IMPRINT YOUR FUTURE

BIOMETRIC AUTHENTICATION IN THE NEW DIGITAL WORLD

Perspectives for the Banking Industry
After many false dawns, consumer grade biometric authentication is now a mature technology—thanks to the proliferation of smartphone-embedded biometric sensors and a near-universal acceptance of passwordless authentication. After all, passwords are difficult to remember, often easy to steal, and a nightmare to manage.

The emerging challenge facing financial services firms now is how to take advantage of the dramatically improved customer experiences and security capabilities biometric authentication makes available while avoiding vendor lock-in or unnecessary commitment to a particular biometric modality, strategy, or architecture.

We believe the solution is an “authentication hub” that has the ability to:

- Pick and choose biometric and non-biometric authenticators
- Embed existing authentication technologies—thereby reducing or eliminating technical debt
- Deploy a flexible architecture for greater fluidity, while facilitating compliance with emerging legislation
- Offer contextual, risk-based, and persistent authentication to help reduce fraud and improve the customer experience
- Prompt customers for a secondary, or step-up, authentication if an omni-channel risk threshold is breached

Now is the ideal time to examine the rapidly expanding applications for biometric recognition and the new breed of solutions designed to take advantage of the current situation.
The idea of using biometrics for authentication is not new. However, a critical mass movement within financial services has brought biometric authentication into the mainstream, driven by the following circumstances.

- Upcoming regulatory requirements under Payment Services Directive 2 (PSD2) and its strong customer authentication (SCA) provisions, as well as Open Banking
- A rapid and steady rise in financial losses due to payment fraud
- Dramatic recent improvements in the maturity of biometric authentication products in the marketplace

Well-deployed, multi-factor authentication can help the financial services sector take advantage of enhancements in authentication processes not only for online and mobile banking customers, but also for those using legacy channels such as branch and contact centers. These enhancements reduce organizational friction, improve interactions with customers and realign the sector’s customer service offerings with the expectations of an increasingly digital, interconnected, and brand-neutral population. There are options for leveraging offerings from a marketplace of established and trusted vendors, as well as new challengers.
MULTI-FACTOR AUTHENTICATION: A REGULATORY REQUIREMENT

In 2007, the PSD created a single market for payments within the European Union (EU). This included regulation covering credit transfers, direct debit transfers and cards.\textsuperscript{5}

PSD2 came to be following the significant digitalization of the European economy since PSD—as new players who entered the market provided new services that fell outside of PSD and the EU regulated framework. In our view, the directive seeks to address the progress made within the European payments space by making payments more transparent and safer, while encouraging innovation and making the market more competitive.

The main changes under the PSD2 framework include:

- **Acknowledgment of new players** accessing consumer accounts (third-party payment service providers (TPPs) will be able to access customer accounts via application programming interfaces (APIs) to make payments on behalf of customers and provide an overview of their various payment accounts, using a single interface)
- **Increased transparency** through a breakdown of payment information that shows the costs involved in a single transaction
- **Promotion of innovation** in the payments space

Along with the new regulations, SCA is bringing new and stronger consumer protections that combine security elements with requirements for authentication elements categorized as:\textsuperscript{6}

- **“Knowledge”** – those elements only the user knows, such as PINs or passwords
- **“Possession”** – those elements only the user possesses, such as a mobile device or token
- **“Inherence”** – those elements integral to each user (and read by devices and software), such as biometrics (fingerprint, face, etc.)
If banks fail to apply SCA, they cannot require payers to bear any financial consequences—unless the payer has acted fraudulently. Banks may also be required to compensate other payment providers, or even intermediaries, “for any losses incurred or sums paid.”7 Banks should consider the level of security and risk, as well as customer usability. While knowledge is likely to be the first factor of choice, inherence remains a preferred solution for the second factor, by way of authentication methods such as biometrics.

Biometric authentication is consumer-friendly and works in real-time. Recent technology improvements also make implementing it more straightforward for financial institutions. Other benefits include enhanced user experience capabilities, improved risk management and greater accuracy—which makes fraud less likely, therefore addressing SCA concerns. Essentially, with biometric authentication, banks can save time and money while fighting fraud.

