# Design and Implementation of a Secure Communication Platform with the Use of Smartcard Mobile Media Enabled Asymmetric Cryptography

Research project funded by the Scientific Research Projects Directorate of Ege University under grant 2004/UBE/001

## Abstract

In this project, we introduce the design and development of a framework for an e-mail protocol where system security components as authentication and message confidentiality are achieved via smart card mobile media and users exchange data with asymmetric encryption. The system operates under client-server architecture. On each client within the system, software components are used as an interface to communicate with smart cards and to make message exchange over a predetermined electronic mail system possible. Within the system developed, security is provided by employing the authentication and confidentiality services of the PGP (Pretty Good Privacy) tool. The use of smart cards enhances the system by providing storage and mobility medium for the private key, but also increases the overall level of security. Having designed and developed the system, we have tested it with messages over real e-mail servers and seen that it operates properly.

**Start Date:** October 1, 2004

**End Date:** July 4, 2005

**Total Budget:** 15.000 TL (~$12,500)

**Project Team:**

Asst. Prof. Dr. Ebru CELIKEL (Principal Investigator)

Geylani KARDAS (Researcher) (Ph.D. Student)

**Related Publications:**

1. Kardas, G., Celikel, E. and Alaybeyoglu, A. (2008) "*A secure message transmission system architecture for computer networks employing smart cards*", Pamukkale University Journal of Engineering Sciences, vol. 14, no. 1, pp. 31-40 (in Turkish).

2. Kardas, G. and Celikel, E. (2007) "*A Smart Card Mediated Mobile Platform for Secure E-Mail Communication*", In proceedings of the 4th International Conference on Information Technology: New Generations (ITNG 2007), April 2-4, 2007, Las Vegas, Nevada, USA, IEEE Computer Society, pp. 925-926, DOI: 10.1109/ITNG.2007.21.

3. Celikel, E. and Kardas, G. (2005) "*Design of a Secure Transmission Platform with Smart Card Supported Asymmetrical Encryption System*", In proceedings of Academic Informatics 2005, February 2-4, 2005, Gaziantep, Turkey, p. 94 (in Turkish).