accenture

consulting | technology | outsourcing

The future of identity in banking

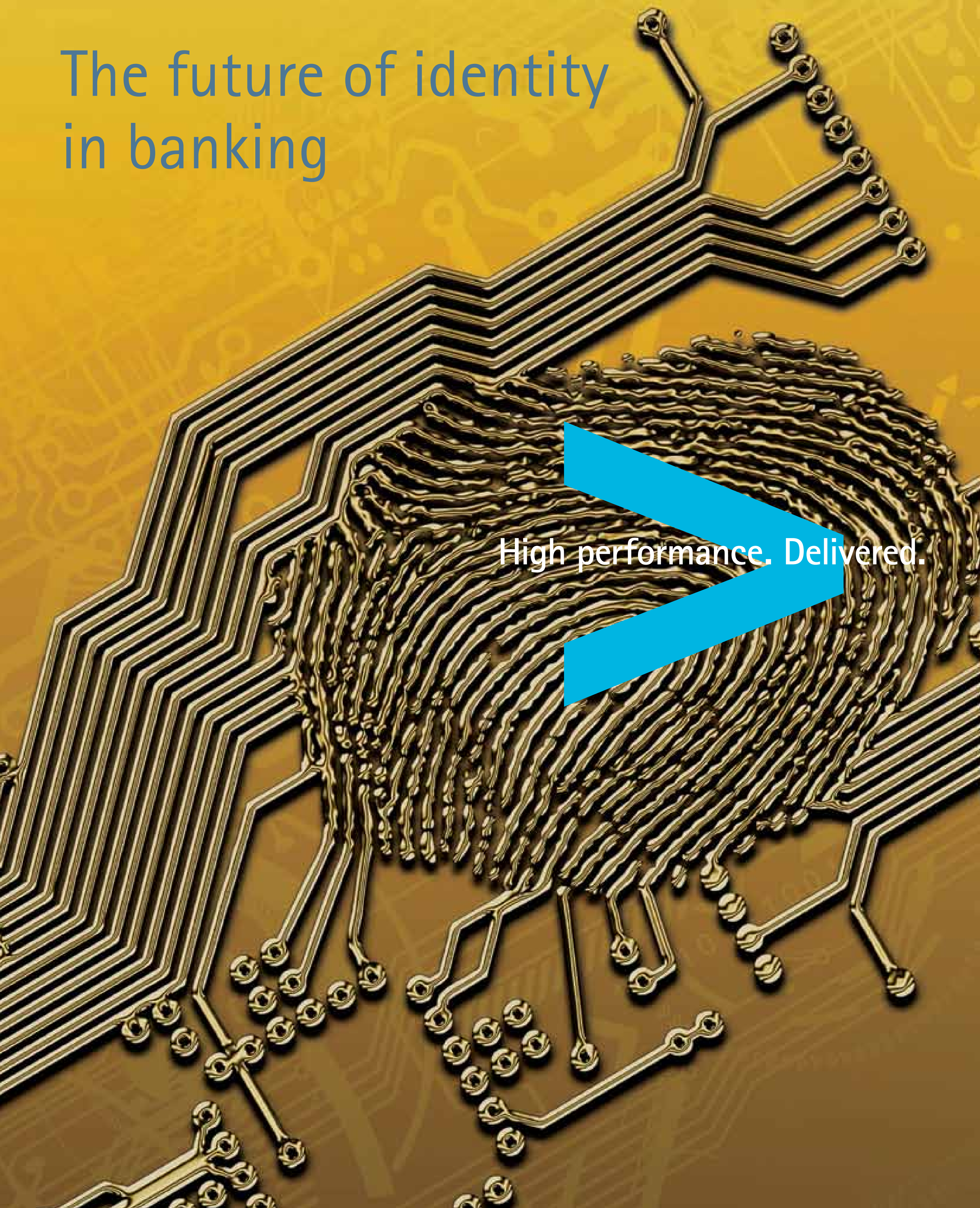


Table of contents

Quick question. Which organizations are the biggest buyers of identity management technology and services? If you answered central government or police agencies, you'd be wrong. Now spending over US$1 billion a year on identity management solutions, banks have been the leading investors in identity management solutions for decades[1].

