SMART PAYMENT ASSOCIATION

shaping the future of payment technology

Biometrics in Payment

Breaking down barriers with high value payments

May 2018

Table of Contents

1. Introduction

In 2013 Smart Payment Association (SPA) published a paper exploring the case for implementing biometric cardholder verification mechanisms (CVM) for card payment applications. Analyzing the interconnected elements of fraud prevention, greater consumer and issuer protection and the predicted growth in remote banking sessions, the paper set out a framework of guiding principles, specifications and best practices – many of which remain wholly relevant today.

With biometrics now accepted and standardized by EMVCo – a key outcome supported by SPA – this updated paper refreshes the discussion in the context of today's payments landscape. It looks again at the value of adding biometric sensors/functionality to EMV cards – both to enhance payment security and further extend financial services to previously hard-to-serve populations.

2. The evolving market for biometric authentication

Biometric authentication has been a mature technology for over fifteen years – with a host of applications in mainstream use – from allowing access to secure facilities with iris and fingerprint sensors to speeding travelers through border control curtesy of ePassports. On-card biometrics sensors had not, however, been widely used for payment and finance applications until now.

A May 2017 study by Juniper Research[1] predicted nearly 2 billion mobile payments would be authenticated by biometrics by the end of 2017. While these numbers have to be confirmed, there is little doubt we have seen a significant rise in the number of biometrically authenticated payments over the past twelve months.

Biometrics have entered the public consciousness – and been widely accepted. A recent Equifax-commissioned survey[2] found some 56% of consumers in Britain would choose a biometric security method to log onto online banking over the more conventional username and password approaches. Taking a world view, acceptance is stronger still. According to IBM, 67% of respondents are comfortable using biometric authentication today, while 87% say they'll be comfortable with these technologies in the future[3].

The catalyst, of course, has been the now-ubiquitous biometric sensors on today's generation of smartphones. By the end of 2017, 1.9 billion biometrically-enabled smartphones were expected to be in circulation[4]. This figure will grow. According to one estimate[5], 99% of installed smartphones in the US will be equipped with fingerprint scanners by 2021 – although Apple's decision to go with facial recognition on its iPhone X model may cause a market-wide rethink.

[1] https://www.juniperresearch.com/press/press-releases/mobile-biometric-payment-volumes-to-triple-in-2017

[2] http://uk.businessinsider.com/uk-consumers-want-biometrics-in-banking-2017-3

[3] https://www.prnewswire.com/news-releases/ibm-future-of-identity-study-millennials-poised-to-disrupt-authentication-landscape-300589262.html

[4] The Global Biometrics and Mobility Report, http://www.acuity-mi.com/GBMR_Report.php

[5] http://uk.businessinsider.com/uk-consumers-want-biometrics-in-banking-2017-3

This is a route already being taken by Mastercard. In a recent statement[6], the payment giant announced that consumers will have the capability to use biometrics, such as fingerprints or facial recognition, as a way to identify themselves when they shop and pay with Mastercard in April 2019.

One thing is for sure, whether it is fingerprint, vein-scanning, facial recognition or something else, the vast majority of smart devices will undoubtable feature biometrics of one kind or another over the next few years.

What of financial service providers and issuers?

We have already seen strong support from banks for today's leading mobile wallets. Over 4000 issuers worldwide worked with Apple Pay as of October 2017 [7]. Not only that, the schemes – including Mastercard's Check Mobile service – have also leveraged the mobile device to offer quick and convenient identity and payment authentication options. More interestingly for an issuer audience, we are also seeing considerable momentum building for adding biometrics to payment cards.

In January of 2018, Bank of Cyrus announced its intention to roll-out EMV biometric dual interface cards in partnership with Gemalto and VISA. Using fingerprint recognition instead of a PIN code to authenticate the cardholder, the card is compatible with existing payment terminals already installed in the country. Bank of Cyprus' customers will complete a swift enrolment process at the bank's branches, using a specific tablet designed for the solution. The biometric personalization and card activation process is designed to avoid transmission of biometric data over the air to ensure users' data privacy is protected. The fingerprint template captured during the enrolment process is stored only on the card. This is believed to be the world's first EMV biometric dual interface payment card for both chip and contactless payments.

JCB and Idemia have also recently announced a partnership to introduce biometric payment cards in Japan and Mastercard has carried out trials in Bulgaria and South Africa.

In the European sphere, this sensor-on-card approach supports the European Banking Authority's Payment Services Directive 2 (PSD2) requiring multifactor or "strong customer authentication" for electronic payment services – enabling authentication on two or more mutually independent factors defined as knowledge (e.g. password, PIN), ownership (e.g. token, device), or inherence (e.g. biometrics). In addition, the European Card Stakeholder Group (ECSG) is working to ensure biometrics payments under PSD2 are in line with the General Data Protection Regulation (GDPR) / ePrivacy Directive now in force across Europe.

