Long-term archiving service for electronically signed documents in Hungary

Dr. István Zsolt BERTA <istvan.berta@microsec.hu>
Csilla Éva ENDRŐDI<csilla@microsec.hu>
Microsec Ltd.

Long-term archiving requires a special, dedicated environment for both paper-based and electronically signed documents. However, in case of electronically signed documents this environment is required for a different purpose and it needs to meet significantly different criteria. A cryptographic algorithm that can be used for creating secure signatures today might become breakable in the future due to sudden advances in cryptoanalysis or in computational capabilities. Thus, there is a possibility that today's secure signatures become forgeable in the future.

The Hungarian law on electronic signatures defines a service for the trusted (qualified) long-term archiving of electronically signed documents. The archiving service provider places timestamps on archived documents with the currently most up-to-date cryptographic technology regularly (e.g. on a yearly basis). These timestamps can be used for proving the validity of archived signatures even if a long period of time passes after their creation and even if the then-secure algorithm used for creating them has already become obsolete.

For certificate authorities there are many international regulations, standards and best practices we can rely on and make use of in our systems. However, we cannot speak of such a detailed, widespread and internationally accepted criteria in case of archiving electronically signed documents.

The first qualified archiving service provider started up in the beginning of 2007. In our paper we disclose our experience with designing, implementing and starting this new service along with the challenges posed by the long-term archiving of electronically signed documents.