HELLENIC REPUBLIC
MINISTRY OF DEVELOPMENT
SECRETARIAT GENERAL FOR INDUSTRY

MINISTRY OF ECONOMY AND FINANCE
MINISTRY OF THE INTERIOR, PUBLIC ADMINISTRATION & DECENTRALIZATION

OPERATIONAL PROGRAM
FOR THE INFORMATION SOCIETY

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND

Work cycle B
Task Force TF B1

"INFORMATION & COMMUNICATION SYSTEM SECURITY IN e-BUSINESS"

Executive Summary of Deliverable

Coordinators: Mr. Sokratis K. Katsikas, Vice Dean of the University of the Aegean
Ms. Lilian Mitrou, Personal Data Protection Agency

Rapporteur: Mr. Stefanos Gritzalis, Assistant Professor at the University of the Aegean

Information & Communication Systems Engineer Department

Athens, July 2002

1. Need for Secure e-business

1.1 Framework for the development of the Information Society and Economy

The general application of Information and Communication technologies is today the main drive of socioeconomic development internationally, leading toward the further shaping of the *Information Society.* Such developments have already started to cause great changes in the international economic, social, and cultural tissue.

More particularly in the economic sector, the general use of the possibilities offered by open networks, leads to an ever increasing globalization of trade, competition, and investments, thus leading to the creation of the *Information Economy.* Such prospects create significant possibilities for private businesses. However, at the same time they also mark the need for the public administration to take urgent action toward the modernization of the services provided to the benefit of the society, on the one hand, and the reduction of operating costs, on the other hand.

In accordance with a study conducted by the International House PriceWaterhouseCoopers, and the results of which were announced in Spring 2000 at the World Economic Forum in Davos, Switzerland, the turnover of businesses around the world shall increase in just a few years as a result of the use of the possibilities offered by the Internet, while businesses performing their activities in that field are not bound to face any serious financial problems within the next three years. 9 out of 10 businesspeople appeared optimistic with regard to the medium and long term growth perspectives of their respective businesses due to doing business over the Internet. In Greece, in accordance with a study by Research International conducted on the behalf of Intel at the end of 2000, from a sample of 1000 small and big businesses from the IT, communication, and financial services, manufacturing and retail sectors, 70% intend to use the possibilities offered by e-commerce, and 43% of them intend to do so shortly, although at the time the study was conducted only 6% of such businesses carried out commercial transactions over the Internet.

However, all of the aforementioned studies confirmed the prevailing opinion that the European Union lags significantly in this sector as compared to the US.

Toward that direction, the Commission had already approved, since January 26th, 2000, a particularly ambitious program for promoting e-commerce in the European Union. The objective is to reduce the gap between the EU and the US in terms of e-commerce. This challenge is important and all required actions are extremely urgent, if one takes into consideration that PCs have already penetrated to 50% of US households, while these figures for the EU and Greece are 30% and 20% respectively.

Also the percentage of US households connected to the Internet is over 30%, while this figure is over 15% in the EU, and about 10% in Greece, representing 900,000 people (Eurobarometer 1999 and V-PRC 2001).

At the same time, the European Union is promoting further the *eEurope* initiative, aiming at also promoting regional cohesion through the Information Society.

Actually, the statements of Finnish Commissioner, Mr. Likaanen who is responsible for the Information Society and Business Policy, are of particular interest, and in accordance with which e-commerce appears to be giving priority to three sectors: banking, tourism and PC sales.

1.2 Secure commercial transactions over the Internet

Nonetheless, recent studies in the US, the EU and Greece point out that business initiatives over the Internet are often suspended due to security issues, which in the beginning cause worries and then discourage potential commercial partners. It is estimated that until recently in the European Union the ratio of secure Web servers and habitants was 1:100,000, while this ratio for Greece is estimated to just 0.2:100,000.

In order to face security related problems, policies must be made, strategies must be developed, methodologies need to be designed, mechanisms must be implemented, as well as the whole enterprise must be constantly assessed, in order to achieve security and reliability during any communication.

In order for a complete framework for secure transactions to be implemented, the Commission, has as of 1997, published a se to techniques, regulatory and legal issues, and announced the preparation of actions for designing a regulations and actions framework toward the implementation of a secure goods and services emarketplace.