This reflects the pivotal role of identity authentication in the financial services industry, where the ability to establish and verify the identities of customers and employees is fundamental to maintaining customer trust, as well as the security of transactions.

Now, however, rapid growth in digitization, new technologies and new user behaviors are revolutionizing the ways in which banks interact with their customers and employees and, in the process, changing identity management obligations forever. As a result, banks are starting to re-evaluate their role in the identity supply chain.

At a time when industry convergence and disruptive innovation around payments and commercial services are so intense, this is a high priority. By capitalizing on their investments and experience in this area, banks recognize that identity can be about much more than security alone. Crucially, financial sector organizations in some countries are seizing far broader business benefits by exploiting new identity sources, biometrics and advanced analytics technologies to increase customer insight and service relevance, while reducing fraud, waste and abuse.

Banks in the United States and Europe are, however, lagging behind. Few of the major players there have adopted biometrics to a significant degree, with the market preferring to wait for a first mover to legitimize the technology. As we show later in this paper, that first mover may well have arrived (with Apple's 2012 acquisition of Authentec).

Balancing the identity management equation

Irrespective of these wider developments, security remains a vital concern for banks. Digital banking is on the increase—and so are the vulnerabilities that it creates. In most mature market countries over 50 percent of customers are signed up for online banking[2] and at least 25 percent of respondents to the 2012 Norton Cybercrime Report[3] regularly access their bank accounts online. The same report showed that over 40 percent of online consumers either use weak passwords and/or are not changing their passwords regularly enough. And perhaps most significantly of all, consumers are failing to recognize how cybercrime is evolving to target mobile platforms and networks. This means cyber attacks—ranging from sophisticated techniques to simple social engineering—are an ever-present threat for banks and their customers.

But protecting against these attacks is just one part of the identity management equation. In a digital world, with data surging in volume and velocity, and customers accessing financial services from multiple platforms, identities are becoming increasingly complex and expensive to manage. To put this in perspective, identity and access management now represent 30 percent or more of a large financial institution's total information security budget[4]. And the costs are rising all the time.

How to balance the need for vigilant, active cyber defense with the pressure to achieve greater operational efficiencies and drive additional business benefits from the massive investments that are being made in this area? We believe the answer lies in banks moving decisively to build on their already strong identity management capabilities. As this point of view explains, this means taking advantage of the stronger and more efficient identity management systems that are now available—systems that can deliver what we term "Unique Identity".

Accenture is already proving the value of Unique Identity in some of the world's largest identity management schemes. Highlighted later in this point of view (see "Why Accenture"), these use cases show how Unique Identity can be used to enhance security and boost efficiency, while simultaneously increasing user satisfaction and improving service levels.

What is Unique Identity.... and why is it so valuable?

Mandated by the regulators[5], and motivated by best practice, banks have been offering multi-layered authentication for years. Until very recently, this has been achieved through username and password recognition schemes.

Though relatively cheap and straightforward to implement, these approaches are inherently insecure as a means of authenticating user identities. Based on an "all or nothing" approach, they afford no protection once they have been compromised—a risk that is exacerbated when so many consumers write down their PINs and passwords and/or use the same ones across multiple environments, from online transactions, to ATMs and call-center conversations.

As well as being vulnerable to security breaches, challenge/response authentication methods are inefficient. Because personal identifiers such as PINs and security codes are so easily forgotten, up to 30 percent of all support calls to banks' call centers are password reset requests. Handling each one costs an average US$25 in labor costs[6].

Nor do the weaknesses end there. These approaches also fuel customer frustration—a major concern when banks are striving to differentiate their operations through improved customer service. Results from a recent survey by the Ponemon Institute[7] put this into perspective. Canvassing the views of consumers in the United States, UK and Germany, this found that 70 percent of respondents in the US and UK are dissatisfied with password-controlled access, and over 80 percent want to see better authentication being deployed.

