mechanisms together with an overview of security solutions on identified communication channels are presented. Deployment of chosen technologies, specifically for distributed e-Government structures, is introduced taking into account the possible extensions in order to provide higher level of security standards. The paper concludes with final objectives on policy enforcement framework and outlines the work in progress.

1 Introduction and Motivation

Citizens interact at regular intervals with municipalities or municipal organizations. Public administrations offer a variety of services like requests/processing of certificates, (local) tax payment, and promotion of city information. An effective and effi-
cient service provision brings benefits to both municipalities and the involved citizens/customers of the particular services. Electronic services provide a unique opportunity to enhance and expand the offered services by making them more flexible, since they may provide location and time independent access to the citizens, as well as a rapid execution of services that might otherwise require a considerable amount of time and effort. These benefits are not realizable where there is a lack of the proper infrastructure to serve citizens, such as in small municipalities with limited resources and/or large areas of responsibility.

The provision of such electronic services can be achieved with the use of multimodal access mechanisms [1]. Due to the fact that exchanged data in forms and documents may contain private or sensitive data, it is imperative to introduce security mechanisms that guarantee to citizens a trustworthy means of communication. Trust can be achieved through the use of cryptographic mechanisms that assure the security requirements of confidentiality, authentication of data and users, integrity of content, non-repudiation by the origin and non-repudiation by the receiver. Further, cross-border services involve different municipalities and other public authorities in the processes. The support of municipalities across Europe in their cooperation is one of the main objectives of the eMayor project. Legal aspects are very important to be considered to run e-Services that must be legally validated.

2 eMayor Project

eMayor addresses the specific audience of SMGOs across Europe. The project looks especially at transactions that are performed on an European level. Such services typically handle the secure exchange of documents, forms, and other information across national borders. The terms of “SMGO” and “cross-border service” has been defined by the eMayor consortium. All participating municipalities fall into the category of SMGOs. They vary greatly in size, the smallest one with 10.000 inhabitants and the biggest one with well over 500.000 inhabitants.

The target group for eMayor comprises municipalities up to half a million citizens normally located in urban or metropolitan areas. The approach is to build a generic platform (eMayor platform) hosting municipal services that are generically designed, adapted and implemented considering specific stakeholder needs, and then validated within several municipalities.

3 Platform Description

The realization approach of eMayor has been planed to go through three major phases: requirements analysis, system design and platform implementation. During the requirements analysis phase of the project, needs and requirements of SMGOs from four different European countries have been investigated. Existing services, data formats and infrastructures were examined and evaluated. The evaluation resulted into the construction of usage scenarios. The result of the requirements analysis served as the base for the next phase towards the realization of the platform, namely the design of