Usual security requirements on the part of users in terms of electronic transactions are: confidentiality and integrity of the messages exchanged, authentication of senders, non-repudiation of message transmission and reception, system availability, timestamping of message reception and transmission, accountability, etc. An important contribution to meeting equivalent requirements is that of encryption applications. For instance, digital signatures are used to verify the data sender, and to ensure non

alteration and non repudiation of messages. Encryption/ decryption are used to maintain the confidentiality of the data involved in the communication.

In accordance with the Commission, the existence of different opinions in legal and technical matters in the wider domain of network security, could create significant obstacles to the internal market, hence it would be enough to hinder the development of new economic activities related to e-commerce. To that end, the Commission has already taken actions and pertinent decisions, in order to assist the existing e-transactions framework. To that direction, Directive 1999/93/EC of December 13th, 1999 has been issued on a Community Framework for electronic signatures, and it was published in the Official Journal of the European Communities on January 19th, 2000. In Greece this Directive has been transposed to the applicable legislation through the publication of Presidential Decree 150/2001 (Government Gazette No. 125 A/ 25.6.2001).

2. Positions and opinions of Task Force B1

Task Force B1 *"Information & Communication System Security in e-business"* has recorded the positions and opinions of its members, as these were discussed during the meetings held, regarding the most important issues of the knowledge domain, placing emphasis on two individual areas:

- Information Security Management in SMEs;
- Personal Data and Privacy Protection in e-business.

In order for the general practice with regard to the above issues among Greek SMEs to be depicted, relevant questionnaires were sent to a number of private businesses involved in various sectors of the economy. The most important points that resulted from the answers given are the following:

- most business executives are sufficiently or very familiar with security issues, and consider unauthorized access to corporate resources and computer viruses to be the most important risks;
- 62% of businesses answered that there have not been any cases of security violation, 21% responded that there had been such cases, while the percentage of those that answered "Don't answer" was 16%;

- 76% of the protection measures adopted by businesses are based on the know-how of executives, while 24% have used external consultants;
- less than 50% of authorities have elaborated plans for the continuation of their business activities;
- the largest percentage answered that they are sufficiently familiar with the terms “personal data” and “privacy protection”, while they state they know of the existence of relevant legislation in our country;
- 47% of authorities have contacted the Personal Data Protection Agency within the framework of personal or business activities;
- 45% of businesses stated that their website/ webpage contains a privacy statement;
- 12% of businesses use cookies or other similar technical options, while 8% did not answer;
- over half answered that they do not know the term "privacy strengthening technologies";
- almost all businesses asked, stated that they believe that fears and hesitations on the protection of personal data have dissuaded consumers from making intranetwork transactions.

At the same time, considering the Information Security Management issues to be of particular importance, the Task Force B1 deliverable is based on the ISO/IEC 17799 “Information Security Management” standard which was prepared by British Standards Institution (BS 7799) and adopted by Joint Technical Committee JTC 1 “Information Technology”, along with its acceptance by national standardization authorities. It addresses information security management issues and is applicable to and of particular importance for the required actions and activities of businesses of any sort, which carry out their activities in digital economy and e-business. Of particular interest is the possibility of its application to SMEs, since it contains complete basic rules of the practice used for achieving an efficient information security management, regardless of the sector of activities of any given business.

The Task Force B1 general conclusions are:

- the extension of the use of electronic services to e-commerce, e-business, e-government is considered particularly important, achieving, however, a documented high security and reliability level;
- it is estimated that the promotion of the required actions on the part of the National Telecommunications and Post Committee for determining the accreditation, operation, supervision and control framework for Certification Service Providers is extremely urgent;
- the first – pilot – efforts of public authorities and organizations to promote and use the possibilities offered by digital signatures, as these are established under Presidential Decree 150/2001 (25.6.2001) in line with the European Parliament and Council Directive 1999/93/EC, are positive;
- the elaboration of detailed and clear signature policies is useful for the electronic services provided within the framework of the Information Society;
- the possibility to use risk analysis and management methodologies for information systems, is considered particularly useful in taking efficient countermeasures, elaborating security policies, and developing complete security plans by public and private corporations;
- the need to assure business systems is stressed, in the usual by now cases where the development of information systems and/or data processing have been outsourced;
- the task force reminds the usefulness of the development of an efficient Business Continuity Plan, adapted to the size of any business and to the level of importance that the information system has for it;
- the results of the work of the Personal Data Protection Agency to avoid the creation of "suspicious citizens" refraining from being involved in electronic transactions over the Internet are particularly positive.