Chapter XVIII
European E-Signatures Solutions on the Basis of PKI Authentication Technology

Ioannis P. Chochliouros
Hellenic Telecommunications Organization S.A. (OTE), Greece

Anastasia S. Spiliopoulou
Athens Bar Association, Greece

Stergios P. Chochliouros
Independent Consultant, Greece

Konstantinos N. Voudouris
Technological Educational Institute of Athens, Greece

ABSTRACT

This chapter presents systems of certification authorities and registration authorities and other supporting servers and agents that perform certificate management, archive management, key management, and token management functions. These activities that support security policy by monitoring and controlling security services, elements and mechanisms, distributing security information, and reporting security events are examined with the main focus on PKI authentication technology.

INTRODUCTION

After a period of rapid growth in 1998-2000, the electronic communications sector is now undergoing a complete "re-adjustment" process, with targeted investments focused on specific technological sectors, able to satisfy a variety of customer-oriented requirements in global and competitive markets. However its implications and possible outcomes raise extremely important

issues for the future and for economic growth, worldwide (European Commission, 2003). In particular, the importance of the electronic communications sector lies in its impact on all other sectors of the economy: It offers the potential and the dynamism for organisations to make best use of their investment in Information Society Technology (IST) and to realise productivity gains, improvements in quality and opportunities for greater social inclusion (Chochliouros & Spiliopoulou, 2003a).

New communication technologies, new media, the Internet and devices carrying modern functionalities are expected to meet consumers' demand for seamless, simple and user-friendly digital tools providing access to an extended range of services and content (i2010 High Level Group, 2006).

In particular, electronic communication networks and information systems have been developed exponentially in recent years and are now an essential part of the daily lives of citizens in various environments worldwide, also comprising the sector of Europe. Such information systems and network infrastructures constitute fundamental "tools" to the success of the broader European economy in the international scenery (European Commission, 2002).

Despite the multiple and obvious benefits due to the modern (and converged) electronic communications development, this evolutionary process has also brought with it the worrying threat of intentional attacks against relevant systems and networks. As cyberspace gets more and more complex and its components increasingly sophisticated, especially due to the fast development and evolution of (broadband) Internet-based platforms, new and unforeseen vulnerabilities may emerge and affect further progress (Organization for Economic Coordination and Development, 2004). Moreover, as Internet becomes ubiquitous for all business and personal communications, the sensitivity and economic value of the content of information transmitted is highly increasing (Shoniregun, Chochliouros, Laperche, Logvynoskiy & Spiliopoulou, 2004).

Thus, the rollout of innovative technologies (such as broadband and 3G) together with the development of new content, applications and/or (public and private) services (European Commission, 2004), results to new and severe security challenges (Kaufman, 2002). Addressing security issues is also crucial to stimulating demand for new electronic communications services and to develop, further, the digital worldwide economy (Chochliouros & Spiliopoulou, 2005). Networks and information systems are now supporting services and carrying data of great value, which can be vital to other forms of applications. Increased protection of infrastructures is therefore necessary against various types of attacks on their availability, authenticity, integrity and confidentiality. In the relevant scene of the current European marketplace, the use of encryption technologies and electronic signatures towards providing enhanced security, are becoming indispensable (European Parliament and Council of the European Union, 1999; Brands, 2000), while an increasing variety of authentication mechanisms is required to meet different needs in wider converged environments (European Commission, 2002).

Within such a generalized context, Public Key Infrastructure (PKI) can perform a central part of securing today networked world. PKI can provide a focal point for many aspects of security management while, *at the same time*, can serve as a "enabler" for a growing number of various security applications both in private and public organizations (International Organization for Standardization, 2005). Most standard protocols for secure e-mail, web access, virtual private networks (VPNs) and single-sign-on user authentication systems make use of some form of "public key" certificates and for that reason require some specific form of PKI. The security of transactions and data has become essential for the supply of electronic services, including e-Commerce and online public services, and