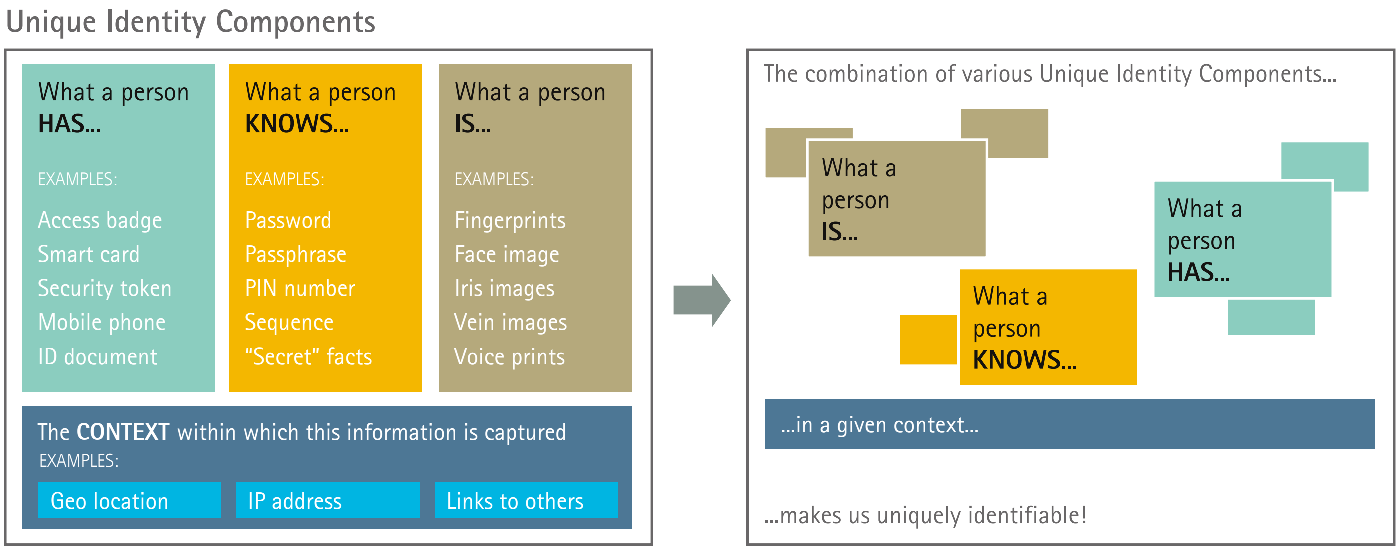
With customer interactions now spanning physical, online, social and mobile channels, banks urgently need new capabilities that will enable seamless, holistic and robust identity recognition over time, and across all encounters. This is driving the adoption of Unique Identity systems.

Traditional identity management systems have been built around the least volatile types of user information (such as biographic details and PINs). Unique Identity systems are different. Based on a process of continuous enrolment and vetting, they use accurate and flexible capabilities to establish a single identity for each individual based on:

- What the customer knows (password, PIN, security code)
- What the customer has (identity card, bank card)
- Who the customer is (biometrics spanning physical/behavioural features)
- Where the customer is (mobile number, geo-location, IP address, social network site)

Shown in Figure 1, Unique Identity is the collection of data that, taken together, uniquely describes an individual. As the foundation of trust for everyday interactions, it exploits new identity sources and analytics technologies during enrolment and authentication to increase insight and service relevance, while reducing fraud, waste and abuse.

FIGURE 1. What is Unique Identity?



The time is right

Three trends are combining to make effective Unique Identity more achievable than ever before:

1. Continually improving biometric recognition technologies and products

Multiple biometric modalities are now on the market at accessible prices. Enabling automated recognition of individuals based on their physiological and/or behavioral characteristics, these range from "harder" biometrics (such as fingerprint, vein and iris recognition) to "softer" modalities (including face, voice, keystroke and signature recognition). As the sophistication of these technologies rises, and the cost of implementing them continues to fall, the number of deployed biometrics solutions is growing fast. Valued at US$5 billion in 2010, the global biometrics market is growing at a CAGR of 18.5 percent, and is predicted to reach US$17 billion by 2017[8].

2. Increasing public acceptance of enabling technologies

Provided that banks take proactive steps to address concerns about privacy[9], they can expect most of their customers to be enthusiastic about the introduction of biometrics modalities. In a 2011 Twitter survey by Nuance Communications[10], 77 percent of participants said they would be comfortable using voice biometrics if it meant tighter security. Another poll by Unisys indicated a 72 percent acceptance rate for banking biometrics amongst customers; the findings showed that they trust fingerprint biometrics over photo identification, PINs, or handwritten signatures to verify their identities when using credit cards, or requesting personal information[11].

