Secure utilization of local and regional data assets through mobile environments

László Aszalós, Norbert Bátfai, László Csirmaz, János Folláth, Tamás Herendi, Attila Pethő and Péter Varga

Faculty of Informatics, University of Debrecen

In 2008 we started the National Technology Program TARIPAR3 together within a consortium under the leadership Geoview Systems Ltd. The aim of the project is the development of local and regional content industry, establishment of the framework of innovative value added service for the utilization of data assets.

This requires the secure utilization of data through mobile environments. Our task is to develop a package, which enables secure authorization, authentication and data exchange. Moreover, it is possible to perform digital signature to ensure data integrity. The speciality of the problem is that the data providers and clients have different computational powers and are running on different platforms.

Typical providers are computers, which are accessible through TCP/IP, while the clients are programmable mobile phones. They usually utilize the WAP protocol suite for communication. The security provided by the WTLS protocol is insufficent, and the TLS protocol can only be established between the server and the gateway. A further difficulty is, that the gateway translating between the protocols is in the possession of telephone providers: altering their implementation is not an option. Taken all round: a new high level protocol is required, that provides the desirable security.

We have developed a hybrid cryptographic test web application based on Bouncy Castle Crypto API. On the server side, we are working in Java EE environment and our clients are Java-enabled mobile phones. The developed test application can be used to perform cryptographic measurements on real mobile phones.

In the talk we present our first results including the raw plan of the system to be developed.