European Association for Biometrics

eab

Human Identity in Europe

‘A hype that’s there to stay’

Report Biometrics in Banking and Payments 2017

A report from the seminars Biometrics in Banking and Payments organized by the European Association for Biometrics in London and Amsterdam in 2017

‘A hype that’s there to stay’

Report from the seminars ‘Biometrics in Banking and Payments 2017’

At least, that is the general opinion of those who participated at the seminars **Biometrics in Banking and Payments 2017**, that took place in London (17 November) and Amsterdam (7 December). Below follows an overview of the topics and observations that were presented during the two seminars.

To hype or not to hype

Once landed into hype mode, it is sometimes difficult to oversee when it ends, if at all. However, during the past few years the development of biometric identification and authentication platforms is quickly proliferating, which indicates that this hype won’t come to an end soon. A strong signal is that those who are once used to biometrics generally don’t want to turn back to the old password or PIN-code again. This, and various other positive outcomes were presented by **Michael Sass** from Mastercard, which has done extensive studying and piloting of biometrics worldwide over the past 5 years. According to SmartMetrics in 2016, 80% is concerned about ID fraud, 67% is eager to use biometrics. Own research by Mastercard showed 90% who used Mastercard’s app Identity Check Mobile would definitely like to replace their password with biometrics. A Visa study confirms: two-thirds of consumers want to use biometrics when making payments. 50% think payments will be faster and easier with biometrics. Fingerprint recognition is the most popular form of biometric. So it seems that we are moving from hype to trend.

The above is supported by the fact that many major banks are integrating biometrics into their multi factor authentication platforms, all be it just as a second factor. Adding convenience while increasing security seems to be the overall driver. **Jacoba Sieders**, Head Identity and Access Management at ABN AMRO and also the kind host of the seminar in Amsterdam, also demonstrated during her opening keynote the evolving role of biometrics into the overall chain of client authentication and transaction security.

Deep Learning and Neural Networks

Another important observation is that there is a clear movement of biometrics moving from a gadget driven point solution towards an element that is part of a broad authentication ecosystem. **Halleh Khoshvenis**, Research Engineer at BioTrust, impressed with her presentation about Deep Learning and Neural Networks, which enables a holistic and real time authentication of transactions and users, having biometrics as an integral part of the overall risk assessment. It seems a prelude to a paradigm shift in the way the risks of using biometrics are being assessed and mitigated, drifting away from the classical models that we are familiar with. In this context however, we should mention a remark from **Richard Tomsett**, Software Enabler Emerging Technology at IBM, that in Deep Learning a computer ‘never says no’. He wanted to remind us that the conclusion of a Deep Learning process may result

into an outcome that doesn't make sense at all to human beings. It won't say, for example, that a certain object doesn't exist based on the given input. That means that measures are needed to validate the outcome of a Deep Learning process. On the other hand, deep learning processes usually gain accuracy the longer they have been learning. So some prior investment is needed before the full potential and usability of a Deep Learning system will be achieved.

Digital on-boarding

A remaining challenge is the digital onboarding of new clients. With branches being closed down, physical interaction (in principle needed for a reliable identity and background check of new customers) is being reduced to the point that a bank should rely on client onboarding without ever actually have seen this client face-to-face. Although it seems not to be an easy job to solve this**, Jasper Fortuijn** from ING Bank and **Maarten Wegdam** from Innovalor demonstrated a digital onboarding solution based on the machine readable passport and the smartphone. The app called Read-ID scans the MRZ of the passport and reads the facial image from the passport chip. Then the smartphone takes an image of the person and a selfie check is done against the reference from the passport. This creates the face as a highly reliable credential for confirming the identity of a person who remotely enrolls into the banks' system.

State of the art

Off course the seminar wouldn't complete if there weren't some demonstrations of state of the art biometric technologies. **Iain Swaine** from BioCatch presented about the cutting edge in behavior recognition, while **Peter de Gier** from Lucom showed the high applicability of dynamic signature for real time authentication and identification. **Eric Gilmore** from the Irish company DAON illustrated how biometric authentication can be designed to be compliant to PSD2. **Hemant Mardia**, CEO of IDEX Norway, presented the latest developments on biometric cards.

