Secure Mobile Payment thanks to a very safe, comfortable, and fake-resistant biometric authentication

Werner Blessing

BIOMETRY
Chilcherlistrasse 1
CH - 6055 Alpnach, Schwitzerland
werner.blessing@BIOMETRY.com

Abstract: This unique solution will ensure that only the authorized person has access to the respective mobile applications, unauthorized access will be denied. It is very safe and very easy to use.

Mobile Communication Biometrics - how it works and where it can be used

By pressing a specific soft button or icon on the mobile phone, four randomly selected numerals appear successively on the mobile phone display. The user speaks these numerals into front camera and microphone. The video and audio data are then securely transmitted to the provider (the so-called "Trust Center") where every numeral is verified with biometric face, -voice (speaker), -speech recognition and lip movement. All is verified simultaneously and hereby none fake able. Since the requested numerals are Random Challenge Response (OTP – One-Time Password), this will protect the mobile phone from replay attacks and spoofing attacks. If the data matches, the user of the cell phone is uniquely authenticated with the fusion of four biometric procedures for each number that is asked, which results in 16 fused authentication procedures.

This very high level of authentication will resolve in a trust level of 100%, enabling the user to pay the maximum amount which his bank has agreed with him or to open doors with the highest level of security. Since there is the risk of theft and fraudulous use, the trust level would drop very rapidly over the first quarter of hour reducing this risk enormously. The lower the remaining level of trust is, the less it`s reduction will be, levering out at 10% remaining trust level, thereby allowing micro payments. For each phone call that the user does, his voice would have a biometric verification and recognized as the proper user this would raise the trust level. Should the user be in a noisy environment he could trigger of biometric face verification by using specific icon for that. This individual biometric verification could raise the level of trust only to a specific height.

By displaying the remaining level of trust on the screen of the mobile phone the user would always know by this percentage of trust level how much money he can pay or which door he can open. Speaking four numbers into the mobile phone in the morning and using the phone only normally with phone calls and voice verifications or SMS and face verification the whole procedure becomes very comfortable for the user. The communication towards the payment equipment or doors could be done optically with a 2D barcode or later on with NFC (near field communication). Since our mobile and fixed hardware is more and more connected to the cloud, one could imagine that this authentication procedure could run on all sorts of various hardware, even with different processes of authentication. Highest security, of course, is obtained with “ComBiom”, the four numbers, i.e. the 16 fused processes, voice only face only or even simple Pin could be used for low level security. Since the trust center would know the sequence of various authentication procedures happening during the day, a plausibility check could be easily done at the trust center verifying geographic plausibility or behavioral plausibility i.e. weekday or holidays etc.

In summary this procedure obtains a very high level of security and yet is a very comfortable process, such as the user simply uses his mobile phone as he would have done in old days.