3. Availability of "Unique Identity as a Service"

Banks can now opt for flexible, scalable and easy-to-integrate identity capabilities, with Unique Identity solutions available "as-a-Service", delivered on-demand via private or public cloud infrastructures, tailored to specific needs and consistent with local privacy requirements (see "Why Accenture").

Now is the time to act. And in doing so, banks will be able to leverage the high level of trust already placed in them by their customers (underlined in the recent Ponemon survey, where banks stood out as the most trusted organizations across all sectors for the quality of their online validation[12]).

In the following section, we present some of the broader business benefits provided by Unique Identity, before highlighting the ways in which banks are applying these solutions to transform their identity management capabilities.

Reaping business benefits from Unique Identity

Identity used to be all about security. Now it has evolved to the point where, properly implemented, it can bring a broad set of business benefits to banks. These benefits are particularly timely in an environment where the identity requirements (such as "Know Your Customer" and identity verification) being imposed on the industry are increasingly onerous—from a bank and customer perspective.

By helping customers to assert their identities more conveniently and more securely, Unique Identity can:

- **Drive efficiency improvements** by speeding identity recognition, and automating processes that currently require human supervision. For example, banks can accelerate client onboarding by capturing biometric identity documents (such as face and voice recognition) in the branch when starting a client contact. For all subsequent branch interactions, some or all of these biometrics can be used to painlessly authenticate the customer.
- **Enhance the end-user experience** through faster, more transparent identity recognition, and through improved personalization. For example, when a customer calls the bank from their mobile, the Unique Identity system uses contextual information (such as caller identity) and voice biometrics to strengthen authentication and reduce the burden on the customer to explicitly prove their identity. Or in another situation, where customers use their tablets for online shopping, instead of being redirected to a verification site, they are instantly authenticated through a combination of home IP address, device identity and face recognition (via the tablet's camera).
- **Improve resistance to fraud and abuse** by assuring that users are genuine, and entitled to the services they are claiming. Examples include customers presenting their biometric identifier (finger, hand, etc.) at the automatic teller machine (ATM) or point of sale. Now commonplace in some countries, notably Japan, where vein recognition technologies are widely used in ATMs (see section below "Unique Identity in practice"), this enables customers to be instantly recognized and authenticated before a transaction is processed.
- **Promote inclusion by helping customers** in emerging economies—where people often lack the necessary identity documentation and/or access to bank branches—to conveniently assert their own identities (through fingerprint recognition, for example) and/or take advantage of new channels such as branchless banking and mobile payment solutions.

Unique Identity in practice

Many banks are already realizing powerful benefits from Unique Identity solutions. Some of the most common use cases include:

ATMs

The use of biometrics at ATMs to improve ease of use and limit fraud is already widespread. Fingerprint, finger-vein and palm-vein readers, the most commonly deployed solutions, are relatively easy to integrate into existing authentication paths. These can be particularly valuable in emerging market situations, promoting financial inclusion in areas where customers may be less financially literate. In Nigeria, for example, the government recently launched a landmark pilot program, rolling out 13 million MasterCard-branded national identity smart cards with biometric and electronic payment capabilities[13]. As well as using the cards to withdraw cash from ATMs, cardholders can deposit funds on the card, receive social benefits, and pay for goods and services. Meanwhile Mexico's Banco Azteca has been using picture- and fingerprint-based payment systems to promote financial inclusion for unbanked customers. Examples in developed markets include Japan's Mizuho Bank and Bank of Tokyo-Mitsubishi, which have, respectively, deployed finger-vein and palm-vein ATMs to provide more secure authentication and combat fraud, and BPS Bank in Poland, the first bank in Europe to secure its ATMs with biometrics based on finger-vein technology, in addition to PIN codes. Elsewhere, in Brazil, Bradesco Banco was the first bank in the western hemisphere to use biometrics as a means of identification at ATMs, installing palm vein technology on 20,000 of its ATMs.