Behavioral authentication is a particularly beneficial addition, in light of the potential exemption from SCA if risks of fraud are low. Banks can transparently apply behavioral authentication and similar persistent authentication methods—which assess customer behavior for a specific transactional scenario risk in real-time.

Doing so further enhances the customer experience by:

- Decreasing organizational friction in low risk situations
- Increasing security in high risk transactions
- Avoiding having to decline a customer’s transaction

Essentially, with biometric authentication, banks can save time and money while fighting fraud.
INTRODUCING AUTHENTICATION IN THE NEW

Three key trends have facilitated the inception of a new class of authentication platform.

1. MOBILE DEVICE EXPLOITATION
Many online service providers, online retailers and banks are offering customers options to authenticate multiple channels through push notifications to mobile devices for added security, ease of use and a better customer experience, and to comply with regulatory frameworks.

2. NEW DIGITAL AUTHENTICATION METHODS
Seamless authentication between channels and services, and interoperable universal authentication schemes, are making it easier for customers to use one set of credentials to authenticate for services provided by different organizations (i.e. under PSD2, among others).

3. CROSS-CHANNEL HARMONIZATION AND INTEGRATION
Authentication at ATMs (automatic teller machines) is now possible via mobile device biometrics. Banks have begun to exploit voice biometrics for added security and an enhanced customer experience in voice channels. Some banks are also pioneering new authentication methods (i.e. social login, risk, context-based).
INTRODUCING PROGRAMMABLE AUTHENTICATION

Digitally-forward organizations tend to employ the following three steps to bring together biometrics, behavioral profiling, push notifications, analytics and other digital building blocks.

1. **Connect applications to an authentication hub** to create a single interface for authentication and provisioning tasks, thereby eliminating the need to embed authenticators into individual applications—which can result in high complexity and high maintenance costs.

2. **Select application agnostic authenticators**, including face recognition, iris recognition, voice recognition, fingerprint, one-time password (OTP), notifications, pattern drawing and more. Once an application is connected to the solution, organizations can select the authenticators they want to use and switch between authenticators without touching the application—simplifying the development process. Existing authenticator investments should be plugged into the solution.

3. **Add context and learn behaviors** to reach better authentication and provisioning decisions, for example, based on device type or location. The solution should automatically profile devices, locations, access times, activities, transaction sizes and other factors. Profiles are built over time to provide a non-linear return on investment.
Our idea of an authentication hub consists of a set of centralized services that:

Facilitate multi-factor authentication, with the ability to choose different authenticators

Support multi-modal biometrics across multiple channels for both customers and internal users

Use data from transactions, risk and fraud systems, and the network layer to make informed decisions on what the user can do

Beyond user-facing, multi-factor authentication and multi-modal biometrics, we see a need to provide traditional identity and access management (IAM) capabilities for customer-facing applications. The hub should also facilitate a risk-based authentication and authorization capability that works in conjunction with fraud and risk engines. Enrollment is another key component of the authentication hub concept in terms of addressing the critical link between a person and their assertion of their identity (e.g. passport, ID card, driving license, employee ID, etc.). Finally, we encourage a robust back-end capability to support these activities (see Figure 1).
Mobile Know Your Customer (mKYC) technology to facilitate identification and verification for digital user enrollment and account sign-up

Biometric Authenticator Framework to integrate biometric authenticators, such as voice and fingerprints

Pick and choose authenticators that allow users to nominate how they authenticate within acceptable security baselines, including the ability to plug and play legacy authenticators, such as OTPs, PINs and pattern drawing; as needed

Risk engine aligned to fraud, and that provide information and context on users, behaviors, devices and transactions

Signing in the new with both tactical and strategic solutions to eliminate wet signature in both the short and long term

Source: Accenture, January 2018
Customers now expect to sign up for new financial services through the devices in their pockets. Disruptor banks are setting the bar here, while established financial services providers scramble to keep up.

There are a number of key obstacles to overcome in order to deliver a fully automated, digital, remote account onboarding process, including complying with requirements like Know Your Customer (KYC) and Anti-Money Laundering (AML) while maintaining confidence in identity assertion, document authenticity and validity.

