CORE®

USE OF BIOMETRICS IN BANKING

Dr. Waldemar Grudzien

27. June 2016

COREtechmonitor | Blogpost

Key Facts

- Biometrics has achieved market-readiness: Both Apple and Samsung have opened up to the possibility of using biometrics in German banking
- The supervisory bodies for banking see biometrics as offering the same level of security as PINs, passwords, and chip cards. This makes the attribute of "being" (unique physical characteristics) equal to possessing (e.g. a bank card with chip), and knowing (e.g. a PIN).
- Biometrics fulfills all data protection requirements because modern biometric processes do not require any centralized storage of unique physical characteristics.
- Biometric identifiers can now be canceled and replaced, just like PINs and passwords.
- Modern biometrics processes currently enable the use of single-use passwords, i.e. they offer the characteristics of a one-time pad and can be used as single-use transaction numbers (TANs) to authorize an individual transaction.
- The formation of single-use passwords via biometrics represents a quantum leap forward: Biometrics now enables the use of the few unique physical characteristics (such as ten fingers, two eyes and one face) in order to safeguard countless instances of personal identification and transactions.

Report

Biometrics is the analysis and metrics of living creatures and their characteristics. The aim of biometrics is for the automatized metrics of a person's individual physiological or unique behavioral characteristic, for the purpose of identification or verification, to be distinguishable from other people.

The physiological (passive) and behavioral (active) characteristics of a person must exhibit the following properties for widespread biometric use:

- Universality (present in all individuals)
- Uniqueness (different in all individuals)
- Permanence (not changing over time)
- Measurability (can be quantitatively measured via a technical system)

In terms of banking, these requirements are reduced to universality, uniqueness and measurability in terms of the customer base, as well as permanence equal to the expiry of a card – bank cards are exchanged after four to five years.

Current biometric characteristics that can be used effectively include:

- Physiological (passive)
  - Fingertip (minutiae)
  - Hand (geometry)
  - Eye (iris)
  - Face (2D, 3D)
  - Finger (vein imaging)
  - Palm (vein imaging)
  - Back of the hand (vein imaging)
  - Gait (acceleration)
- Behavioral (active)
  - Signature (writing speed)
  - Handwriting (writing semantics)

- Typing behavior (sequence, type speed)
- Voice (timbre, frequency)

The passive characteristics (i.e. those not influenced by behavior) are often openly recognizable – with the exception of the vein imaging – i.e. they can be seen from the outside and are thus more susceptible to unauthorized use. Associated with this is the possibility of metrics being recorded unnoticed for the unauthorized purposes of monitoring movement and identity theft. The best-known example of this concerns the fingerprints of Dr. Wolfgang Schäuble, which were analyzed and made public when he was the German Federal Minister of the Interior.

While PINs and passwords can be forgotten and, like chip cards, can also be passed on to third parties, an individual always has his or her biometric characteristics "to hand" – they are impossible to forget or to pass on unwittingly to a third party. In the instance of a PIN, it is impossible to check whether the user entering the correct PIN is actually its rightful holder. While authentication via PIN entry is either bit-perfect or not, all biometric processes have to have the result of the analysis contrasted with a reference value in a fuzzy comparison because it cannot reconcile a live-recorded – living – characteristic with the reference pattern saved with 100% bit-perfection.

The decisive factor in a biometric process is the protection of the biometric reference data (template protection). Of course, the biometric templates could be protected via "classic" cryptography, i.e. encrypted. Provided the encryption key remains secret, the template is safe. With each use of the template, it has to be decrypted, which then increases the vulnerability of the data available in plain text. Overall, classic encryption offers a feasible, yet inconvenient, solution because the encrypted data and the key have to be stored in a secure environment.

