accenture

CONNECT TO YOUR CUSTOMER

WITH SECURE BIOMETRIC BANKING

How biometrics can help banks balance convenience, compliance and security under PSD2—in a world where the right user experience will always win out

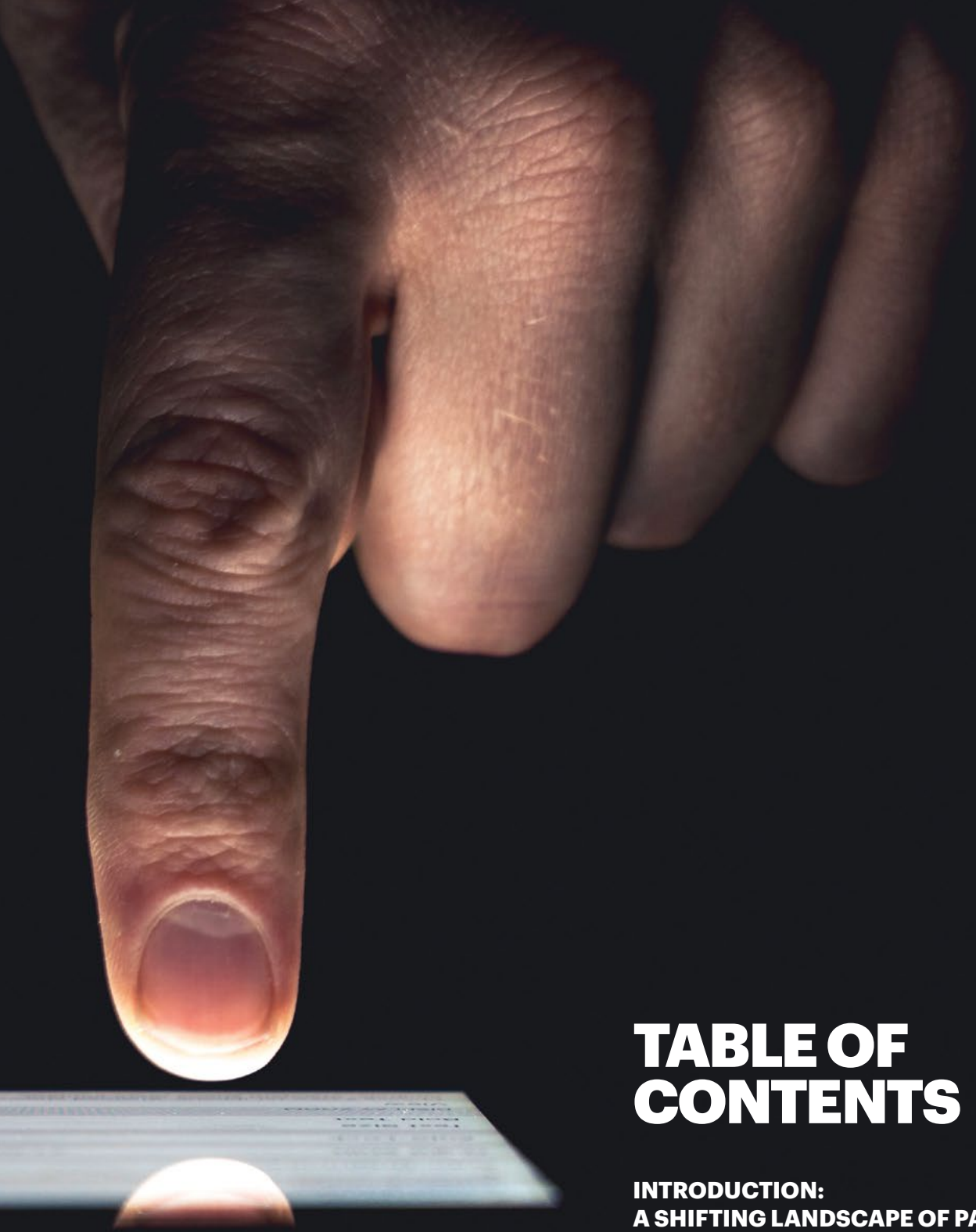


TABLE OF CONTENTS

PAYMENTS EVERYWHERE

The exploding growth of e-commerce and payments innovation continue to delight consumers globally and fuel their appetites for more.

Consumers today can make payments online, on mobile devices, and via social media. Now, they expect—indeed demand and reward—seamless, fast, secure, and invisible payments as part of their buying experience. Fast-evolving regulatory- and technology-driven advances like immediate payments, Open Banking, blockchain, and application programming interfaces (APIs), are sure to make payments processes more convenient, even invisible, in ways that create positive customer experiences like those offered by ride sharing and similar "sharing economy" platforms.

