WHAT IS ARCHIVE ELECTRONIC SIGNATURE GOOD FOR?

Endrődi, Csilla <csilla@microsec.hu>
Berta, István Zsolt, Dr. <istvan.berta@microsec.hu>
MICROSEC Ltd.

There stands the problem, that "old" electronic signatures – just like pristine paper-based signatures – can be hardly verified dependably. As a general rule, the more time elapsed since the creation of the signature, the more difficult the task becomes.
It causes a problem that the validity of a simple electronic signature (one without timestamp) can be proven just while the certificate is valid. That is, authenticity of signature like this vanishes, when the signer's certificate is revoked or expired. Therefore, if the signature must be usable for long time, we must timestamp the electronic signature shortly after the signing process.
Furthermore, it can cause remarkable trouble at the posteriori verification, that in the course of time the information needed at the verification (revocation information, certificates, signature policies) can be lost. We can prevent this situation by attaching these data for the electronic signature.
In addition, the certificates of used timestamping authorities can be expired, what induces the invalidity of the formerly given timestamp. Furthermore, it can happen that the applied cryptography algorithms became obsolete with the used size of key. Than they became crackable, that is the signature became falsifiable. The last two problems are superable by regularly posting new archive timestamp for the signature.
It is visible, that for assuring long-term validity, the procuring and attaching of several validation information is needed. Range of the data to be attached depends on the time-period in which the signature should be verifiable, and the security level which the verifier requires. Accordingly to these levels, distinct electronic signature formats are defined. ETSI (European Telecommunications Standards Institute) TS 101 903 recommendation contains the requirements of the XML format electronic signatures, it determines eight signature formats. In Hungary, the recommendation issued by the IHM "technical specification of electronic signatures applicable in civil services" basically builds on the previous one. This defines the "momentary", "short term", "long term" and "archive" signature formats.
The highest security level is provided by the archive signature; the most elementary problems are solved by this, even for long time period. Nevertheless, there can be found some special affairs, when the validation of this type of signature – even thought the precise application of the recommendation – can lead to disputed result. Such situations can be raised by the deficiency of the applied PKI solution (e.g. CRL technology, application of obligatory waiting period).
In our talk we review the electronic signature formats. We introduce the data elements of the archive signature, the rules about its creation and treatment, and the available security level. We delineate those PKI situations, which possibly can cause some problems even the application of archive signature. Taking into account these, we can answer the question: what is good for, when and against what can shield the archive electronic signature.