BIOMETRICS APPLIED TO PAYMENTS
CONTENTS

Biometric payments are ready for prime time 3
Authentication systems are evolving 4
Biometrics will reduce the cost of fraud borne by PSPs 6
Improving payments customer experience 8
The road to implementing a biometric-based authentication for payments 10
Are you ready for biometrics? 12
Biometrics technologies are designed to be more accurate and cheaper, allowing a more convenient payment with a lower risk of fraud while being more accessible to retailers and customers.

Biometrics payments are not only a way for Payment Service Providers (PSP) which intends to reduce fraudulent payments, they are also an opportunity to bring a user-friendly experience to the final customer.

At Accenture, we believe that biometrics is now a must-have. To stay in the race, PSPs may provide to their customers at least one payment method using either facial recognition or fingerprint authentication as a starting point before going toward behavioral biometrics. Regarding retailers, PSPs, for example through partnership between fintechs and traditional banks, can offer merchants biometric payments services to distinguish themselves from competitors.

BIOMETRIC PAYMENTS ARE READY FOR PRIME TIME

Paying for your coffee at the local coffee shop by looking at a screen may once have sounded futuristic. But payments using biometrics, such as face recognition, are happening right now, and their use is growing.
AUTHENTICATION SYSTEMS ARE EVOLVING

The painful life of passwords
From the dawn of the Internet, passwords have been the cornerstone of authentication processes. However, with digital services gathering momentum, passwords have become unmanageable. The average user owns approx. 90 online accounts. Remembering a new password for each service is difficult. Mostly half of users admit reusing their passwords\(^1\) and approx. 49% of them write them down\(^2\). Authentication through passwords may be harmful, both to security and customer experience. Biometrics are one of the effective replacement for passwords, even more with regulations encouraging biometrics adoption.

PSD2 sets a new legal framework for security in financial services that will boost biometric-based authentication
The Revised Payment Service Directive, released by the European Commission\(^3\), introduces a new security requirement for accessing payment accounts and initiate payments: Strong Customer Authentication (SCA). SCA requires at least two of three independent elements:
- **Knowledge**, something only the user knows (login, password ...)
- **Possession**, something only the user possesses (smartphone, paired device, hardware token ...)
- **Inherence**, something the user is, that is to say biometrics.

SCA provides a higher level of security as independence between the authentication elements ensures that if one is compromised, the other(s) stays secure. Furthermore, PSD2 Regulatory Technical Standards (RTS) adds other requirements for SCA such as dynamic linking – the authentication code generated through the SCA needs to be specifically linked to both the amount paid and the payment recipient and shown to the payer – to pursue this objective of security.

In 2017 about 25% of e-commerce transaction requires SCA. According to a Mastercard’s executive, this rate will double or triple once the Regulatory Technical Standards (RTS) which provide detailed specification to comply with PSD2 come into force\(^3\). With the rise of SCA, biometrics may gather a strong momentum. The mobile payments using biometric authentication could reach 18 billion in 2021 (30-fold increase in 5 years)\(^4\).
Biometrics is the process of measuring physiological or behavioral characteristics of an individual as a mean of identification or authentication. **Identification** aims at establishing someone’s identity, answering the question “who this person is?”, whereas **authentication** (also called verification) is about confirming someone’s identity, answering the question “is this person the one he claims to be?”.

Physiological characteristics are inherent features of the human body while behavioral characteristics refer to personal demeanor. Fingerprint-recognition is one of the most widely known biometric mean of authentication, especially since Apple introduced it in its smartphones in 2013. Nonetheless, an increasing number of other methods are used for biometric authentication: physiological biometrics such as face recognition, eye recognition (iris or retina), palm print recognition or veins recognition, and behavioral biometrics such as signature or keystroke scans. Some biometrics can even combine physiological and behavioral metrics analyses, for example voice-recognition which analyses inherent characteristics of the voice and the speaker’s phrasing.

Biometric authentication systems require first an phase, during which the system records the biometric traits of the user to create a template. This phase is critical to authentication process reliability. The system must ensure that the person performing the enrolment is really the client. A strong authentication or an identity check in person in branch is therefore necessary. Once users are enrolled, the system uses the following steps to authenticate them:

- First, a sensor captures the biometric trait of the individual. The technology used may vary from one biometric method to another and even within the same method.
- The biometric sample is converted into a template, then compared by a matching algorithm to the template(s) in the database. The matching algorithm issues a matching score, in other words the probability that both samples belong to the same person.
- Based on this score, a decision module identifies the individual and/or approves the authentication.