Still, no level of customer experience innovation is deemed positive if users feel exposed to threat. Consumers will only enjoy and trust the latest generation of seamless payments experiences if they have confidence that the payments are authenticated and highly secure.

Biometrics is emerging as the bedrock of keeping consumers' financial transactions and data secure while ensuring a compelling user experience. Leading banks are already working with biometrics. For example, they are using fingerprint for customer identification and transaction authentication in their branches or employing facial recognition and iris recognition for authentication at ATMs. As payments show up just about everywhere in consumers' everyday lives, banks can imbed biometrics to make their payment offerings even more relevant and secure.

GDPR AND PSD2 PUSH FOR MORE SECURE INNOVATION

Addressing the security needs of more innovative payments are two new sets of regulations from the European Union: the General Data Protection Regulation (GDPR) and Second Payment Services Directive (PSD2). While both regulations originate from Europe, they have global impact and implications. From a payments perspective, their effect is to require security of transactions and data while also mandating certain customer experiences.

At the heart of GDPR's impact is a mandate for banks to give ownership of data to customers directly, bringing them the right to review the data held on them, demand updates/erasure of data, and provide consent on how their data can be used.

PSD2 enables entirely new types of payment service with third-party providers to perform payment initiations, request account information such as transaction history, and request confirmation of funds—allowing customers' accounts to be accessed via APIs or screen scraping.

The PSD2 Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common Secure Open Standards of Communication dictate two-factor authentication using two or more of three elements for authenticating a payment or granting access to account information:

Knowledge—*Something you know*—PIN, password

Possession—*Something you have*—hardware token, smartphone

Inherence—*Something you are*—a biometric characteristic

The RTS' requirement for two-factor authentication increases the level of security, but at the same time creates challenges in the customer experience.

PSD2 has been national law in EU Member States (not yet in the Netherlands) since January 2018, and the RTS will become effective September 14, 2019. Banks and payment service providers have until that date to upgrade their payments and security systems to meet the RTS SCA requirements.

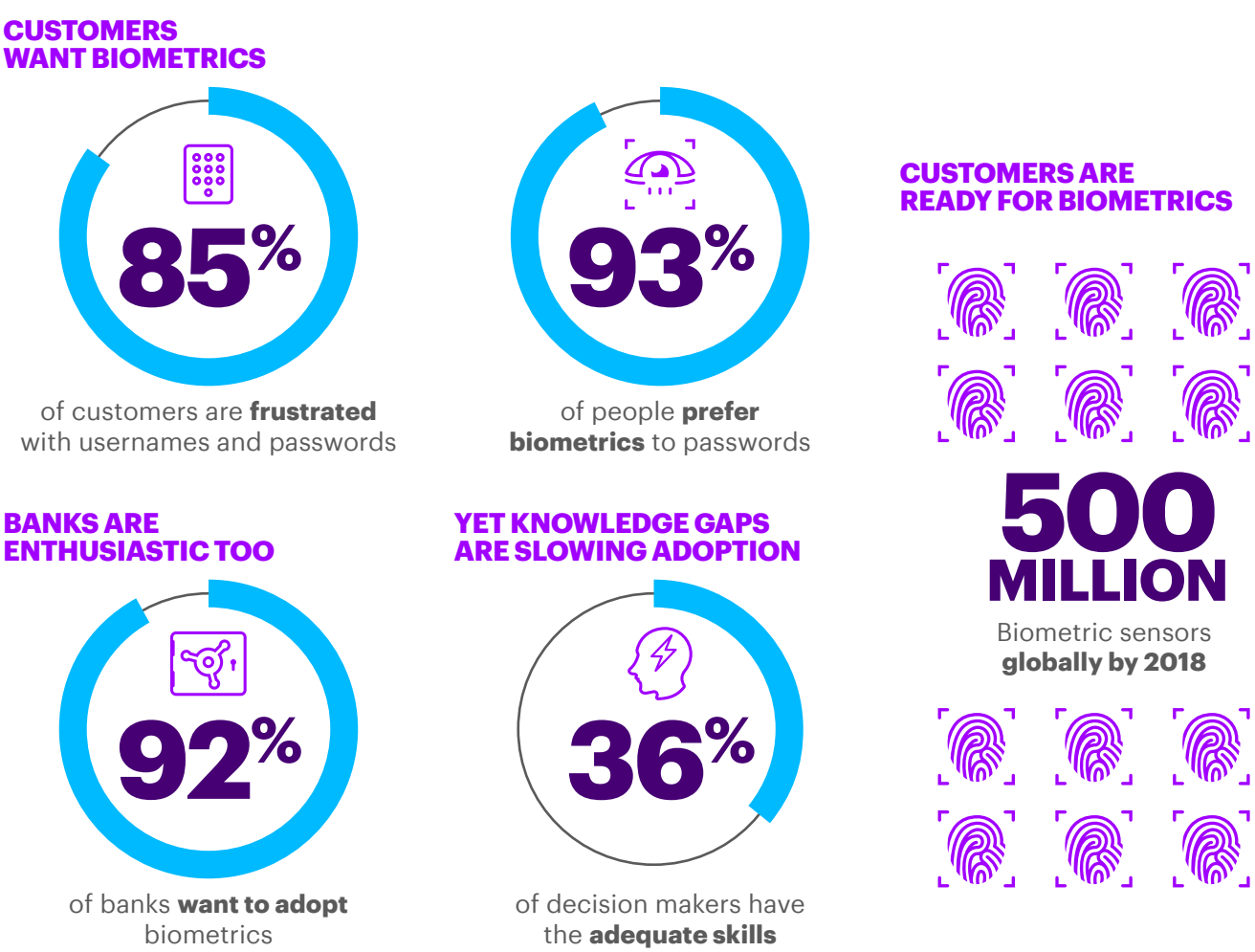
STRIKING THE RIGHT BALANCE: BIOMETRICS CAN HELP