Call centers/phone banking

Consumers typically favor voice recognition over all other types of biometrics[14], and this modality has already been widely adopted by banks. Solutions include customer authentication technologies for call centers, as well as interactive voice technologies allowing customers to access a bank's database via telephone keypad or by speech recognition (expediting interactions including balance enquiries, credit card payments, changes to PIN codes and payments to third parties). In one recent example, Barclays Wealth & Investment Management deployed a voice biometrics solution to securely and automatically confirm customers' identities[15]. The technology compares the customer's voice to their unique voiceprint on file, silently signalling the operator once the identity has been verified. Since deployment began, customer feedback has improved significantly, with 93 percent of customers ranking the bank nine out of 10 for speed, ease of use and security. Other examples include one of Australia' largest retail banks, which has improved security and customer satisfaction by rolling out voice biometrics to all personal banking customers; it is also planning to use mood detection technologies to enable angry customers to be handled more quickly. Outside the financial sector, voice biometrics technologies are increasingly being deployed by telecommunications companies to improve customer satisfaction and prevent fraud. A number of clients are considering deployment of voice biometrics to help their customer care agents enforce Unique Identity amongst customers, as well as establishing "voice watchlists" of known fraudulent customers. This can reduce financial losses from social engineering and customer identity fraud, as well as improving efficiencies through call time reduction and streamlining authentication processes.

Customer onboarding

We are seeing more banks use biometric technologies to capture Unique Identities at contact initiation. In countries where governments are launching national identity schemes, banks can use the identity credentials held on identity cards to accelerate onboarding, as well as providing strong authentication for customer transactions. In Malaysia, for example, the government's national identity scheme gives each citizen a biometric smartcard, MyKad, a multi-functional card that can be used for identity verification, remote access to public services, low-value payments and automatic ticketing. One Malaysian bank, Easy by RHB, uses MyKad readers and a paperless account opening process to enable its customers to open new accounts in just 10 minutes.

Mobile-enabled solutions

Mobile banking solutions are increasingly in demand (according to Juniper Research, there will be over 1 billion mobile banking customers by 2017[16]). However, because mobile security in most financial institutions is still far behind the solutions that have been developed to prevent and mitigate PC-based attacks, mobile transactions are particularly vulnerable to cyber attack. To address this situation, smartphone and tablet applications are being developed that use voice biometrics as part of a multifactor authentication process for secure mobile banking. In one recent deployment, a top-three global US financial institution launched a voice biometric application simultaneously in 40 countries[17]. The first voice biometric application to have obtained global regulatory approval, this uses voice biometrics as part of a multifactor authentication process for securing commercial banking automated clearing house (ACH) payments and wire transfers.

Online/desktop verification

Technologies in this area are moving on from at-home readers to biometrics techniques, including fingerprint recognition (via biometrics readers, such as those integrated into some laptops and smartphones, or distributed by the banks), face recognition (via webcam) and keystroke dynamics. Fingerprint recognition technologies are already widely used by banks. United Bankers Bank, for example, has eliminated password sharing by enabling bank clients to log in using fingerprints instead of passwords and PIN codes The Los Angeles Firemen's Credit Union is another. Instead of having to remember up to 10 different passwords, employees of this institution now use a biometric fingerprint access system for single sign-on to all systems. Over time, we expect to see banks achieving online verification through a combination of "weaker" biometrics (voice, face, keystroke authentication) and contextual information (geo-location, device identification)—all of which can be captured without the need for any additional hardware.

Merchant payments

The ability to pay using biometrics (where customers are enrolled into the system, put credit into their account using kiosks and credit cards, and pay using their fingers) is gaining in popularity. Biometric payments bring added flexibility and speed to customers, increase customer loyalty to the merchant, and boost transaction flow for the bank. Biometric payment systems have been successfully used in Europe for years. And momentum is building in the US market. Seven thousand shops there already offer these systems to around two million customers—a trend that many commentators believe will gain rapidly in momentum following Apple's 2012 acquisition of Authentec, a company specializing in fingerprint scanning technology. More widely predicted to be the "first mover" moment that will legitimize more widespread adoption of biometrics by US banks. Designed to work with near-field communication (NFC) technology, Authentec's solution allows users to unlock their phones and turn on the NFC transmitter with a single swipe of the finger across the smart sensor. Payment is made by tapping the phone on the point-of-sale (PoS) terminal. Meanwhile, in France, a group of banks, IT firms and retailers has trialed a point-of-sale system that combines fingertip biometric readers with contactless cards. Developed by Natural Security—a biometrics specialist owned by banks, retailers and Ingenico—the system was piloted for six months by a group of banks including Banque Accord, BNP Paribas, and Crédit Agricole. In another example, Italian bank UniCredit has market tested a new biometric payment system using infrared sensors at PoS terminals to recognize the geometry of veins in users' palms. Sensors capture the image created by hemoglobin when struck by an electromagnetic impulse and translate that information into a unique numeric code.