**FIGURE 1: BIOMETRICS METHODS**

**NON-BEHAVIORAL BIOMETRICS**
- Fingerprint recognition
- Iris, retina recognition
- Vein recognition
- Palm print recognition
- Face recognition

**BEHAVIORAL BIOMETRICS**
- Signature scan
- Keystroke scan
- Voice scan

**FIGURE 2: MATCHING PROCESS**

Source: Accenture
**BIOMETRICS WILL REDUCE THE COST OF FRAUD BORNE BY PSPS**

**Biometrics accuracy is increasing**

To meet PSD2 requirements, biometrics must provide a level of security high enough to be used as an authentication method. Unlike a PIN code, for which verification is binary (correct or incorrect), biometrics authentication result is a probability and therefore involves a margin of error.

Biometrics accuracy can be measured with two rates:

- **The False Acceptance Rate (FAR):** the probability that a security system will incorrectly accept an access attempt by an unauthorized user. In case of a biometric payment, a fraudster may have a payment accepted when it shouldn’t be. As a Payment Service Provider, you want to avoid the cost of fraudulent payments supported as much as possible, therefore, FAR must also be as small as possible.

- **The False Rejection Rate (FRR):** the probability that a security system will incorrectly reject an access attempt by an authorized user. In case of a biometric payment, the customer may have his payment rejected when it shouldn’t. As a Payment Service Provider, you want to offer the final customer as little inconvenience as possible. In other words, FAR needs to be as small as possible.

The FAR and the FRR will vary depending on the sensitivity of the biometric method used. This sensitivity can be measured by the number of characteristics considered during enrolment and sample verification (i.e. when the biometric print entered by the user is compared with the one stored by the system). These characteristics can be, for example, the number of check points of a face, or the duration and the pressure of a keystroke. The more characteristics the system considers, the more sensitive it is.

The graph below shows that:

- the higher the sensitivity, the higher the FRR
- the lower the sensitivity, the higher the FAR

To have both the FRR and the FAR the lowest possible, a sensitivity threshold must be defined by the system.

If a Payment Service Provider wants to prioritize fraud avoidance, at the risk of increasing customer annoyance, it will set a high sensitivity threshold. On the contrary, if it wants to provide a smooth user experience and support the risk of a higher fraud, it will set a lower sensitivity threshold.

---

**FIGURE 3: FRR AND FAR VARIATION**

Source: Accenture, January 2018
Machine learning improves biometrics accuracy

Behavioral biometrics (writing, key-stroke behavior…), taken alone, may be less accurate than non-behavioral ones (face recognition, iris…). However, with machine learning, behavioral biometrics could be powerful enough to secure a mobile payment. The way people hold their smartphone, use the keys, scroll the screen, or how long they keep it on, are data that can be used through machine learning to create a dynamic print that authenticates the user. This process known as “continuous authentication” is transparent for the customer.

Limits of biometrics accuracy

No biometric-based authentication system is 100% safe. Latest face recognition devices are harder to be fooled by a simple photo anymore. However, it can be with a digital 3-D model or with a high resolution picture. As for voice recognition, it is possible to generate a copy of a voice, including accent and intonation, based on several voice samples. Fraudulent methods described above, and that can be found in news articles, could be worrying for the customer. However, a mass fraud with these methods, in other words a fraud that would fool the system for hundreds or thousands of transactions, is unlikely.

Technologies will keep pushing the limits of the reliability of a biometric system. Payment Service Providers will have to answer this challenge by:

• relying on better device readers: new devices are released regularly with better performance
• setting the right sensitivity threshold to have both the FRR and FAR as low as possible: to define them, PSP must consider several factors such as their client market type, their geography, the number of transactions they process, the risk of loss.
• setting a deadline for each biometric print during enrolment: as technology evolves, devices used to register a biometric print will improve, making possible to register a print of higher quality. Moreover, depending on the biometric method, the original print of an individual can evolve with time (for example, with face or voice recognition). PSP need to consider these re-enrolment processes.
• adding another type of authentication, depending on the level of security required for the transaction: this other layer of authentication can be a password such as a PIN code, or a persistent authentication based on behavioral biometrics.

What if a biometric template is compromised?