For banks, the effect of the new SCA requirements is to force banks either to keep their existing SCA methods—if they're already compliant—or adjust them to be at least minimally-compliant. In doing so, they will need to strike the right balance among three potentially conflicting attributes: regulatory compliance, a frictionless and convenient customer experience, and robust fraud/liability management.

However, there are significant challenges to overcome. The most RTS-compliant technologies require a separate security device, which is inherently inconvenient for users and, yet, not usable for omnichannel authentication. This means that banks need to develop innovative, secure, and convenient authentication methods using multi-purpose devices. In the next few years, this will become a major differentiating factor for banks

Just a few banks have already adopted multi-factor authentication (MFA)—usually using a password and dedicated authentication device or app—and most banks plan to adopt MFA in the future. While MFA does help to shield resources from security threats, cyber criminals are always searching for new methods of attack. For banks, the problem lies in the choice of authentication factors: what a user possesses can be lost, duplicated or stolen; what a user knows can be shared or assumed; but what a user is or does is unique to him or her.

FIGURE 1: Drivers for adoption of biometrics—fueled by customers' demand for a seamless experience



Sources: Mastercard, Gartner research.

This is why choosing biometrics as one of the factors in multi-factor authentication can address the shortcomings posed by other means of authentication. What's more, biometrics also scores highly on convenience. And while a balance between security and convenience is needed, the fact is that—when users have a choice—a more convenient solution will ultimately win out. In addition to these benefits, biometrics also offers banks lower processing costs—it can be used as a substitute for expensive one-time password systems such as a one-time code SMS—and can enable them to differentiate themselves from the competition (Figure 1).

WHAT IS BIOMETRIC AUTHENTICATION?

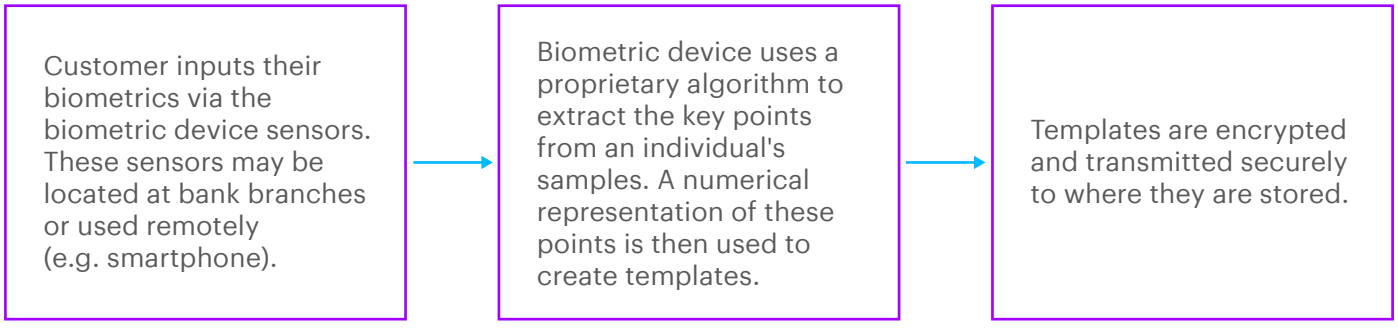
A biometric is defined as any measurable, robust, distinctive physical characteristic or personal trait that can be used to identify—or verify the claimed identity of—an individual through automated methods. All biometric systems consist of two basic elements: enrollment and matching.

ENROLLMENT

Enrollment is the process of collecting biometric samples from an individual and generating a template that is used for all subsequent matching (Figure 2). Templates are created by a biometrics device which uses a proprietary algorithm to extract "features" appropriate to that biometric from the individual's samples.

