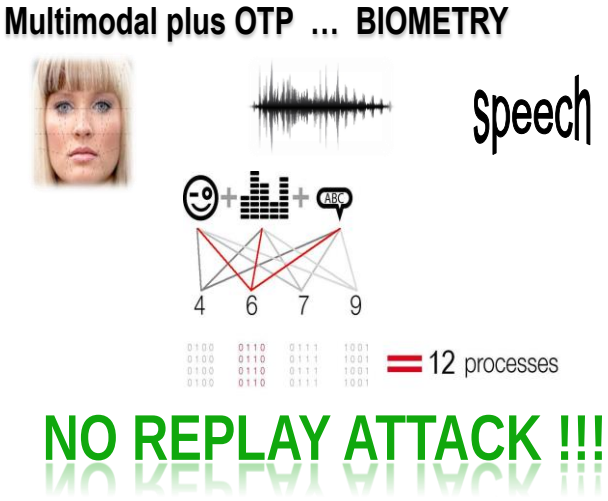
BIOMETRY: Whitepaper on Mobile Biometrics, Safe & Easy

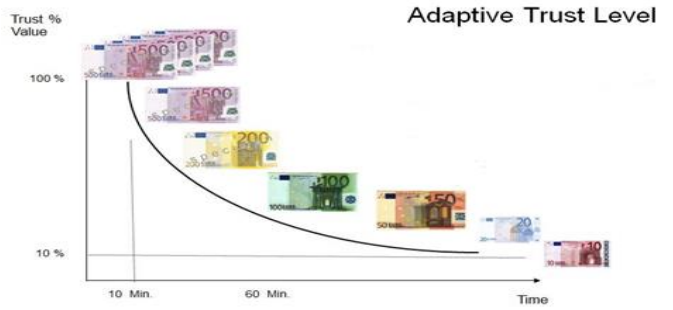
For strong safety the user will get four randomized and subsequent numbers or words displayed on the screen and would speak them. Each number is verifying simultaneously his biometric face, voice and speech. The results of the twelve biometric procedures are fused, to allow one and very safe authentication. Fraudulent imposters cannot fake three biometrics and twelve processes, recorded simultaneously on front part of smartphone. Random Challenge Response renders spoofing and replay attacks impossible. No specific Hardware is needed. Even older smartphones are good, allowing a fast and easy market entry.



Easy handling is achieved by verifying the user's voice on each phone call and verifying his face whenever he does an SMS or e-Mail on his smartphone. Public phone habits need not to be changed, biometrics are taken "on the fly" and totally effortless, resulting in a high consumer acceptance. We also registered a patent on a biometric procedure fusing up to four features for a normal answer to an incoming mobile call. When the phone rings and the user looks who is calling, we do biometric face verification. When the user moves the phone to speak, the camera will capture his face profile and the ear conch, both biometric features that we verify. Last not least the voice is verified. All steps are redundant, so all remains smart and fast. The more of the four features we verify positively, the stronger and safer is the authentication.

Easiest availability with ATL "Adaptive Trust Level": BIOMETRY separates the moment of authentication from the time of using it and manages the level of trust in an embedded App. The icon "ID" on the top line (see red arrow, left) indicates the trust on the mobile. A simple click shows % and QR-code for use and communication to interfaces. Voice only or face only authentication carries the risk of replay attacks and weak security. Therefore the level of trust should be increased by 10% only, on positive voice during a phone call and face for SMS. Individual biometrics can be staged but not bypass 35% trust level. To reach highest trust, the process with the four numbers and the twelve processes are used, see strong safety above.

The higher the trust the faster it drops away, for security reasons. The lower the trust, the slower it drops, see image next. 10% minimum trust is always retained allowing instant action for Micro-Payment or unsafe doors etc.



Mobile payment, mobile Apps: Payment can simply be linked to the percentage of trust, see image above. 10% could be for 100 CHF, 20% for 200 CHF etc. This allows most of our daily payments without executing any cumbersome process of authentication. It is achieved by simple and regular use of the phone. Only for high amounts the user is requested to reach strong security and would start the process of speaking the four randomized numbers see above. The same method applies to the different security levels of doors which could be opened via the mobile phone. Also the various apps on the mobile phone. One can even set mobile phoning to 10% trust level, mobile contacts to 20% and usage of mobile e-Mail to 30%, securing the use of the smartphone itself.

Mobile Banking would request the strongest security and need the application of the four numbers and fused twelve processes, equalizing 100% trust. For **Transaction Confirmation** we take the checksum of the amount and recipient IBAN, resulting in two pairs of numbers, which would be asked in the same way, fusing again the 12 biometric processes. Should the Man in the Middle modify the IBAN, our biometric check No's wouldn't fit to the content of transaction. The banking server would immediately see the fraud attack and the client can be notified. For the user it is a simple four numbers to open e-Banking and to close it.

Additional Security: Since all authentication processes are routed via the cloud based authentication server we check the geographical location of the user and his usual habits of the newly registered authentication request. If it does not match, the other interfaces are informed of the misuse and the rightful user can call the police after a strong authentication.

The hardware needed for BIOMETRY is a microphone and front camera which is already incorporated in most smart phones today. Our software solution does work immediately on existing phones in the market.

BIOMETRY outperforms the solutions of Google 4.0 and 4.1 and also Apple's solution developed by Authentec. The future user will no longer carry a wallet or a key. Currently we are in negotiation with several International companies and also with the Ministry of Internal Affairs in Estonia (pilot for mobile state security). To protect BIOMETRY technology several new patents have been registered.

BIOMETRY has achieved a significant level of publicity. The magazine "Global Identification" has published a study regarding the **Top 50 mobile authentication suppliers**. We are also listed amongst world's 64 biometric companies (see BIOMETRY.com/News).

06.07.2013, Werner Blessing

+ 41 79 434 4535 Mob
w.blessing@biometry.com
www.BIOMETRY.com

BIOMETRY
SWISS IDENTITY SECURITY SYSTEMS