Another, better option would be the use of a pseudonymous identifier (PI). A PI is the derivation of a pseudonym from the user's biometric data as biometric hashing. Instead of the body's biometric template, only the PI of this data is used. A PI is a hash that reflects the unique features of the biometric characteristics. It builds on the biometric data and comprises a tolerance range that does not automatically lead to a different hash whenever there is a change in the biometric data measured (e.g. eyes blinking) but that remains unchanged within limits. A classic encrypted hashing process cannot be used for biometric data because classic hashing is very sensitive to changes in the input data – which is why hashing was invented in the first place. In biometric use, for example to secure banking transactions, biometric information with a certain degree of variation has to result in the same biometric hashes, otherwise an authorized customer might not be able to authorize various banking transactions with the same biometric characteristics – which are always subject to slight changes – and the inevitable errors involved in measuring them. However, the PI can solve this problem.

Until now, fuzzy processes have generally been used for PIs; however, their mathematical characteristics require us to choose between conformity with data privacy policy or higher accuracy in terms of recognition. Ac cording to the latest research, PIs based on Bloom filters offer both high compliance with data privacy policy and also high accuracy in recognizing biometric data.

In general, pseudonymous identifiers based on Bloom filters can be said to have the following characteristics:

- Privacy: The references saved as PIs can be compared without the need for decryption.
- Unlinkability: PIs relating to the same person can be created for various applications without the person being traceable in the various applications' databases (cross-referencing not possible).
- Non-invertibility: The PI cannot be extrapolated to the original biometric reference data, and therefore not to the person either.
- Renewability: The reference data can be recalled and replaced.
- Illustration of biometric variation: The variability of physical characteristics is integrated into the PI.

PIs fulfill all data protection requirements thanks to the characteristics of "Privacy," "Unlinkability," and "Non-invertibility" because the person's biometric reference data cannot be extrapolated from the system. This means that PIs could even be stored on central servers without this biometric use contravening data protection requirements. Thanks to the characteristics of "Renewability" and "Illustration of biometric variation," the limited number of unique physical characteristics available to us (such as ten fingers) can be reused countless times for authentication or authorization. One customer can therefore use his or her few unique physical characteristics countless times for authentication purposes, for example to log in to a banking platform, and also to authorize countless transactions – for example, approving wire transfers via online banking. The use of the limited number of physical characteristics is also not constrained by the fact that they can be obtained without the user's consent (e.g. if the fingerprints are copied from a glass) because they can be canceled. This means that biometrics using PIs based on the use of Bloom filters exhibit the cryptographic characteristics of a one-time pad, i.e. it is now possible to integrate unique physical characteristics as an ever-changing factor as often as desired in order to authorize banking transactions featuring an IBAN and sum, for example.

What is also very important in day-to-day practice is the system security of biometric sensors, which is expressed in live tests. These check whether a living person wants to trigger authentication or whether the sensor is to be presented with an artifact relating to this person (e.g. photo of their face, iris, rubber finger, etc.) One restriction here is that there are not yet sufficiently reliable live tests available for all features, although they are available for fingerprints, irises, veins and faces (3D).

Biometrics has been acceptable at least since the launch of touch ID by Samsung in the summer of 2014 and by Apple in October 2014. Prior to its launch into the market, the level of interest in biometrics for retail banking among German banks was at best a simple 'wait and see'. This attitude appears to be changing slowly within a small number of banks: As part of the digitalization process,