In basic terms, templates are numerical representations of key points taken from a person's body or behavior. The template must be stored somewhere like a biometric device, central computer, secure element or smart card, so it can be used for comparison when a user tries to access the system.

FIGURE 2: The process for creating a biometric template



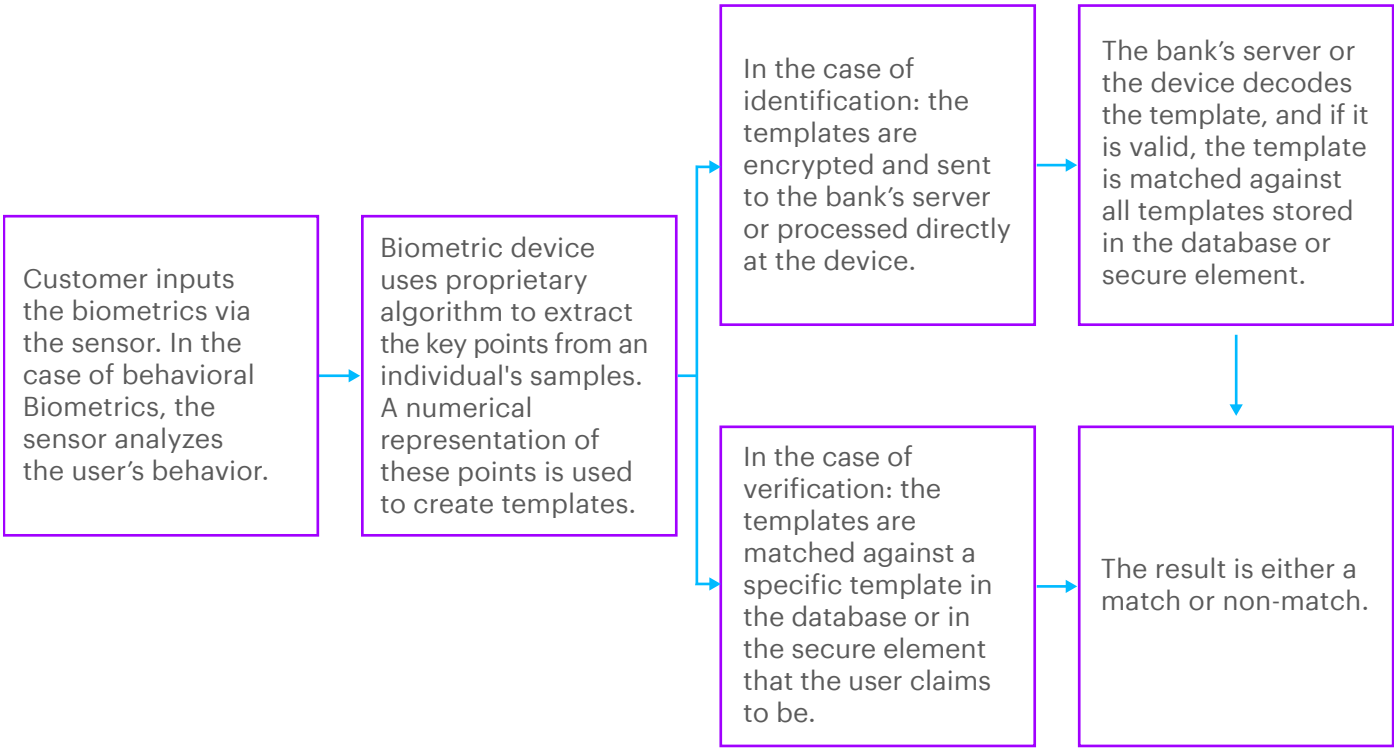
HOW TO ENSURE THE RIGHT SECURITY CREDENTIALS ARE CREATED AT ENROLLMENT IN A FRICTIONLESS WAY?

During the enrollment process, how can a bank be sure that the security credentials are being created for the right customer? Current fingerprint solutions provided by smartphone manufacturers offer a single enrollment of one profile allowing mapping to multiple fingerprints and different individuals at the same smartphone device. How can a bank know who among these many users is actually authorizing a transaction? One approach for the bank is to run the enrollment in the existing mobile banking app using existing authentication methods. In addition, the bank might require a minimum baseline data set for the user to proceed with enrollment and reject individuals as unauthorized if the data set isn't present. The initial data requirement might potentially be met using a biometric picture of the customer stored during the bank's KYC process, or even through an official eID (electronic identity) scheme. The bank could use face recognition in the first step of enrollment to compare the applicant's face with available biometric data, and then start the actual enrollment and issuance of security credentials in the second step.