[6] https://newsroom.mastercard.com/eu/press-releases/mastercard-establishes-biometrics-as-the-new-normal-for-safer-online-shopping/

[7] https://techcrunch.com/2017/10/23/apple-pay-now-in-20-markets-nabs-90-of-all-contactless-transactions-where-active/

3. A growing security opportunity

Biometric-enabled payment cards is a market set to grow. ABI Research predicts card shipments will reach 160 million shipments by 2022 with a 5-year CAGR standing at approximately 400%. While the Middle East, Africa and North America will be among the first regions to enjoy higher shipments in 2018, the study forecasts Europe and Asia Pacific will have a larger penetration rate over the coming years.

Here, the opportunity to extend security – while at the same time paving the way for high value contactless payments - is clear. It is exactly this sort of innovation that will enable issuers to tackle the growing ambitions of wallet providers to evolve from simply being a place to store other bank-issued payment instruments, to becoming the payment and storage instrument itself.

4. How biometrics works on a smart payment card

To use a biometric system, individual persons must be enrolled first. During the enrolment stage, the reference biometric is captured, processed, associated with other identity attributes in a biometrics template and finally stored in a card issued to the enrolled person, who becomes the cardholder.

When using a biometric authentication system, a new sample of the cardholder biometrics is captured. A comparison (often referred to as 'matching' or 'verification' depending the sources) between the 'fresh' captured sample and the corresponding enrolled reference is then performed.

5. Off-card matching

The off-card comparison (off-card matching) process takes place in the terminal or back-end system; e-Passports are a good example of off-card matching. Typically, biometric data is captured locally on the device, converted to a biometric template on the device, then the template is encrypted and sent to a connected terminal and/or server for authentication.

In this approach, because the terminal host powerful computing resources with advanced comparison algorithms, the biometrics authentication is faster.

However, as we have seen, off-card matching requires the biometrics reference template to be retrieved from the card. For security reasons the terminal should be authenticated by the card first.

A secure channel must be established between the terminal and the card prior to the transmission of biometric data. The implementation of the off-card comparison process therefore requires a significant investment on the terminal side.

Added to this, there is some concern – both from security and data privacy perspectives– surrounding the creation of cloud-based biometric databases. The financial, reputational and regulatory consequences of the kind of breaches we have recently seen with Experian would be considerably amplified should a central biometric database be compromised.

6. On-card matching (using embedded biometric sensor)

In a match-on-card process (with the card featuring a biometrics sensor), the enrolled biometrics reference data never leaves the card. The captured biometric is processed off-card and then transmitted down to the card encoded as a template for comparison with the biometric reference stored in the chip memory. The card compares both templates using a matcher, a high-performance algorithm. This means that the card must feature enough computational power to perform an accurate comparison calculation in very short transaction times (several hundreds of msec).

Despite this, and some standardization and interoperability challenges, SPA believes this 'sensor-on-card' approach offers a more secure way forward for fingerprint verification implemented in payment cards. Sensor-on-card presents definitive advantages in terms of security and data privacy, a central concern for payment applications. For instance, the fact that the reference never leaves the card means that the attacker has no prior knowledge of the stored biometrics. This way, if an attacker manages to get a legitimate card, he/she has no hints on the particular fingerprint template (spoofing) that if presented to the card would result in a successful comparison.

In terms of performance, different marketed solutions are able to make secure on-card comparisons in less than 500 ms, which is compatible with transaction time requirements. Finally, the adoption of ISO standards for interoperability of sensor-on-card solutions should facilitate a good user experience.

7. Breaking the €30 barrier

With the global contactless payments market expected to reach USD 2.23 trillion (by transaction value) by 2025[8], the competitive pressures to capture market share alone are significant. Biometric-enabled payment cards offer issuers a clear area of advantage – by providing consumers (and merchants) with multiple authentication factors; not just 'something I have', but 'something I am'. Also, and should it be necessary, biometric-enabled EMV cards can provide the 'something I know' with a PIN.

Key to success, today's generation of biometrics sensor-on-card solutions ensure the biometric reference never leaves the card – avoiding the implementation of a central database of biometrics references and so reducing the data protection, privacy and security issues that can arise.

[8] https://www.prnewswire.com/news-releases/the-global-contactless-payments-market-is-expected-to-reach-usd-223-trillion-transaction-value-by-2025-300563167.html

And with assured security comes the ability to address the single issue holding back card-based contactless payment.

While contactless payment offers consumers a fast, secure and convenient way to pay – and provides merchants with significant opportunities to reduce queuing, improve in-store payment experiences, increase brand loyalty and so on – it has always been limited by transaction value.

Typically, around €30, this limit is set to avoid monies being fraudulently spent should the card be lost or stolen, or (more unusually) cloned. Adding a biometric authentication layer, where the user simply presents the card to the reader while keeping their finger on the biometric sensor, removes security concerns without adversely impacting speed and/or convenience. Similarly, the biometric provides an appropriate personal authenticator to allow it to be used at an ATM to withdraw cash. In this way, the last limitation of the contact payment card can be eliminated.

