Introduction

The objective of the 2nd International Workshop on Certification and Security in Inter-Organizational E-Services (CSES-04) was to discuss technical and organizational aspects regarding the two interrelated areas of certification and security of e-services, presenting both real-life application experiences and methodological proposals, from participants belonging to the governmental, industrial and academic communities.

The field of services managed and accessed through communication networks is, in fact, growing in magnitude throughout society. A crucial aspect of this process is the capability of certifying what has occurred in the interaction over the networks, and ensuring that the integrity of the involved computer-based systems was maintained. This is even more important given the uptake of distributed computational infrastructure oriented to service provision, like Web-Services and Grid.

Certifying the execution of an e-service provided on the network as the result of the interaction among independent organizations is a critical area for the underlying IT-infrastructure. In fact, given the legal value that is often attached to data managed and exchanged during the execution of such an inter-organizational e-service, being able to document what was actually carried out is of the utmost importance. This is made more complex in cases where e- services are based on legacy systems managed by autonomous and independent organizations, as often happens in the public administration sector.

Additionally, the whole area of security issues, from the basic (availability, authentication, integrity, confidentiality) to the more complex (e.g., authorization, non-repudiation) involves the equally critical ability to track down responsibilities ("who did what"). This capability is mandatory to increase the presence and use of e-service IT-infrastructures.

The two areas of certification and security have therefore a common technological intersection, since both are based on the reliable and efficient mon-

itoring of executed and running processes. Monitoring requires the capability of tracing and analyzing what is going on in the distributed system and in the underlying IT-infrastructure. Monitoring is also important for contractual and quality reasons, i.e. to serve as a basis for checking the respect of obligation and duties and the value of performance levels.

Certification and security are as well fundamental processes in organizational and economic terms. Organizationally, they support an easier cooperation between autonomous and independent organizations in the building of a new complex service to be made available in the electronic marketplace. In fact, they allow to build this new cooperative service without having each involved organization fear to lose their control and their influence on its core business and on application fields it knows better. Moreover, by allowing to clearly pinpoint responsibilities in the cooperation they enable a more efficient management of organizational interactions. Economically, they make it possible, for example, to provide and effectively manage value-added services with many different "options", supplying different service levels with different fees. Additionally, they support the substitutions of providers of basic services, thus fostering economic competition and quality level improvements.

Certification and security are also two foundation stones on which to base the realization of more advanced e-services obtained by composition of more elementary ones. In fact, operating at the immaterial level of electronic technologies is easier to combine and integrate existing services to provide new and better ones. But, since systems providing advanced e-services are based on a complex interaction among many large IT systems higher risks of failure are possible due to the lower degree of system reliability that newest information and telecommunication technologies have.