MATCHING

Matching involves comparing the template produced during enrollment with the one produced "on the spot" as a user tries to gain access. The matching can be of two kinds. The first is identification, where the biometric system attempts to answer the question, "Who is X?" using a "one-to-many" search (1:N). The second is verification, where when the biometric system attempts to answer the question, "Is this X?" using a "one-to-one" search (1:1). The matching process may result in a match or a non-match (Figure 3). A heavy emphasis on user convenience results in little tolerance for denying legitimate matches and will tolerate some acceptance of imposters. In contrast, a heavy security emphasis errs on the side of denying legitimate matches and does not tolerate acceptance of imposters.

FIGURE 3: Matching process



ASSESSING RTS-COMPLIANT BIOMETRICS

There are many biometrics solutions out in the market, but they must meet the same strict RTS requirements on SCA as the existing less convenient authentication methods do (Figure 4). The final RTS indicates that the following high-level criteria will be applied in assessing whether authentication methods qualify as SCA:

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. Also, all information about the amount paid and the payment recipient must be passed on across all phases of the authentication. For biometrics, the numerical representation generated from the data points collected at the customer's device needs to dynamically linked.

INDEPENDENCE OF CHANNELS.

The channel used for the initiation of a payment or account information transaction must be separate from the channel used for the reception of the authentication code. Multi-purpose devices can be used for more than one of the authentication elements, provided separate execution environments on the device are used for the different elements, and the device or software is not altered by the payer or TPP.

CREATION AND VALIDATION WITHIN BANK'S ENVIRONMENT.

The creation of the PSU security credentials, their integrity and confidentiality, their association with the PSU, and their secure submission to the PSU all need to be performed within bank's secure environment. The validation of the personalized PSU security credentials is also the bank's responsibility, and needs to take place within the bank's environment as well. For biometrics, the creation of the templates needs to be performed in the bank's environment, and the software that collects the data points on the device must also be provided by the bank. The validation of the data points collected at the device also needs to be performed in the bank's secure environment.

UNDERIVABLE AUTHENTICATION CODES.

Authentication codes must not give any indication about the algorithms of the authentication methods. Also, it must not be possible to derive or forge codes from previously created ones. For biometrics, there is no such concept of authentication codes, but the idea can be applied on biometrics as well. The data points collected at the device must be changed in such a way that every data point package can be considered as a new "authentication code," is unique for every request and, at the same time, is capable of being verified by the bank in the matching process. This is critical to avoid hackers spoofing and reusing data points.

NON-DISCLOSURE.

Security credentials must not be stored in plain text, and the related secret cryptographic materials must be protected from unauthorized disclosure. For biometrics, the biometric data points or raw data and matching templates must not be stored in the device or the bank, in order to prevent reverse engineering of the raw biometric data. Matching templates should be stored at the bank server or at the device; for example, in a hardened bank app that stores templates in the secure element within the device. However, in these cases, the bank must still have control over this function.

The RTS does not clearly specify what the biometrics requirements are, or what the authentication methods should look like—regulators are leaving it open to the market to come up with standards for RTS compliance and evaluation. The FIDO Alliance is aiming to adapt its framework to comply with the RTS, and this can be used by banks, enabling them to rely on an internationally recognized interoperable ecosystem of authenticators. Existing authentication methods have their strengths and weakness in terms of user convenience. Biometrics can help in combining security and convenience for the user.

A further factor to consider is that the RTS requires banks to ensure that security credentials—in this case biometric profiles—are generated in a secure bank environment, and delivered in secure way to the right customer. Today, commonly-used biometrics solutions such as Face ID and Touch ID generate and store credentials in the device, and the bank is not involved in the process. This makes them potentially non-compliant with the RTS—although they're undeniably convenient and popular with users. Dynamic linking is a further challenge for banks: how do they link the amount and the transaction with a specific request when using a biometric-based solution?

Figure 4 shows an assessment of the most widespread existing authentication methods used in Europe against the SCA criteria set out in the RTS.