Beside the business benefits banks are already realizing from Unique Identity solutions, there are real opportunities to generate additional returns on their investments in biometric technologies. Examples include Citigroup leveraging its advanced capabilities in identity verification to provide the US Department of Defense with a secure travel card solution, and Royal Bank of Scotland's TrustAssured which provides registration, certification and validation services to corporate clients as a managed identify service.

Why Accenture?

As a leader in biometrics technologies, Accenture has helped banks and other organizations to deploy a wide range of Unique Identity solutions, increasing security, driving efficiencies and delivering targeted business benefits.

We have an unsurpassed track record in delivering the largest identity management systems in the world, including US-VISIT, UID of India, and EU BMS. Key facts about each of these landmark solutions are shown in the sidebar on page 16.

We have also developed a range of proprietary solutions, assets and tools in this area. These include:

Unique Identity as a Service

Provided through our Unique Identity Service Platform (UISP), this is our primary offering, with a design grounded in Accenture's more than ten years' experience in delivering identity solutions to clients worldwide. It draws on the latest thought leadership to implement Emergent Identity—the progressive enriching of knowledge about an individual's identity as it evolves over time. Offering flexible, scalable and easy-to-integrate identity capabilities, it helps our clients to resolve identities across multiple encounters and systems. Customized to the financial services industry, UISP can be used wherever there is a requirement for Unique Identity solutions—either as a deployed solution, or "as-a-Service", on demand via private or public cloud infrastructures (according to client needs and consistent with local privacy requirements)

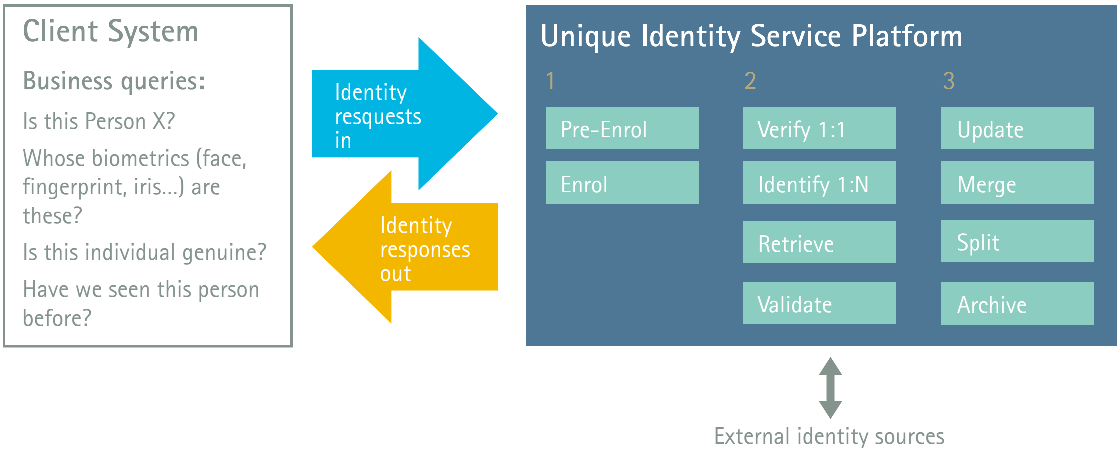
Proprietary solutions for banks

Our Unique Identity solutions include an intuitive and rapid enrollment process (capturing biographic information, identity documents, ICAO-compliant facial images, fingerprint, iris and digital signatures). UISP is designed for easy integration with PoS and merchant facilities to create an end-to-end secure payment solution.

Continuous investment in innovation

We are committed to investing in innovation through Accenture Technology Labs, our global network of dedicated research and development organizations. This commitment has seen us turning technology innovation into business results for over 20 years. We also have a dedicated Unique Identity technology group that specializes in prototyping and developing identity solutions, and a Unique Identity Community of Practice numbering over 200 members.

