# Digital Signatures with Signer's Biometric Authentication

**Péter Orvos**

The two aims of digital signatures are to preserve the integrity of the signed document and to ensure the receiving party about the identity of the signing party. The currently used technologies authenticate the signer by proving that the signature was generated using the proper secret key, therefore it identifies the signing person assuming that the secret key can only be possessed by its legal owner.

Unfortunately in real life circumstances this assumption may not stand as the secret key may be stolen from or swindled out of the unqualified user. For this reason several efforts have been taken in order to enforce the relationship between the secret key and its owner: the user of the key is usually identified by a password or a PIN (Personal Identification Number). However, another authentication scheme may be able to strengthen further more this relationship using biometric user authentication techniques.

**Biometric User Authentication.** In systems using biometric user authentication some physical properties of the user is measured and verified being compared to certain biometric profiles, which were previously created from authentic samples of the appropriate users. This way of user authentication is ideal as it verifies the user himself/herself, however there are also some disadvantages that must be counted with.

Acquiring biometric information requires certain measurements, and because of the nature of measurement techniques the results will contain certain errors that the authentication algorithm must model and eliminate introducing the possibility of false decisions, of which the possibility must be minimized. Another problem originates from the fact that certain biometric information, such as a fingerprint image is handled as classified personal data in several countries, therefore it must be handled accordingly.

**Integration of Biometric Authentication and Digital Signatures.** Current smart-card based implementations store the secret key and the biometric profile of the owner in the card´s inaccessible memory, and perform biometric authentication each time before creating a signature. Card manufacturers claim that the stored information is inaccessible using current technology, however it might be more secure to store the secret key encoded; that is, it cannot be used even if the memory contents can somehow be retrieved.

The elementary target of my algorithm is to calculate a binary personal identification vector from the retrieved fingerprint image and the biometric profile, what can later be used for encoding or decoding the secret key. In order to result the same vector every time a signature is to be created an error correction method must be applied, of which the correction capability must be carefully adjusted, since correcting too much errors may lead the system to accept fingerprints of unauthorized people.

Two, essentially different algorithms are the subjects of my research, both of which will be introduced in my lecture. One is based on the relative positions of minutiae points [1][2], which are characteristic points of fingerprints situated where ridges end or branch. Another examined approach is based on the calculation of FingerCodes [3] using graphical filters and calculating divergence of certain image regions.

## References

[1] Éva Nikodémusz-Székely, Dr. Vladimir Székely, "Image recognition problems of fingerprint identification", Microprocessors and Microsystems, Vol 17, No 4, 1993, page 215-218.

[2] M. Kawagoe, A. Tojo, "Finger pattern Classification", Pattern Recognition, Vol. 17, No 3, 1984, page 295-303.

[3] Anil K. Jain, "FingerCode: A Filterbank for Fingerprint Representation and Matching", MSU-CPS-98-36, 1998.