Presentation attack detection

An important topic is the detection of spoofing attempts to biometric sensors, also called Presentation Attack Detection (PAD). In short that means the potential of using an artifact to mislead the biometric sensor to force a successful false acceptance. **Roney Castro** from UL explained how spoof resistance can be tested. At the UL testing laboratories they have gathered all thinkable technologies and materials that can be used to make artifacts that can potentially spoof the sensor. These can be used to test any presentation attack detection mechanism that a biometric sensor may have. Although there is a standard in the working (ISO/IEC 30107-3:2017), it will remain a case by case effort to measure a sensor's vulnerability against presentation attacks, as the kind and impact of the associated risks partly depend on the overall context of a specific application. However, the new ISO standard will certainly help in standardizing the process of performing those PAD tests.

Biometric cards: the 3rd revival?

In our recent history it has been said at various occasions that the times for the smartcard are over. The first time was some 15 years ago, when biometrics became mainstream and expectations were almost limitedness. The story was that there was no need for a token anymore, just biometrics would

do the trick. Now we know biometrics is more suitable for being a 2nd factor for authentication, which doesn't wipe out the smart card at all. The second time was more recently, when the smartphone was used for 3rd party authentication purposes, increasingly using biometrics (e.g. iTouch). Today the biometric smartcard seems to have entered a new era of usability: seamless and low cost integration of a thin-film bendable fingerprint sensor makes the biometric card attractive for mass production. In addition, the new generation of fingerprint sensors and processors take so little power, that it only the power coming from the card reader is used, even contactless ones. So no extra batteries are needed anymore to lengthen the otherwise shortened life-cycle of the cards. In addition, **Hemant Mardia**, CEO of IDEX (Norway), explained a new remote fingerprint enrollment method, that doesn't require a person to be physical present at a bank or credit card branch anymore. Research by Mastercard revealed that biometric cards significantly improve the user's convenience, as a pincode was not needed anymore. During the discussion opinions were mixed regarding the business potential of this new generation of smartcards. Although more secure than a smartphone, there were doubts if a biometric card could fully beat the flexibility and convenience of the smartphone. However, in certain geographical areas, where (national) identity and payment are converging (e.g. Asia, Middle East, the Africa's), a biometric card may prove its advantage by being cheaper and better to control by the issuer than a smartphone.

Legislation and regulation: fixing the legal holes

With the new EU legislative actions on payment services (PSD2) and data protection/privacy (GDPR) in place one would think that matters concerning the adoption of biometrically enabled payments have finally become clear from a legal perspective. Unfortunately, presentations from the experts **Catherine Jasserand** (University of Groningen), **Paul Anning** (lawyer at Osborne Clarke) and **Johannes de Jong** (Head of Regulatory at Osborne Clarke) unfortunately took a different course. They had the opinion that not only these two main legislative tools were occasionally conflicting, they also pointed out that many important terms were poorly defined, including key words like 'biometrics', 'explicit consent', 'data protection by design' and various other terminologies that are frequently used in biometric projects. Reference was made to the international standard on biometrics vocabulary, ISO/IEC 2382-37:2017. It was further concluded that better harmonization between the terminology from the PSD2 and GDPR is needed. Where PSD2 speaks about 'personalized security credentials', the GDPR uses 'personal data'. Both legislative tools are leaving a lot to the interpretation of specific cases. In order to fill any legal gaps of current biometric enabled authentication solutions, a closer alignment between the legislative frameworks will be needed. If not, fragmentation of solutions may impair a more standardized way of efficiently implementing all these biometric solutions into the payment ecosystem.

Max Snijder, December 2017

Appendix

The following banks and financial institutions (total 27) have participated to the seminars: ABN AMRO, ING Netherlands, C. Hoare & Co., Capital One, Commerzbank, Coventry Building Society, Credit Bureau Of Turkey, AK Bank, CYBG plc, Investec Bank, JP Morgan, Lloyds Banking Group, Rabobank, Santander, TSB Bank, UK Finance, Payments UK, Vanquis Bank, Merpay, American Express, Mastercard, Capital

One, Insignia Group of Companies, Volksbank (NL), Dutch Payments Association, Card Complete Service Bank AG, International Card Services.

The seminars were organized by the **European Association for Biometrics**, in cooperation with **Financial Fraud Action UK** (London) and the **Platform Identity Management Netherlands** (Amsterdam).

For inquiries please contact Max Snijder at secretariat@eab.org.