MobiComBiom

Mobile Communication Biometrics

Development of mobile technology: mobile all-rounders as our daily companions

Mobile technology has advanced quickly and created all-rounder which accompany and support us in our day-to-day life. They yield many possibilities of applications, but are also associated with high risks. Who can guarantee that the user of a handheld is actually allowed to use all the mobile services?

MobiComBiom, the Swiss solution from BIOMETRY.com AG

To solve this security problem, BIOMETRY.com AG has developed the product **MobiComBiom** (Mobile Communication Biometrics. This guarantees unique user authentication by requesting **four authentication processes** – biometric face recognition, biometric voice recognition, recognition of biometric lip movement, and word recognition – simultaneously with randomly generated numerals (random challenge response or otp – one-time password).

By pressing a specific “soft button” on the cell phone (e.g., numerals 1 and 3 are pressed simultaneously), the **MobiComBiom** authentication process is started. With it, four randomly selected numerals appear successively on the cell phone display. Similar to video telephony, the user speaks these numerals. The video and audio data is then securely transmitted to the provider (so-called trust center), where every numeral is converted into files (so-called templates, c. 4 KB). These are compared to the reference data that was previously learned by the user for the numerals 0,1,2, to 9. If the data matches, the user of the cell phone is uniquely authenticated.

Mobile payment: high security thanks to MobiComBiom & Trust Level

With mobile payment, the process is exactly the same as described above. A positive authentication includes the user as confirmation of a 2D barcode on his mobile telephone that he uses for payment at the point of sale (e.g., shops).

After authentication, the barcode receives a 100% trust level for a period of 10 minutes. The maximum amount authorized by the bank institute (e.g., CHF 5000) can then be paid. After that, the percentage rate successively lapses to percentage and payment amounts of lesser value (e.g., CHF 500)

in order to allow for the chronologically increasing risk of theft. However, a

trust level of at least 10% (e.g., CHF 50) is guaranteed in order to always be able to guarantee micro payments, e.g.,

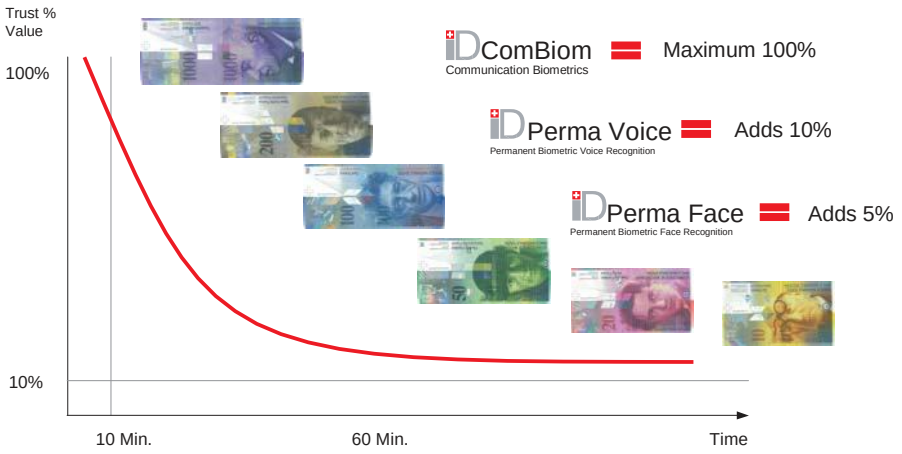
for parking fees. With every telephone call, the voice is

biometrically authenticated and the trust level is increased with a match. However, the increase in trust level is limited to 10% per telephone call. The maximum trust level of 50%

cannot be exceeded in this way.

This is because a replay attack on an individual biometric could be carried out by clever hackers. However, this danger does not exist for the multimodal, simultaneous, biometric authentication to random challenge response contained in MobiComBiom.

If the user finds himself in a noisy setting, the possibility also exists of the user increasing the trust level solely through biometric face recognition. If the user wants to use the maximum sum, he must simply authenticate himself briefly, i.e., he must invoke MobiComBiom and verbally repeat the four numerals. Mobi-



ComBiom is a very secure process on one hand (with 4 nume-rals and 4 verifications = 16 simul- taneous authentication processes) and very user-friendly on the other hand. The “plausibility check” is another additional security feature. Since all authentication processes are routed via the server, they are checked there as to whether the geographic whereabouts of the user or his/her usual habits fit the newly registered authentication request. If, for instance, an imposter has broken into the user’s home with a “fake face” but the authorized user is sitting in the office and rightfully authenticated, the fraudulent attempt will be recognized on account of the irregularity. The system is then locked, all interfaces are notified and the 4 numbers for the16 processes associated with the rightful user will be required to unlock the system again. Also, embedded gait is foreseen. Should someone steal the smartphone, it would be recognized by the different style of walking and it could be programmed to immediatly stop specific actions. Online authentication as described above would then be needed. Last not least, BIOMETRY is working on Multi – Facial Authentication. When we receive a call, we look who is calling, thereby the biometric face is verified, then the smartphone is moved to the ear, where the ear lobe is used for biometric verification.

BIOMETRY.com AG in short

Biometry.com AG is a high-tech security company head-quartered in Switzerland that offers secure and easily usable biometric authentications. A multimodal product as well as the individual application of certain modes results in an all-in-one software. This enables the most varied applications to protect the personal identity of people and their property. The algorithms used are known worldwide which ensures absolute Security and Comfort.

BIOMETRIC AUTHENTICATI ON FOR A SECURE WORLD!

BIOMETRY

SWISS IDENTITY SECURITY SYSTEMS

swiss identity security systems

Headquarter
BIOMETRY.com AG
Chilcherlistrasse 1
CH–6055 Alpnach OW
Switzerland
Tel.: +41416703272
www.BIOMETRY.com

BIOMETRY Estonia
Akadeemia tee 19
12618 Tallinn
Estonia
Tel: +37 (0) 25 241 819

BIOMETRY United Kingdom
Rowood House, Murdock Road
BICESTER, OX26 4PP
United Kingdom