René Baltus, Auf den Steinen 7, 53125 Bonn. +49 170 7766 480, +49 228 257125, www.hesy.de 09.05.2002

Your own signature – more than just biometry!

In these times when there are numerous discussions of the advantages and disadvantages of biometric procedures, the question of using one's own signature always crops up at the same time as conventional biometric procedures are mentioned. This is a huge over-generalization, which is hardly appropriate for the refined procedures involving signatures. This is also easy to prove:

- Nobody gives out his or her own signature unintentionally.
- You cannot pass it on to somebody else. Nor can you lose it.
- The dynamics of your writing cannot be "sniffed out" or stolen.
- The signature at the end of a document is beyond any doubt a clear and explicit statement of intent.
- Given a forensically correct reading of the dynamics of your writing, a signature cannot be forged.[1]
- The system automatically detects whether the signatory is alive.
- A comparison or recognition is only done immediately as required or as wished.[2]
- A signature is the sole biometric characteristic that can be produced SIMULTANEOUSLY on paper AND electronically. The latter becomes an "electronic blueprint", which can likewise be verified by a handwriting expert – offline. The writing pressures are IDENTICAL on paper AND in the electronic blueprint.[3]
- The citizen / customer / user has a valid piece of evidence that can be presented in a court of law. "His" (or her) piece of paper that can be filed – as before. He can see what he has signed – and that is all that matters! On the other hand, the various forms of administration are given a procedure that saves on archiving costs, one that generates a genuine work flow that is not broken by different types of media.[4]
- Thus it is also possible to record and store documents in digital and paperless form from the 50% of the population that does NOT WANT or is NOT ABLE to use an electronic seal as per SiG. This immediately renders obsolete the whole matter of "digital underdogs" or "digital have nots".
- A PIN or a password written by hand can be noted and changed as often as wished.
- The field for handwriting input also allows a PIN to be entered. As before, with recognition of the number that was input– with recognition of the number AND of the typing dynamics of the person making the entry.[5]
- This then becomes a system that can be used in several different ways, which greatly improves the rates of recognition and rejection.[6]
- The following are available for stringent security requirements, and either together or in any desired combination as required: possession (chip card), knowledge (conventional PIN), biometry 1 (the dynamics of typing the PIN), biometry 2 (the dynamics of writing the PIN or password), or biometry 3 (the dynamics of writing a signature).[7]
- The amount of data required is so small that it can easily fit on a chip card.[8]
- In its capacity as a biometric random number generator, it derives a biometric random number from the writing dynamics at the same time that the writing is entered.[9]
- The user can also use the pad as a substitute for a mouse for cursor control – and this always functions, even in the event of high temperatures or high levels of relative humidity.[10]

---

[1] A signature can be imitated and a facsimile of it produced, but it can NEVER be forged. The BKA [Bundeskriminalamt = Federal Criminal Police Office] says so. HESY records 1600 pressure values per second; and in addition the writing time and pauses in writing. See the expert opinions in www.hesy.de, and the presentation to the EDP Gerichtstag 1999, and from there the excerpts from the book "Forensic handwriting recognition" by Dr. M. Hecker.

[2] Who would be recognized by a package acceptance on-line? Nobody! An off-line-verification by a handwriting expert would only follow of the acceptance was questioned – as if he can tell anyway from a signature produced there! The BKA rejects this. What is missing is the pressure of the pen on the paper, or in other words, the writing dynamics recorded with large amounts of data.

[3] None of the participants can retrospectively change the documents in his possession. And certainly not if TWO signatures were made; those of the member of the public and the official, or of the customer and the salesman respectively.

[4] In which documents that were given a digital seal as per SiG will also be stored later. ONE digital archive can thus handle ALL future tasks.

[5] For that reason it was called the "analog keyboard".

[6] A so-called "multi-mode system". Nonetheless, it is questionable whether 100 % of the population could be recognized. According to Gauß, not so in practical terms. With HESY it would be around 95 % - the only people missing are those who cannot write AND who cannot enter a PIN or who simply want to have nothing whatsoever to do with computers. The remaining ones will have no need anyway!

[7] "Possession and knowledge" or "possession and one or more biometric characteristics" suffice for digital seals as per SiG. With a signature as well, electronic seals then become genuine digital signatures or electronic signatures.

[8] 1 kb should be adequate, but there are chips that can store up to 32 kb of data.

[9] Indispensable for electronic seals as per SiG. See with reference to this the illustration of writing dynamics in the HESY expert statement in www.hesy.de, on page 12. Since each signature is unique, with differences in the writing pressure and time sequences, it is possible to resort to a different sequence of pressure and non-pressure by means of a coordinates grid. This can be represented as a sequence of 1's and 0's.

[10] The cursor will be faster or slower, in the same way as the pressure on the pad – as we are accustomed to from many other things.