# Chapter XXXIII
# Public Key Infrastructures as a Means for Increasing Network Security

**Ioannis P. Chochliouros**
*Hellenic Telecommunications Organization S.A.*
*and University of Peloponnese, Greece*

**Stergios P. Chochliouros**
*Independent Consultant, Greece*

**Anastasia S. Spiliopoulou**
*Hellenic Telecommunications Organization S.A.,*
*General Directorate for Regulatory Affairs, Greece*

**Evita Lampadari**
*Hellenic Telecommunications Organization S.A.,*
*General Directorate for Regulatory Affairs, Greece*

## ABSTRACT

*The work investigates some "core" features of public key infrastructures (PKI), including fundamental technologies and infrastructures, within the context of recent market demands for increased network security applications. To this aim, we explain the basic features of public key cryptography, in parallel with a variety of other major PKI functional operations, all able to affect network development and growth. Then, we discuss some among the relevant basic and PKI-derived services, in order to comply with current needs and security requirements, thus supporting both usage and deployment of such infrastructures in competitive markets. In addition, we focus on several recent advances of information and communication convergence, and the effect those advances have on the notion of PKI, especially if considering future challenges. PKI have now become a central part of securing today's networked world and it should be expected that it will continue to have a huge impact on businesses. Furthermore, we correlate the above activities to recent European regulatory initiatives and similar commonly applied policies, to promote the appliance of digital signatures in a fully converged and liberalized market environment.*

## INTRODUCTION

After a period of fast growth from 1998-2000, the electronic communications sector is currently undergoing a "severe" adjustment process. Its implications and possible outcomes raise extremely important issues for the future and for economic growth worldwide (European Commission, 2003). In any case, 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 organizations to make best use of their investment in information society technology (IST) and to realize productivity gains, improvements in quality, and opportunities for greater social inclusion (Chochliouros & Spiliopoulou, 2003).

The rollout of innovative technologies (such as broadband and 3G) as well as the development of new content, applications, and/or (public and private) services (European Commission, 2004) result in new 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 applications. Increased protection against the various types of attacks on infrastructures, therefore, is necessary to maintain their availability, authenticity, integrity, and confidentiality. In the current European markets, the use of encryption technologies and electronic signatures towards providing enhanced security is becoming indispensable (Brands, 2000; European Parliament and Council of the European Union, 1999), while an increasing variety of authentication mechanisms is required to meet different needs in converged environments (European Commission, 2002).

Within such a generalized context, public key infrastructures (PKI) are becoming a central part of securing today's networked world; they can provide a focal point for many aspects of security management, while, at the same time, they can serve as an "enabler" for a growing number of various security applications, both in private and public organizations (International Organization for Standardization (ISO), 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 electronic commerce (e-commerce) and online public services, and low confidence in security could slow down the widespread introduction of such services. Given the rapid evolution of today's computer and network technology, our work intends to examine the impact of this evolution on the notion of PKI and the supporting business and legal framework in the context of relevant policies, mainly promoted through the European Union (EU).

## BACKGROUND: PKI FUNDAMENTAL TECHNOLOGIES AND BASIC INFRASTRUCTURES

In general, a PKI is a combination of hardware and software products, policies, and procedures that offer enhanced security, required to carry out e-commerce activity in order that various users can communicate securely through a "chain of trust." Its basis is digital identifications known as "digital certificates" (Brands, 2000). These act like an electronic passport and bind the user's "digital signature" to his or her public key. In the following sections, we discuss some basic notations relevant to public key cryptography processes, and then we analyze some essential features of PKI. In fact, PKI is an authentication technology, a technical means for identifying entities in an environment.

## PUBLIC KEY CRYPTOGRAPHY

Public key cryptography is used (Feghhi, Williams, & Feghhi, 1998) in conjunction with the following options to create a technology for identifying entities: (i) a mechanism for establishing trust according