It’s important to note that in some situations, it may be necessary to maintain in-person ID proofing (for example, when complying with standards such as NIST SP 800-63-3). However, the good news is that most bank customers own all the necessary equipment (i.e. smartphones or webcam enabled computers) to allow remote document capture, leveraging advanced cryptographic capabilities and several biometric sensors to deliver facial, voice and fingerprint recognition to positively match users to the identity documents provided.

The onboarding process can be broken down into three phases:

1. **RESOLUTION**
   Where centralized matching is used, the application collects core attributes from the customer to uniquely distinguish them from among a given population or context. These core attributes can contain image scans of acceptable documentation, such as drivers’ licenses, passports and proof of address.

2. **VALIDATION**
   Evidence collected during the Resolution phase is validated against an internal or external golden source of data. Validation should prove documentation authenticity, validity and accuracy. It should also be related to a single, real-life subject. Once this process is complete, a claimed identity has been established.

3. **VERIFICATION**
   Typically, linkage between the claimed identity and the real-life existence of the subject holding the device is asserted through biometric recognition technology, such as facial recognition matched against the supplied photographic ID. “Liveness Detection” should be deployed at this stage to help reduce one of the risks of fraudulent account sign-up.
“They (fingerprints) have the unique merit of retaining all their peculiarities unchanged throughout life, and afford in consequence an incomparably surer criterion of identity than any other bodily feature.”

– SIR FRANCIS GALTON, 1892
Support for biometric capabilities and authenticators is critical to the success of the hub concept. The authentication hub provides the framework to support multi-modal biometrics.

Biometric modalities can be described as either physiological, behavioral or mixed. They have varying characteristics suited to different populations, environments and risk tolerances. Assessing these factors is key to designing a system that balances user experience against security (see Figure 2).

Different biometric modalities have different strengths and weaknesses. In the authentication hub concept, solutions are not tied to one technology or even a single vendor. Different combinations of matching algorithms can be combined to achieve the best fit with business requirements. The framework orchestrates the flow of information—translating challenges and responses without the need for multiple point-to-point integrations.

The authentication hub decouples biometric capture and matching from the back-end business logic. This provides the flexibility to change authenticators as the market and customer expectations evolve, without needing to go back to the drawing board.

Because the framework only needs to be integrated once to provide access to all the authenticators, it is easy to reuse them for a myriad of business functions—such as transaction authorization, third-party access via APIs or cross-channel authentication from branches or contact centers.

“Fingerprints cannot lie, but liars can make fingerprints.”

9
Figure 2. Biometric Modality Success Factors

- **Universality**: Presence of the trait in all members of the relevant population
- **Permanence**: The stability of the trait over time and resistance to ageing, disease and injury
- **Collectability**: The ease by which good quality samples can be acquired
- **Vulnerability**: The vulnerability of the modality towards fraud
- **Acceptability**: User reservations around the use of a specific modality
- **Usability**: The ease with which a user interfaces with a system
- **Cost**: Hardware and software costs of collecting a sample
- **Accuracy**: The expected false acceptance and rejection rates under varied circumstances

Source: Accenture, January 2018
Wearable devices are starting to hit the market, and with them come a wealth of new authentication capabilities. These new capabilities present new possibilities for increasing customer choice, reducing the friction of authentication and capturing greater value from legacy systems.

Leveraging behavioral device characteristics can provide continuous authentication—supplementing explicit authentication requests. This allows for a move away from fixed business logic toward a dynamic risk profiling of each transaction.

Using mobile device biometrics is an ideal secondary authenticator across multi-channel applications such as web, phone and branch—achieved by utilizing push notifications to deliver this request from any channel to the mobile device. Doing so not only provides a standardized, simple, and secure secondary authentication experience across all channels, it also smooths the path to upgrade and strengthen legacy security systems, such as card readers and one-time passwords.

In addition to giving the business more choice, a flexible hub architecture also provides much greater consumer choice by allowing end users to select their preferred means of authentication—within the risk guidelines defined by the hub. The available authenticators can be broadly grouped into two categories: explicit and persistent (see Figure 3).