8. Driving financial inclusion

Biometrically-enabled contactless cards are also playing a key role in improving welfare and financial inclusion. Across Africa, South America and the Indian sub-continent multi-application smartcards are bringing identity and payment together – authenticating users to simplify consumer-to-merchant payments, while allowing the effective targeting and distribution of government-based welfare payments.

One of the most advanced examples is India’s Aadhaar - the world's largest biometric ID system with more than 1bn enrolled members. At its heart is a 12-digit unique identity number issued to all Indian residents based on their biometric and demographic data.

Linked to a number of public subsidy and unemployment benefit schemes, including the subsidized kerosene and LPG scheme and the MGNREGA ‘right to work’ program, Aadhaar linked cards provide direct benefit transfers to retailers – with local biometric authentication delivered by a fingerprint sensor. While this is an off-card approach, with biometric data held centrally, the Aadhaar initiative is a clear demonstration of the value of multi-application payment cards.

Adding biometric functionality to an EMV card can also contribute to making cards more widely accessible in areas with a high illiteracy rate. This has the potential to facilitate access to financial services for individuals unused to PINs or passwords. In this context, biometrics offers a convenient, easy-to-implement solution to verify the customer identity when no other official credentials by government are available. Added to this, should biometrics authentication be based on an interoperable standard solution, regional payment cards will enable cash withdrawal and other transaction services at ATMs or self-service bank kiosks.

9. The crucial role of enrolment

With identity the central pillar of an effective biometric payment card strategy, secure and accurate enrolment is crucial. Here, methods vary – from user-driven enrolment through smartphone apps to physical attendance at an enrolment point. Either way, the process is essentially the same, and consists of collecting and formatting biometric, personal and payment account data for the issuance of the payment card.

From a SPA perspective, the four main objectives to consider when designing an enrolment subsystem are:

- Capturing high-quality fingerprints at the enrolment stage is essential to ensure the best matching rates. Early quality verifications during enrolment will ensure fewer rejection rates during the operational use of the card. However, if the quality of the capture at enrolment is not maintained consistently, the verification systems are likely to experience unreliable performance. Responsibility for ensuring the quality and the security of biometric enrolment process are usually in accordance with contractual requirements. A performance management program should be put in place to monitor enrolment performance, applying corrective measures when required and report enrolment performance to the issuer bank where enrolment is subcontracted to a third entity. As part of this program, the enrolment entity should develop metrics for measuring the impact of poor quality enrolments. The design of the biometric enrolment service should allow for the right metrics to be collected.

- The cardholder experience at enrolment is likely to impact the perception of the operational system and the acceptance of the technology. Indeed, the enrolment session may be the first time that the enrollee is in contact with biometric equipment. Actions to improve the enrolment quality or cardholder experience will have a cost/time impact on the enrolment service: the ease and speed of biometrics capture at enrolment and later verification is therefore important.

- Fraud arises when falsified applicant declarations are made at the enrolment phase in order to obtain false identities. Enrolment is the phase when the document that proves an individual's identity is created, so there cannot be room for error. The identity verifications employed during enrolment have to guarantee the applicant's identity as well as avoiding the duplication of applications by the same individual.

- Specific data protection mechanisms should be designed for the enrollment process. Indeed, sensitive personal data are likely to be stored during a certain period of time in a central data base prior to personalization in the card. The mechanisms used for the transfer, storage and later retrieval of these data, including but not limited to the biometric reference, have to guarantee their confidentiality and integrity.

10. Conclusions

With significant growth expected over the next 18 months and beyond, SPA considers that the introduction of biometrics sensors on payment cards would represent an important step forward for the finance industry, opening the way to eliminating fraud for issuers and cardholders, reducing costs and providing the additional security and identity verification required to support remote or cross-border transactions.

It is our view that a biometric sensor-on-card authentication solution – using a fingerprint in combination with a smart bank card – will meet new security demands while protecting the individual’s privacy. Furthermore, sensor-on-card functionality binds the card to one specific person, removing the possibility of contactless fraud, or transferring or delegating card usage; making the card truly personal and truly secure.

We believe that sensor-on-card fingerprint recognition fits with EMV architecture, as cardholder verification is performed inside the smart card. It is completely scalable and can be introduced to any segment of cardholders and activated on specific terminals. Crucially, as the function is integrated on the card and completely local, there are minimal infrastructure costs.

Finally, the new generation of card platforms makes it possible to simultaneously achieve security and performance when executing a biometric authentication process. Security is achieved by minimizing system error rates. Performance is the result of implementing fast cards whilst keeping error rates low.

Taken together, the stringent security and data protection elements of a biometric-enabled smart payment card should be enough to satisfy the most rigorous of regulators when it comes to eliminating the value ceiling of a contactless transaction. Doing so, SPA believes, will allow issuers to deliver an accelerated and convenient payment option, while at the same time extending financial inclusion through strong authentication to underserved markets across the world.