If a biometric template is compromised, it can be revoked. The user will have to re-enroll by recapturing a new sample in order to produce a new biometric template. This new template will be similar to the revoked one but strictly different as each sample is different. Biometrics templates are a mathematical representation of a biometric trait sample. However, it is quasi impossible to proceed with reverse engineering to reconstruct the original sample. This means that the voice of an user can not be found back using his/her biometric template. Moreover, best practices of biometrics system design intend to forbid to link directly biometrics templates with personal data to make this link harder for hackers.

Biometrics to prevent fraudulent payments

When a fraudulent payment occurs, depending on the type of payment used by the customer, the bank will support the cost (for example, in a card transaction in a brick and mortar store or in online transactions with 3D-Secure).

For banks, the cost of the fraud is not only the amount of the transaction reimbursed to a customer. It also includes the cost of back offices that processes them (resources, infrastructure, arbitration cost with other banks and with schemes such as Visa and Mastercard…). Moreover, fraud has a negative impact on the bank’s image and on the reliability of its security, not to mention the stressful and inconvenient experience it is for the customer.

To reduce the risk of fraud, PSPs need to provide systems with a high level of security. Biometrics is mature enough to provide this level.
Biometrics systems are not only a way to improve security, but also a way to improve user experience. For banks, authentication process occurring during a payment has always been a tricky equation: find the balance between a high-level of security – to prevent fraud – and a seamless customer experience – to avoid transaction abandon. Biometrics is a solution to solve this equation, and ultimately offer a new payment experience to customers.

Demand for biometrics is on the rise
According to a recent research conducted by Oxford University in collaboration with Mastercard\textsuperscript{13}, the vast majority of consumers (93%) prefers biometrics over passwords for validating a payment. Most of the customers are more and more open to technologies and willing to use innovation. With the ongoing roll-out of smartphones with an embedded sensor – there are now approximately 500 million of biometric devices in circulation\textsuperscript{14} – customers are familiar with using their fingerprint or finger veins to access a service or taking a selfie to unlock their phone. Biometrics have entered everyday life, and we are convinced that familiarity combined with the availability of the technology are leading to an increasing appetite of biometrics-based authentication methods, specially from the youngest customers.

However, customer acceptance among diverse forms of biometrics is not equal and depends on familiarity with the technology, intrusiveness perception, effort required (time and gesture requested from the user) and accuracy of the system. A study conducted by Visa in Singapore\textsuperscript{15} stated that fingerprint (88%), facial (56%) and iris (50%) recognition are in first position in terms of customer acceptance.

The choice between different biometrics forms is also led by the use case: naturally, most of the customers are more willing to use voice recognition on a phone channel than to conduct a face-to-face payment. Sometimes, one of the best way is to let the user choose: Atom Bank offers both voice and face recognition to their customers, and once a customer’s identity credentials are registered (face, voice and passcode), they can choose which biometrics form they want to use to log into the mobile banking application\textsuperscript{16}.

Taking the opportunity of growing customer acceptance, Payments Services Providers and retailers are keen to implement a wide range of customer friendly banking use cases.

Providing opportunities to differentiate through new biometric-backed ways to pay
According to a study conducted by Visa\textsuperscript{17} in September 2017, one consumer out of two (49%) already abandoned an online purchase because they couldn’t remember their password. Some have abandoned simply due to the hassle of entering their password (16%). To tackle this loss of revenue, banks, more generally Payments Service Providers, and merchants, are on the same path to provide a new, seamless, convenient and fast payment experience to customers, for both digital and in-store payments. Initiatives implementing several types of biometrics are tested and deployed to replace passwords or PINs during the payment process pursuing the goal to increase potential revenue from reduced false declines or forgotten passwords and PINs.

Last year, Idemia (ex-Morpho) presented a proof-of-concept\textsuperscript{18} that allowed a cardholder to make a face-to-face payment, first by entering the banking card in the terminal, and then by validating the payment with face recognition via a camera into the payment terminal. Some banks are now issuing cards using fingerprint recognition, instead of a PIN code\textsuperscript{19}.
Visa and MasterCard are both developing this new type of banking card which support high-value contactless transaction, with the same convenience as a mobile payment transaction (such as Apple Pay or similar solutions), but without a battery to keep charged (the card is fully powered by the payment terminal) or requiring any specific device at the merchant, and at a fraction of the cost (by eliminating intermediaries).