Mobile biometric technology has made a huge leap in recent years. It is now easier than ever before to seamlessly integrate these sensors into mobile applications.
Leveraging behavioral device characteristics can provide continuous authentication—supplementing explicit authentication requests.
A well-tuned system is one where security and usability are balanced to meet business objectives.
BIOMETRIC MODALITY TUNING

It’s critical to tune the system using a statistically significant and representative user population as well as an understanding of business risk appetite.

Many factors impact the tuning process, including environmental conditions, population size, demographics, hardware and the biometric modality itself. Unlike PINs and passwords, biometric matching is not binary, but probability-based (see Figure 4).

The performance of a biometric system can be benchmarked, preferably using operational data. Continuous benchmarking and re-tuning are recommended, due to gallery growth and quality distribution. A biometric recognition system with a match threshold set too high will too often falsely reject customers, whereas a threshold set too low will tend toward false acceptance. A well-tuned system is one where security and usability are balanced to meet business objectives.

Figure 4. Biometric Tuning and Benchmarking Thresholds

Source: Accenture, January 2018

FAR: False Acceptance Rate
FRR: False Rejection Rate
An omni-channel, real-time fraud detection and prevention capability adds context and actionable intelligence to a firm’s authentication decisions.

Traditionally, fraud has taken the path of least resistance across banking channels. In the last decade, the online channel was the primary target—resulting in a number of high profile attacks. This led to greater investment in cyber security and a gradual improvement in banks’ security posture—leading fraudsters to focus efforts on the call center or mobile banking channels.

However, in more recent times, full multi-channel attacks have risen to prominence. For example, an attacker can steal login credentials through shoulder-surfing, social media “doxing” or social engineering. Using these credentials, an attacker can gain access to online or telephone banking to set up a new payment recipient before downloading and installing the bank’s mobile app to initiate a payment.

Traditional single-channel fraud detection applications would be useless in this situation, as the events in each channel are not significant enough to suggest fraudulent activity on their own. However, with a cross-channel view, one could easily detect this suspicious activity before automatically triggering a secondary, or step-up authentication prompt to the mobile device initiating the payment. Ideally, this subsequent authentication would prioritize a biometric credential tuned to a low False Acceptance Rate (FAR) to assert, with a high degree of accuracy, that the payment is initiated by a legitimate user (see Figure 5).
In addition to an omni-channel approach, it’s also critical that an effective risk engine take feeds from multiple sources to better understand the risk factors from three key areas:

1. **Contextual device factors, including location information and travel times**

2. **User behavioral factors**

3. **Financial transactional factors**

**Figure 5. Risk Engine Elements for Detecting and Preventing Fraud**

Source: Accenture, January 2018
SIGNING IN THE NEW

The traditional “wet” signature is slow and expensive, and has held back the advancement of integrated, mobile financial services solutions.

The manual, time consuming process of posting contracts to customers and waiting for responses is both tedious and expensive, not only in terms of postage but also through back office operations, scanning and storage of signatures. With even small organizations handling tens of thousands of paper documents each month, moving away from the wet signature can realize significant economies of scale. The authentication hub provides banks with digital alternatives that are legally equivalent to a wet signature, but cheaper and faster.

One option is to replace the wet signature with a digital signature captured either on-screen, on a mobile device or through an electronic signature pad in a branch or kiosk. A more advanced approach is to introduce a solution that is compliant with the EU electronic identification and trust services for electronic transactions (eIDAS) regulation, and which provides a legally equivalent digital alternative to the wet signature. Substantively, the eIDAS regulation consists of two sections.

The first section addresses government-recognized electronic identification systems and establishes a legal framework that will allow all EU member states to mutually recognize each other’s identification systems. This section targets the public sector and requires Member States to permit citizens from other member states to use their own localized electronic IDs to access their online services. Private sector companies are not directly impacted by this portion of eIDAS. However, there are opportunities here to link with public sector services and facilitate cross-border customer migration.

