IKTA5-160/02.

Biometric digital signature

Project summary

The rapid development of computer science made it necessary to accept documents manifested only in electronic format as conventional, paper-based ones, therefore *authenticity has to be provable*. Authenticity of electronic documents is required by e-business applications, electronic administration, tax returning, and other customer relation oriented solutions. Hence it is necessary to have available secure electronic signature techniques, which can provide the *authentication* of the signer individual, *non-repudiation* of the fact of signing and *protect the integrity* of the signed document using strong cryptographic methods.

The technology of *biometric digital signatures* that this project proposal is based on fundamentally concentrates on the strengthening of signer authentication and non-repudiation. The current technology of digital signatures is based on public key encryption, in which strong cryptographic algorithms guarantee that the digital signature of a document can only be created using the proper secret key, and only those signatures can be successfully verified using a public key that were created with the proper secret key-pair. The correspondence between the real person and the public key is justified by Certification Authorities.

Since the strength of cryptographic algorithms can be raised to almost any high level – typically by setting the key-length –, the weakest link of the chain during the verification of an electronic signature is the correspondence between the real person and the secret key. The equipment holding the secret key can be stolen, while the access of the key can only be regulated using passwords in current solutions, what is practically inefficient against attacks as the computing capacity of computers increases.

That is, in current solutions an authentic digital signature proves that the signer *possessed* the proper secret key, however it cannot be verified whether really the rightful owner of the key used it, or someone else.

The basic idea of our proposed method is to store the secret key *encoded* in a way that it can only be restored using some information extracted from the fingerprint of its owner, and only after its successful restoration can it be used for creating signatures. This way it is much harder to abuse the stolen signing device, that is, the encrypted key, since the creation of the signature requires the owner's fingerprint – besides the currently used PIN code. It is important to notice that this algorithm does not influence the usage of the public key; therefore it remains fully *compatible with the recommendations of PKI and the current applications*.

The knowledge centre of the consortium has already been making scientific investigations of the above algorithm for years. The theoretical results made it worthy to start investigations of practical feasibility issues depending on the basic research and the experiences of a recognized member of this industry.

The technology centre provides the conditions of feasibility and assures the exploitation of the project results. This centre is a recognized company in the Hungarian market of fingerprint-based user authentication. Their experiences and product scale covers both the hardware and software aspects of fingerprint recognition. The proposed method would firmly extend the scope of their services.

Based on the basic research results of the knowledge centre and the experiences of the technology centre we plan to develop a prototype application until the end of the 20-month-long project, which could be transformed into a marketable product with little effort. We would also create a freely available version of this product, which can enable people to become familiar with the security and comfort of this novel technology. Our scientific results would be published in the form of professional conference talks.