Beyond payments, we believe that PSP should also leverage on biometrics authentication systems to provide services requiring access account information compliant with PSD2. Advances in voice recognition used in vocal assistants such as Apple Siri, Amazon Alexa and Google Home, allow customers to initiate hand-free payments: these systems identify users’ voice patterns to recognize their identities and, thanks to artificial intelligence algorithms, understand users’ speech. For example, customers of Capital One, a US bank, can manage their accounts, track spending and pay their bills simply by using their voice. In China, customers can log-in their mobile-banking application to initiate transfers using their voice by saying this short simple phrase: “My voice is my password”.

These initiatives champion the replacement of password or PIN-based authentication methods with biometrics-based ones to make payment acceptance easier for merchants and faster for customers. Moreover, according to the study led by Visa in September 2017, from customers point of view, banks are best positioned to provide and host biometrics solutions: US consumers are most likely to say they would trust their bank (65%) and their credit/debit card network (54%) to store biometric data, compared to a major online brand with a global name (29%), a wireless service provider (23%), or a department store (12%). Banks can use this customer’s trust to provide innovative new payment experiences by leveraging the use of biometrics to differentiate themselves from their competitors.

One step further: invisible payments

Invisibles payments are payments made without any password, PIN, physical card or device, leveraging on the unique inherent characteristic of each person to make a payment.

For example, fast-foods chain KFC in China partnered with the Alibaba’s subsidiary Ant Financial to allow customers to process their payments simply by smiling after placing their order at one of the fast food restaurant’s self-serve screens. A 3-D camera built-in the self-service kiosk scans the customer’s face to recognize and authenticate them, then allowing the payment. The technology also predicts the customer’s order, based on the previous ones.

Invisible payments are also designed to allow customers to check-out and pay for products or services without any action from them. BBVA is testing a facial recognition system at its inhouse cafeteria that can recognize both users’ faces and their orders on the tray thanks to a camera at the checkout location, and then charge their related registered cards.

Technological readiness and consumer interest urge merchants and Payment Service Providers to offer new frictionless payment experiences.
Payment Service Providers willing to add a biometric-based authentication service in their payment process will have to comply with regulations and decide how to implement the biometric solution in their system.

**PSD2, GDPR and others**

PSD2 requires Payment Service Providers to use Strong Customer Authentication such as biometric-based authentication. However, the Regulatory Technical Standards (RTS) on SCA deliberately doesn’t give any specific rules for biometric authentication such as authorized biometric methods, or maximum and minimum FAR and FRR.

Regarding data protection, the GDPR (General Data Protection Regulation) enforced since the 25th of May 2018, gives a set of requirements related to data privacy, including biometric data. GDPR gives the right for European users to access their data and to ask for their data to be deleted or to be transferred to another company. This requirement could turn out to be tricky to implement, especially for sensitive data such as biometric data.

On top of these two regulations, several actors develop guidelines or standards related to biometrics:

- Standards Development Organizations such as the ISO (International Organization for Standardization) and the IEC (International Electrotechnical Commission) whose joint technical committee is particularly active in the biometric field.
- Industry consortia such as the FIDO (Fast IDentity Online) Alliance (consortium including amongst others Mastercard, Visa, Samsung, Oberthur Technologies, Bank of America, Alibaba or Google) that is used for example in Samsung smartphones.

Individual initiatives also push the use of biometric. For example, Mastercard positioned itself as a forerunner in biometric authentication by setting a deadline for all its issuers to offer biometric authentication by April 2019.

**Turnkey solutions**

To support the growing demand, biometrics solutions manufacturers are striving to ease integration in the Payments Services Provider and merchant’s systems.

Implementation of biometrics solutions has become easier and cheaper for merchants and banks. They have a wide choice with no deployment costs since many biometric sensors are now packaged in consumer devices and several biometrics manufacturers provide SDK (Software Development Kit) – a set of tools built to make the call of functions of the underlying software solution easier – ready to integrate into mobile banking applications.

A few specialized vendors – Gemalto, Idemia (ex-Morpho), Vasco and some others – have started to develop turnkey biometric solutions specifically to help banks face up to the challenge of meeting all the requirements of PSD2.