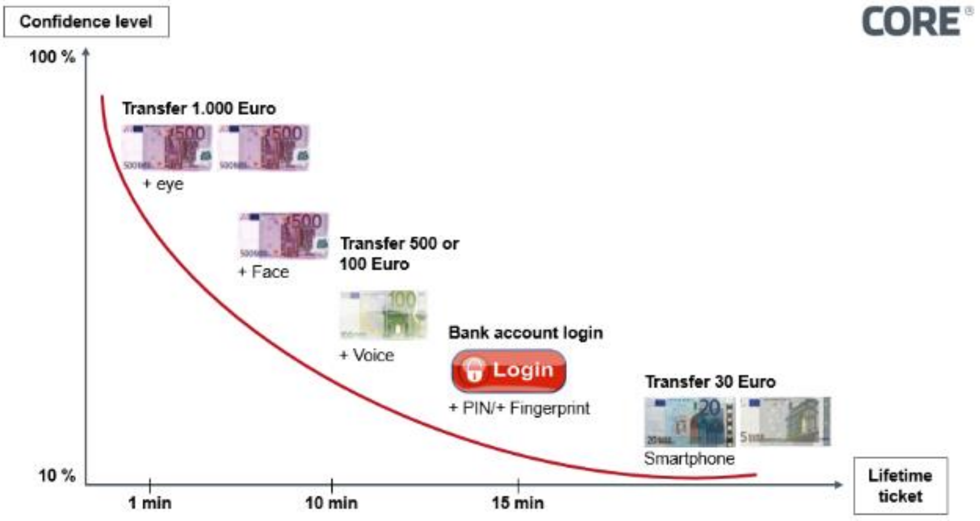

Figure 1: Risk-based securing of transactions via multi-modal biometrics

the opening up of the markets by PSD2 and the entry of global ecosystems from the non-banking field, the convenience of an app for the customer is becoming ever more significant. In addition, biometrics can not only keep pace with the security offered by conventional procedures such as a PIN and bank card (and sometimes surpass it), it can also keep up in terms of supervisory legislation because biometrics (the state of being) is equal to ownership and knowledge under banking supervisory law: According to MaSI [legislation on minimum security requirements for Internet payments], strong customer authentication is a process based on the use of two or more of the following elements, which can be categorized as knowledge, ownership or inherent properties: i) something the user knows, e.g. a static password, code, PIN, ii) something that only the owner possesses, e.g. a token, smartcard, cell phone, iii) a characteristic of the user, e.g. a biometric characteristic such as a fingerprint.

With biometrics, risk-based use is even possible, i.e. riskier transactions can be subject to stricter authentication requirements than lower-risk transactions. In addition, transactions can be secured in a multi-modal way. To do this, several different physical features are used at the same time rather than just one single feature, as is currently the case in the fingerprint system used in banking. For example, depending on the transaction amount, a time-limited ticket can be issued and not just for one, but up to four different biometric modalities can be requested for authorization.

In summary, we can say that biometrics can guarantee all of the advantages that customers expect of banking services in the digitalized world, in realtion to both convenience and security. This is shown by:

- Higher security than PINs
- Considerably increased convenience as an established banking process, and
- Ease of integration into app-based and in-app architectures

The first banks in Europe have recognized the advantages of biometrics and are championing their use in order to defend market shares or to build on them in competition with larger organizations, which will keep well-established structural security architectures in production for longer.

Sources

C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, J. Fierrez: “Towards Cancelable Multi-Biometrics based on Adaptive Bloom Filters: A Case Study on Feature Level Fusion of Face and Iris”, in Proceedings of the 3rd International Workshop on Biometrics and Forensics 2015 (IWBF 2015), March 3–4, 2015, Gjøvik, Norway, (2015).

J. Breebaart, C. Busch, J. Grave, E. Kindt: “A Reference Architecture for Biometric Template Protection based on Pseudo Identities”, in Proceedings BIOSIG2008, pages 25–37, GI-LNI, (2008).

N. Buchmann, C. Rathgeb, H. Baier, C. Busch: Towards electronic identification and trusted services for biometric authenticated transactions in the Single Euro Payments Area, in Proceedings of the 2nd Annual Privacy Forum (APF’14), 2014.

Dr. Waldemar Grudzien is Transformation Engineer at CORE and focused on the security regulations of the financial industry and their technological effects on IT infrastructures. During his work at a national federation of the financial industries he was a specialist for retail banking and banking technologies. He graduated in electricial engineering at the TU Berlin and publishes about security policies, IT technologies and IT transformation of banks.

Mail: waldemar.grudzien@coretransform.com

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany

www.coreinstitute.org

Phone: +49 30 16344 020

office@coreinstitute.org

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany

www.coretransform.de

Phone: +49 30 26344 020

office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia

www.coretransform.ch

Phone: +41 442 610 143

office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain

www.coretransform.co.uk

Phone: +44 203 319 0356

office@coretransform.co.uk