SOFIA UNIVERSITY “ST. KLIMENT OHRIDSKI”
FACULTY OF MATHEMATICS AND INFORMATICS
DEPARTMENT OF INFORMATION TECHNOLOGIES

Subject:	Pocket PC application enabling secure storage of personal information
Student:	Milena Radeva Iordanova
Tutor:	Assoc. Prof. Dr. Sylvia Ilieva
Defense date:	14.02.2007
Key words:	Pocket PC, cryptography, hash functions, HMAC, data protection, user interface, asynchronous operations

Annotation:

Data protection is becoming an increasingly important problem in modern information society. Everybody’s need to carry various information with them, without at the same time putting it at risk of falling in other people’s hands, is increasing every day. Mobile devices like Pocket PC, smart-phones, and mobile computers, encourage carrying personal information, but the problem for its protection remains.

This diploma paper offers a solution to the problem for secure storage of personal information in Pocket PC. An application is developed, allowing cryptographically secure storage of various kinds

of user data and giving easy access to it. Suitable cryptographic algorithms are chosen, and the authors' implementation is offered for some of them. The problem for a responsive user interface is also solved by using asynchronous operations and a mechanism for two-way communication between the user interface and the threads of the operations being executed.

The developed application is of great practical use; some of the features it offers cannot be found in any of the existing applications the paper looks at.