Banks and historical biometrics solutions manufacturers are not the only ones keen on biometrics. Several fintechs are also active in this space, taking opportunities from PSD2 SCA to position themselves in the innovative payments ecosystem. These fintechs provide mainly biometrics-based authentication methods easily pluggable to any use case thanks to SDK and API. For example, AimBrain offers a full set of propriety biometrics authentication methods from voice and facial recognition to behavioral analysis. Some fintechs provide, on top of the biometrics authentication, a fully-packaged improved payment experience immediately available for customers. Saffe, for example, lets merchants use customer face-recognition during the checkout to process the payment linked to their Saffe electronic wallet.
**Architectural considerations**

We encourage the vision of an authentication hub, conceptualized as a set of centralized services, supporting multi-factor and multi-channel risk-based authentication of customers. To pursue this idea, Accenture provides a multi-modal biometric platform which integrates the best of breed algorithms on the market into an overall security scheme with the ability to add any new authentication methods as they become available. Accenture delivery framework supports clients to implement biometrics-based authentication in their ecosystem, from developing blueprint, conducting a pilot, until the build and the run, regardless of the solution chosen.

In the landscape of biometrics, payments services providers have at their disposal different models to implement biometrics-based authentications methods:

- **Develop or own in-house technology:** this option requires heavy investments but allows more flexibility.
- **Interface with a cloud-based solution** from an external provider: this option has minimal integration impacts but could lead to privacy issues.
- **Integrate software authentication solution** from a biometrics solution provider to keep control on the data with affordable costs.

When it comes to biometrics solution implementation, there are two schemes for the hosting architecture of the enrollment processing, template storage and matching computing:

- **Server-side matching:** the biometric sample is captured on the user device, but the template creation, storage and matching are processed on a remote server.
- **On-device matching:** biometric data never leave the user’s device.

The main benefit of on-device matching approach is privacy allowing users to keep the control of their data (in case they want to revoke it), and to protect against a mass attack to breach biometrics data. However, this type of implementation forces users to have as many enrollments as they have devices. With server-side matching approach, PSPs manage a unique identity for users, allowing users to authenticate from different channels (online banking and mobile banking for example). In terms of security, hosting entity can implement strong security measures and make any reverse engineering attacks more difficult.

Biometrics manufacturers provide on-device solutions (promoted by FIDO Alliance), server-side matching approach (such as Nuance or AimBrain promoting BIDaaS – Biometric Identity as-a-Service), or even both, letting the choice of implementation led by the use case and the related constraints (privacy, security, performances).

Thanks to massive deployment of smartphone with biometrics capabilities, Payments Services Providers and merchants willing to implement biometrics-based experiences for their customers have at their disposal a wide range of solutions from historical and new players, easy to set-up, to fit their requirements in terms of security, privacy and customer experience. With its expertise in biometrics innovation, security, and payments, and its experience in delivery, Accenture support clients in their journey to biometrics-based solutions implementation.
ARE YOU READY FOR BIOMETRICS?

Biometric-based authentication applied to payments may grow exponentially in the coming years. Technology and customers are indeed ready to use biometrics in payments, and regulatory organizations are also pushing for it.

Implementing a biometric system is now easier. We are convinced that Payment Service Providers should take the plunge in order to gain market share and stay ahead of their competitors. To do this, they must offer user-friendly and secure ways to perform payments while guiding their clients in this innovative journey to ensure they adopt this new trend.
REFERENCES

3. Many ‘password challenged’ internet users don’t take steps that could protect their data, by Pew Research Center, 2017 (http://www.pewresearch.org/fact-tank/2017/01/26/many-password-challenged-internet-users-dont-take-steps-that-could-protect-their-data)
5. Biometric Authentication in Payments, Promontory (http://www.promontory.com/uploadedFiles/Articles/Insights/Biometric_Authentication_Payments_REPORT.pdf)
14. Beyond Biometrics – Authentication in the new Accenture Deck (https://kxd.documents.accenture.com/contribution/c70262fa-739a-49b8-b553-1e2a1f13e8f7)
18. Payment with face recognition (https://www.youtube.com/watch?v=3BOUXumq77k)
20. Capital One integration with Alexa voice assistant (https://www.capitalone.com/applications/alexa)
21. HSBC Voice ID (https://www.hsbc.co.uk/1/2/voice-id)
ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world’s largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

AUTHORS

Stéphane Ray
Principal Director
Retail Banking/Technology Consulting
Lead of Gallia “Open Banking & Innovative Payments” tribe
stephane.ray@accenture.com

Gabriel Hababou
Consultant
Retail Banking/Technology Consulting
Lead of Gallia “Innovative Payments & Card Management” workgroup
gabriel.hababou@accenture.com