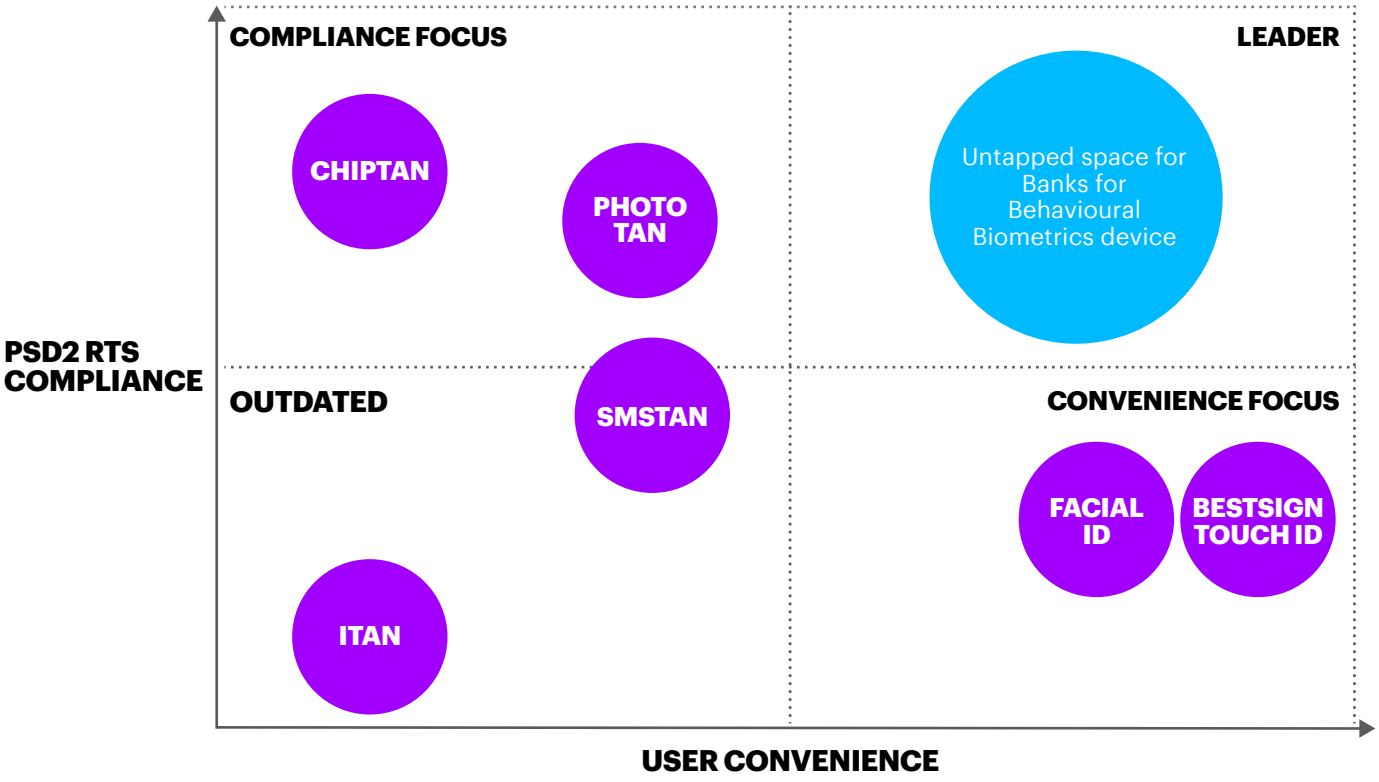
FIGURE 4: An assessment of existing authentication methods against the RTS requirements

AUTHENTICATION METHOD*	DYNAMIC LINKING	INDEPENDENCE OF CHANNELS	BANK ENVIRONMENT	UNDERIVABLE AUTHENTICATION CODES	NON-DISCLOSURE
iTAN (list of printed indexed Authentication codes)	X	✓	X	✓	X
smsTAN (Authentication code is sent to a GSM mobile number)	✓	X	X	✓	✓
photoTAN (Authentication code is sent as a graphic picture on a secure smartphone app)	✓	X	✓	✓	✓
chipTAN (Authentication code is generated on a separate security device with a smartcard and PIN)	✓	✓	✓	✓	✓
BestSign Touch ID (Authentication performed via Apple's Touch ID)	✓	X	X	X	X
BestSign Dongle (Authentication code is generated on a separate security device using Bluetooth and PIN)	✓	✓	✓	✓	✓

*TAN stands for 'transaction number', and is equivalent to 'authentication code'

Existing authentication methods meeting SCA criteria have their strengths and weaknesses both in terms of security and convenience for the user. Banks will move into the leader quadrant by developing biometric authentication that combines RTS compliance and user convenience (Figure 5).

FIGURE 5: Authentication methods on a matrix of potential RTS compliance and user convenience



BIOMETRIC MODALITIES: AN EXPANDING RANGE OF OPTIONS

INNOVATION IS ADVANCING.

Until a couple of years ago, use of biometrics for authentication focused almost exclusively on finger scanning or signature scanning. However, new technologies are now enabling rapid innovation in biometrics, in two areas in particular.

The first is ***visual biometrics***, using five characteristics.

- **Facial recognition**—by recording the spatial geometry of the face. For example, Alipay™ is using a facial recognition system called "Smile to Pay" for customers at a KFC fast food restaurant in China.[2] The system works by using a photo ID of the customer, previously stored in the system, and scanning their face for a match.[3]
- **Fingerprint**—using the ridges and valleys on the surface tips of the human finger. Bank of America is using Touch ID by Apple on customers' mobile phones when they are signing into its mobile banking app.[4]
- **Finger-vein**—using the finger veins below the skin.
- **Hand/finger geometry**—measuring many dimensions of the hand and fingers.
- **Eyes**—including iris recognition and retina recognition.