FIGURE 2. Accenture's Unique Identity Services


Client System
Business queries:
Is this Person X?
Whose biometrics (face, fingerprint, iris...) are these?
Is this individual genuine?
Have we seen this person before?
Identity resquests in
Identity responses out
Unique Identity Service Platform
1
2
3
Pre-Enrol
Enrol
Verify 1:1
Identify 1:N
Retrieve
Validate
Update
Merge
Split
Archive
External identity sources

Accenture's Background in Unique Identity

Accenture is unique in having delivered the largest Identity Management systems in the world, including US-VISIT, UID of India, and EU BMS.

European Commission

Biometric Matching System

- European Commission's general purpose multimodal biometric matching system
- First implementation is to support the introduction of biometric visas in Europe
- Implemented over a 3 year period starting in 2007

OUTCOMES:

Now used live by 27 countries, 3500 consulates and over 10,000 border posts worldwide.

On the way to containing 70 millions records, designed to accommodate over 100,000 transactions per day.

Unique Identification Authority of India

Unique ID Program

- Ability to scale to 1.2 billion Indian residents
- Solution is an open multi-modal biometric architecture with high efficiency and reduced vendor lock-in
- Defining the best practices for biometric capture

OUTCOMES:

Largest biometric storage with 10 fingerprints (4-4-2), two iris images, one face image and demographics.

376 million enrollments since deployment.

False acceptance rate < 0.04%. False reject rate < 0.06%.

US Department of Homeland Security (DHS)

US Visitor and Immigrant Status Indicator Technology (US-VISIT) Program

- Accenture helped create and deliver a world class program—US-VISIT
- US-VISIT biometric entry procedures
  - 115 airports, 15 seaports and in secondary inspection areas of 154 land ports of entry
- US-VISIT exit procedures are operating at 12 airports and 2 seaports

OUTCOMES:

World class scale: 140+ million people.

World class speed: 400,000 transactions/day.

329M transactions processed (over 135,000 wanted criminals identified).

UK BA, BAA—London Heathrow Airport

Self-Clearance for EU ePassport Holders

- Introduced automated e-Passports gates at Heathrow and Stansted Airport
- Both airports represent 54% of all incoming passenger traffic to the UK
- Featuring advanced anti-tailgating solution (single gate with detection portal)

OUTCOMES:

Highly-positive passenger experience and feedback.

Over 7 million transactions since deployment in 2010.

Transaction time < 10 seconds.

100111010
0100110011110
1110100110010
0011001110101000
0101001100111 010
0111101001100101
1001100111010100
1010100110011110
0111101001100101
100110011110
01001100

Find out more

If you would like to know more about Accenture's leadership in Unique Identity, and the benefits this can bring to your business, please contact:

Alastair Partington CBP
Unique Identity Lead—Emerging Technologies Innovation
Accenture (UK) Ltd
alastair.partington@accenture.com

Anton Pichler
Banking Research Director
Accenture (UK) Ltd
anton.l.pichler@accenture.com

End notes

1 See www.banktech.com/risk-management/tipping-point/229625350

2 Eurostat, National Statistics Agencies

3 See http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

4 www.banktech.com/risk-management/tipping-point/229625350

5 See Federal Financial Institutions Examination Council (FFIEC) guidelines

6 See www.networkworld.com

7 http://www.bankinfosecurity.com/users-want-new-forms-authentication-a-5692

8 TechSci Research, "Global Biometric Systems Market Forecast & Opportunities, 2017," July 2012

9 See www.accenture.com/gb-en/Pages/service-biometrics-privacy-positive-match.aspx

10 See www.nuance.com

11 See www.planetbiometrics.com/article-details/i/310/

12 http://www.bankinfosecurity.com/users-want-new-forms-authentication-a-5692

13 See www.finextra.com/News/FullStory.aspx?newsitemid=24801

14 http://www.bankinfosecurity.com/users-want-new-forms-authentication-a-5692

15 See www.finextra.com/News/FullStory.aspx?newsitemid=24800

16 See www.juniperresearch.com/view-pressrelease.php?pr=377

17 www.businesswire.com/news/home/20130416006470/en/VoiceVault-voice-biometric-financial-services-mobile-app

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 275,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$28.6 billion for the fiscal year ended Aug. 31, 2013. Its home page is www.accenture.com.