The second section of eIDAS outlines the requirements for electronic signatures. It clarifies existing rules, but also introduces a new legal framework for electronic signatures and seals. While service providers are not obliged to significantly change their way of working, eIDAS does offer incentives to follow European rules (granting greater legal certainty to services that follow eIDAS rules and designed to improve the reliability of these services).
Leveraging an eIDAS-compliant signature service can provide an improved customer experience, but also increased certainty over the validity of both signatures and the integrity of the documents they are attached to—leading to reduced costs and lowered overheads.

With an authentication hub orchestrating the overall business logic, it’s possible for customers to utilize existing authenticators to confirm documents, and for firms to integrate the signing process directly into wider business flows and customer journeys.
There are two conflicting schools of thought concerning the hosting architecture for the feature extraction, template creation, storage and matching processes that underpin any biometric authentication system.

One side argues that biometric matching should be executed within a centralized server environment—where strict security standards can be more easily enforced and monitored, while taking advantage of the vast processing power available (server-side matching). The opposing argument is that biometric data should never leave the end-user device (typically a smartphone)—eliminating the risk of a large-scale data breach and prioritizing user privacy (on-device matching).

There are a number of proponents of the on-device approach, including Apple Inc.—with its provision of Touch ID® and Face ID® on mobile devices and a growing industry body, the Fast Identity Online (FIDO) Alliance. The FIDO Alliance standardizes the authentication protocol used between the client and the online service. The protocol is based on standard public key cryptography, where the client registers a public key with the online service at initial setup. Later, when authenticating, the service verifies that the client owns the private key by asking it to sign a cryptographic challenge. The protocol is designed to enhance user privacy and security in the current state of the internet. FIDO Alliance standards define a common interface at the client for the local authentication method the user exercises. The client can be pre-installed on an operating system or web browser. Different authentication methods, such as secure PINs, biometrics and dedicated hardware devices, can be “plugged in” to the client via this standardized interface.

We understand that this is a developing market with a rapidly changing landscape. Partnering with vendors who appreciate the perspectives from either side allows us to present an unbiased view of the merits and disadvantages of either approach. Ultimately, the deployment of an authentication hub allows for a hybrid approach that may be most suited to the requirements of financial services firms. This is partly due to different modalities carrying different risk profiles and privacy concerns, and that many emerging use cases demand a server-side matching architecture to facilitate one-to-many rather than one-to-one matching—such as mKYC.
**THE ARGUMENTS FOR SERVER-SIDE MATCHING**

- Enrollment and re-enrollment is possible “en masse” using an online database of, for example, photo IDs for facial recognition or voice recordings for voice recognition.

- Server-side matching helps integrate biometrics into the identity storing and KYC processes, permitting one-to-many validation and de-duplication.

- Many established biometrics vendors are incompatible with the FIDO Alliance framework authentication, including BioCatch Ltd. and Nuance Communications, Inc. Additionally, some biometric modalities (such as behavioral) require central matching.

- Significantly greater computational power is available during server-side authentication, which fosters “deep-learning” and advanced behavioral biometrics.

- Older devices are not compatible with FIDO Alliance requirements, e.g. secure elements or hardware acceleration.

- True omni-channel authentication is feasible on the roadmap of a server-side authentication product (e.g. call center to online to mobile).

**THE ARGUMENTS FOR ON-DEVICE MATCHING**

- Captured biometric templates never leave the device, reducing the attack surface area. Attacks designed to breach biometric data on a single device are not scalable to the entire user base.

- Enhanced privacy can lead to greater security and control perceptions among the public. End users can register and revoke biometric modalities at will.

- A modular framework reduces the re-engineering required to add new modalities or support new devices. It also results in lower ongoing costs to develop and enhance the platform to address future needs.

- There is no requirement for organizations to tokenize and manage biometric data for their customers, which is critical in the face of new regulations like the General Data Protection Regulation (GDPR) that punishes the loss of user data.

- There is no need for high-performance back-end infrastructure, as the processing of biometric data is offloaded to end-user devices.

- The authentication customer experience is decoupled from identity and access management back-end systems.
KEY TAKEAWAYS

It’s important to consider the end, not just the means. Firms should define how the use of biometrics helps them achieve their objectives.