The second area of innovation is ***invisible and frictionless behavioral biometrics***, including:

- **Dynamic signature verification**—examining dynamics such as the speed, direction and pressure in an individual's signature.
- **Keystroke dynamics**—examining dynamics such as speed and pressure in an individual's keystrokes.
- **Voice recognition**—using vocal characteristics to identify individuals using a pass-phrase.

The actual innovation towards a frictionless user experience is in the combining of multiple behavioral biometrics parameters. For example, continuously collecting data on the angle the device is positioned during a specific time period as well as the user's typing speed and finger pressure, while using an application to match those parameters against templates in the background (without explicitly asking the customer for inputs) allows for strong customer authentication for any transaction without the need to apply RTS exemption rules or unwanted friction in the customer experience.

BUT, EACH METHOD HAS SOME DRAWBACKS

While all these modalities have been enabled by advances in technology, each has some drawbacks. For example, iris recognition could potentiality be hacked using a combination of nightshot camera images and contact lens; people's retinas can change due to high blood pressure or other medical conditions; and fingerprint authentication may be hampered by dirt, sweat or water on the hand or on the scanner. Meanwhile, facial recognition can encounter performance problems from dark background lighting, and voice recognition can be hampered by factors such as background noise.

FRONTIER INNOVATIONS: BaaS AND IoT

Alongside the emergence of new modalities, other innovations are also in development. One is ***Biometrics as a Service (BaaS)***, an approach based on sharing data with a remote server holding a centralized biometric database and offering biometric-based authentication as a service over the internet. Like other cloud-based services, this relieves the customer—in this case the bank—of the complexity and cost of developing and standing up the capability itself.

The other frontier is ***biometrics and the Internet of Things (IoT)***. Security is a major challenge to the IoT, and millions of new devices joining an IoT network with traditional authentication methods could pose a big security risk. Passwords can be forgotten, guessed or shared, and the security of other IoT devices can be compromised if the same password is used. Combining passwords with an additional factor to achieve two-factor authentication enhances security—and biometrics are a natural fit.

REALIZING THE POTENTIAL

OVERCOMING THE HURDLES...

As we've highlighted, in approaching the RTS SCA requirements banks need to balance regulatory compliance, a frictionless and convenient customer experience, and robust fraud/liability management. The payments offerings with the most convenient authentication experience will have a clear edge in the marketplace—and biometrics offers the best chance of achieving such an edge.

As biometric solutions gain momentum and uptake, they face three hurdles. The first is regulation; given the need to comply with the PSD2 RTS. The second is technology; ensuring the solution's functionality and security. And the third—arguably most challenging hurdle—is the need to develop an ecosystem in which biometric methods are used in a consistent and standardized way across multiple markets benefitting from network effects.

...BY FOCUSING ON FIVE KEY PRIORITIES

In Accenture's view, banks can realize the opportunities of biometric authentication by focusing on five priorities.

1. Consider the end, not just means.

Biometric modalities need to be assessed in light of the bank's specific requirements, and the approach to integrating multiple modalities must be considered carefully.

An important part of this assessment should include comparisons of different modalities' strengths and weaknesses.

2. Omnichannel is key.

Banks should create an omnichannel vision before considering their biometrics strategy. Many financial institutions are already benefiting from an authentication hub approach that provides authentication for all banking channels, including branches, ATMs, mobile and online. Biometrics in the cloud or as-a-service offering may also help to meet omnichannel authentication needs.

3. Implement risk-based authentication.

Banks should consider creating a risk-based authentication and authorization capability to work in conjunction with their fraud and risk engines. Under this model, the risk engine is linked to an authentication solution and prompts for step up and step-down authentication based on the risk involved. The step-up creates some friction in the payments experience for customers, but they are generally willing to accept this if they know it is for their own security.

4. Choose the right solution architecture.

There are two main schools of thought for hosting biometrics architectures: server-side biometrics (centralized) and on-device (de-centralized). Server-side biometrics offers the benefit of tapping vast processing and computational power, fits well with omnichannel authentication and makes it easy to enforce and monitor security standards.

A decentralized framework (on-device matching) enables user authentication to happen locally on a trusted device, rather than passing credentials for authentication by a central platform. With this approach, biometric data should never leave the end-user device—typically a smartphone—eliminating the risk of a large-scale data breach. However, omnichannel authentication and integration with other applications like KYC will not be possible if biometrics are kept only on the device.

