# DIGITAL SIGNATURE: INTEROPERABLE AND SECURE APPLICATIONS

***Áron Szabó, aron@ik.bme.hu***
*BME Centre of Information Technology*
***Szabolcs Szigeti, szigi@ik.bme.hu***
*BME Centre of Information Technology*

The legal requirements of digital signature that was developed in the second half of '70s was born in 1999 as an European Union Directive which was adopted by Hungary in 2001.

Experts had great expectations in connection with new opportunities of using digital signatures at web-based services or at document management systems but interest remained low. There were also technological reasons in the background among other things. The technology of asymmetric cryptography is almost 30 years old, but developers have just faced the problems of world-wide interoperability 4-5 years back, because of several standards and solutions. This is the reason of generating a signature with one application which can not be correctly verified by another application. Main things are the same such as certificates, algorithms but the format of signatures can be different (PGP, S/MIME, XMLDsig).

Standardization of formats is one of the most important requirements of interoperability of applications therefore IETF, W3C and ETSI standardization bodies started to work out the solution. Beyond technological requirements legal aspects have been taken into account. Finally, the XAdES (TS 101 903) standard was born which fulfilled every requirements in connection with standardized signature formats.

Beyond the standardized signature format, other problems can occur in connection with interoperability. The operational logic of the applications or in some cases the implemented functions of development kits can also be wrong. These opportunities were recognized therefore standardization bodies organized some interoperability tests with the participation of developers.

In Hungary joined group of rivaling developers cooperating with MELASZ and the independent laboratory of BME Centre of Information Technology held the first interoperability test – based on the experiences of IETF, W3C and ETSI – in the autumn of 2005. The success of the project was important for the electronic public administration services and it also provides good example for other member states in the European Union.

The results and experiences of this interoperability test will be explained in the presentation.