We recommend careful consideration regarding integrating multiple modalities, specifically:

• For mKYC or remote account signup implementations, consider how to de-duplicate enrollments to produce a single identity for each individual.

• Evaluate the merits of a server-side versus on-device matching model, or a hybrid of the two. This evaluation should be aligned to the firm’s technology vision, risk appetite, corporate culture and customer experience expectations.

• Define which customer journeys will be supported by biometrics. Are they driven by enhanced security, ease of use or both? We recommend the creation of an omni-channel vision around an authentication hub.

• Deploy a flexible architecture, embedding existing authentication technologies while reducing or eliminating technical debt. This promotes fluidity while facilitating compliance with emerging legislation, such as GDPR, PSD2 and eIDAS. At the same time, the use of pick-and-choose biometric and non-biometric authenticators balances security with the user experience.

• Offer contextual, risk-based and persistent authentication to help reduce fraud and prompt customers for a convenient secondary, or step-up, authentication if an omni-channel risk threshold is breached.

• Reuse authenticators to solve wider business problems, such as document signing, third-party access, customer onboarding and transaction authorization.
References


9. Paraphrase of a quote (“Figures do not lie, but liars do figure.”) attributed to Mark Twain. Handbook of Biometric Anti-Spoofing, Trusted Biometrics under Spoofing Attacks,” Sébastien Marcel, Mark S. Nixon, Stan Z. Li, Springer 2014. Access at: https://books.google.co.uk/books?id=Go4kBAAAMBAJ&pg=PA35&lpg=PA35&dq=%22Fingerprints+cannot+lie,+but+liars+can+make+fingerprint%22&source=bl&ots=w_Ib5PFXHN&sig=K-qZhCRhRb-QePR0gKIHltGArl&hl=en&sa=X&ved=0ahUKEwjoy67tnubXAhXBmBoKHdJWDAo0Q6AEIUzAL#v=onepage&q=%22Fingerprints%20cannot%20lie%2C%20but%20liars%20can%20make%20fingerprint%22&f=false


11. Ibid


13. Ibid
ABOUT THE AUTHORS

Christine Leong

Christine Leong, Managing Director, Accenture Security. Based in Houston, Christine leads Accenture’s Digital Identity Innovations efforts globally and she also leads Accenture’s Blockchain Identity offerings. She has over 18 years of experience in digital identity & biometrics. Previous to her IT roles, she worked for over 9 years in financial services. Her security relevant experience and knowledge spans: biometrics, payments & fraud, digital identity, blockchain and authentication. She is a regular speaker at conferences globally and has published articles on identity & blockchain. Christine has an MA in Politics, Philosophy & Economics from Oxford University. In a past life Christine volunteered for a dog shelter and currently owns 3 dogs with a combined weight 3 times her own.

Daniel Bachenheimer

Dan Bachenheimer, Principal Director, Accenture Security. Based in Washington D.C., Dan is an electrical engineer with extensive experience analyzing, designing, and delivering technology solutions to meet disparate mission objectives. From large scale identity management systems to air traffic control solutions to firearms and tool mark identification, Dan has been designing and delivering solutions to drive business success. During the past 15 plus years, his focus has been on identity-related efforts, including biometrics, working on border, policing, and identity management solutions across the globe. With these global obligations related to biometric recognition solutions, Dan is no stranger to the challenges of husband recognition.
Dan Preston
Dan Preston, Manager, Accenture Financial Services Technology Advisory. Based in London, Dan brings over 10 years of experience to Accenture and its clients. In his current role, Dan leads a team focused on helping Accenture’s financial services clients navigate complex cyber security and regulatory challenges. Specialized in authentication and biometrics, Dan is also a brand-new father of one, presently focused on helping his son understand the subtle difference between night and day.

James Alexander
James Alexander, Manager, Accenture Financial Services Technology Advisory. Based in Manchester, James works with financial services clients across Europe to answer the challenges presented by digital identity, increasing regulation and customer demands for ever more streamlined digital experiences. James works with multifactor authentication technologies, and in particular biometrics. James has a PhD in security technology from the University of Manchester. When not working, James can usually be found at the side of the road, having broken down in another wildly unsuitable car purchase.
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 435,000 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.

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.