5. Select solutions carefully in terms of RTS compliance.

Before deploying authentication solutions, banks should ask potential solution providers some probing questions about RTS compliance. Who has access to the biometric data and the algorithms? How are they stored? How can dynamic linking be ensured? Will banks in control of the entire solution end-to-end? How will the solutions support multi-factor authentication with biometrics as one element? How will customers give their biometric inputs at the endpoints? With many laptops and smartphones now equipped with built-in scanners, is it possible to use these as part of the solution?

SOME BIOMETRICS USE CASES IN BANKING AND BEYOND

BIOMETRICS IN BRANCH BANKING

Banks are using fingerprint and finger vein biometrics for customer identification and transaction authentication in their branches because these two biometric authentication methods deliver fast results, are user friendly and ensure reliable security.

BIOMETRICS IN BANKING ATMS

Usage of biometrics in banking ATMs is growing in developed countries. There are two approaches—using only biometrics and a bank card, or a PIN along with biometric authentication. Facial recognition, fingerprints, finger vein patterns and iris recognition are the most suitable methods for ATMs.

BIOMETRICS IN INTERNET BANKING

Many computers, laptops, and even smart phones already have webcams, microphones, and fingerprint scanners, offering flexibility for banks to adopt biometric authentication in online banking services, often as part of multi-factor authentication.

BIOMETRICS IN MOBILE BANKING

While mobile banking is growing rapidly worldwide, many customers still have concerns over the security of mobile banking platforms. Banking transactions or customer services can be secured through a voice or speech recognition system using the microphones in customers' phones.

BIOMETRICS IN-STORE WITH INVISIBLE PAYMENTS

Large grocers and other retailers are tapping into the potential of frictionless commerce in their physical stores, where customers walk into the store, are recognized using technologies such as face recognition, and have all their purchases tracked electronically. Then the payment is made invisibly—without involving the customer—as they walk out of the store.

THE EYES—AND FACE AND FINGERPRINTS—HAVE IT

There are various technology strategies banks can employ to assess, implement and take full advantage of biometric authentication. For example, a growing number of banks are looking to create an authentication hub that can:

- Pick and choose biometric and non-biometric authenticators. A number of solutions—the likes of BehavioSec, Vasco, Nuance, and Transmit Security—are designed to provide multi-modal biometrics functionality.
- Embed existing authentication technologies, reducing or eliminating technical debt.
- Deploy a flexible architecture, enabling fluidity while facilitating compliance with PSD2 and GDPR.
- Offer contextual, risk-based and persistent authentication to reduce fraud and improve the customer experience.
- Prompt customers for a secondary, or step-up, authentication if an omnichannel risk threshold is breached.

By connecting applications to the authentication hub, banks can avoid the need to embed authenticators into individual applications and create one interface for requesting authentication and provisioning services. Once an application is connected to the solution, organizations can plug in the biometric authenticators they want and switch between them without touching the application.

As biometric authentication gains traction and usage, it's clear that it offers competitive banks a way to strike the right balance in customer experience, compliance, and security in a PSD2 world. While there will be challenges along the way, leading banks will follow a structured approach to effect security innovation. Grounded in our experience helping banks and payments providers prioritize and realize the opportunities of biometric authentication, Accenture can guide you in selecting the right suite of biometric solutions for your business and connecting with your most valuable customers.

AUTHORS

SULABH AGARWAL
Managing Director
Accenture Payments
sulabh.agarwal@accenture.com

HAKAN EROGLU
Senior Manager
European Open Banking Lead
hakan.eroglu@accenture.com

NOTES

[1] The FIDO Alliance. https://fidoalliance.org/

[2] The Verge, "KFC in China tests letting people pay by smiling," September 4, 2017. https://www.theverge.com/2017/9/4/16251304/kfc-china-alipay-ant-financial-smile-to-pay

[3] TechCrunch, "Alibaba debuts 'smile to pay' facial recognition payments at KFC in China," September 4, 2017. https://techcrunch.com/2017/09/03/alibaba-debuts-smile-to-pay/

[4] Bank of America, "Mobile Banking Account Management." https://www.bankofamerica.com/online-banking/mobile-banking-account.go

ABOUT ACCENTURE PAYMENTS

Accenture Payments helps banks, payments providers and other players transform their payments systems and operations to grow and win in the digital economy. We offer unmatched capabilities, scale and experience of Accenture to address the end-to-end needs of payments stakeholders— from the boardroom and C-suite to the back office. Our services support every phase of the payments value chain, and can help reduce costs and improve value outcomes. Our more than 4,300 payments advisors and payments systems integration specialists bring together strategy, business function consulting, digital technology and delivery execution know-how to help keep our clients on the leading edge of payments. To learn more, visit www.accenture.com/payments.

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 specialised 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 442,000 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.

www.accenture.com/banking

Accenture Banking

@bankinginsights

Accenture Banking blog

180829U