Verifying that someone is who they claim to be is a perennial challenge for banks. It spans the whole banking spectrum, from private banks seeking to avoid money laundering, to retail banks guarding against identity theft, to institutions servicing the unbanked who have no record of their identity. Biometrics has already gone a long way to solving this problem. Through fingerprint authentication, banks can establish and verify a customer’s identity, unequivocally. This overcomes issues of forgery and impersonation, greatly enhancing security, while decreasing costs.

Now, as banks transform from being branch-focused to becoming digital organisations, biometrics will have an increasingly large role to play.

**Photo ID obsolete**

As banks move away from having a physical presence, paper-based forms of identification, such as photo ID and signatures, are losing primacy. This is good news from a security point of view, owing to the notorious unreliability of these forms of evidence. It also removes the onus from staff to visually match up sets of signatures or a face with a photo. Instead, they are being replaced by a variety of truly unique biometric identifiers.

**Biometric enrolment**

During the enrolment process at a bank, customers simply touch a fingerprint scanner. Quality scanners capture complete images and create minutiae templates that are one-of-a-kind, unique identifiers. Combined with demographic data, biometrics create a complete identity file for each customer. When customers access funds or services, they scan a finger and the authentication system compares the scanned template to the stored templates. Unlike relying on photo ID, fingerprint identification ensures that multiple identities cannot be created for the same person.

Employees of banks and other financial institutions can follow a similar process when logging onto systems, accessing secure assets or clocking in at work. Instead of typing in a user ID and password, a finger scan verifies their identity and security levels, providing fast access to applications, systems and networks. Employee biometrics templates are linked with their credentials account (usually based on Microsoft Active directory, a special-purpose database).

For both customer and employee activity, access is only granted when the scanned biometric matches the information stored in the individual’s secure identity file. Suspicious activity is automatically flagged and detailed in management reports, which can be delivered individually in real-time, or as part of an aggregate report.

**More than fingerprints**

Fingerprint scanning is the most common form of biometric identification. It has been used for many years, and relies on the uniqueness of each person’s fingerprints. Contrary to a common assumption, however, the actual fingerprint image is not stored in the database. Instead, a mathematical representation of the fingerprint, known as a template, is stored, making it very difficult to compromise the fingerprint data. Creating templates from multiple fingers can also result in a more secure system, and improve access for the broadest range of customers.

Indeed, as Mexico-based Banco Azteca discovered, fingerprints are not always straightforward to obtain. A high proportion of its customers are from poor rural communities, working as farmers or labourers, and often their fingers are damaged or worn. Consequently, a fingerprinting solution had to be developed that was sophisticated enough to image and authenticate these difficult-to-read fingerprints.

As a further level of security, mechanisms have been developed that can identify whether blood is flowing through the finger at the moment of authentication. This, of course, ensures that the finger belongs to a live human, countering concerns that it’s theoretically possible to fake fingerprint biometrics.

Fingerprints are just one of a many unique human identifiers, and further technological advances are allowing banks to use other measurements to verify identity. These include iris, facial, and finger-vein scanning, and voice recognition. Finger-vein scanning is an interesting twist on fingerprinting, where the tip of the finger is also scanned, but the patterns of the veins beneath the skin’s surface are recorded instead. Blood vessel patterns are unique to each person, and are more challenging to counterfeit, as the ID scanner can only authenticate the finger of a living person.

---

VIEWPOINT: Vinod Raghavan, Security Architect, Temenos

*Branch transformation: biometrics in ATM and mobile banking*

---

“...as banks transform from being branch-focused to becoming digital organisations, biometrics will have an increasingly large role to play.”

Vinod Raghavan, Security Architect, Temenos
Biometrics for ATMs

The potential for biometrics in banking is vast. As Michel Nerrant, of Crossmatch, a fingerprint biometric solution provider, observes, “with one fingerprint you can do so many things in so many contexts with both small and large banks.”

Biometric authentication can be used in two key channels – ATMs and mobile banking. ATMs can be fitted with fingerprint readers where customers can identify themselves and complete basic banking ATM transactions, including reviewing their balance, withdrawing cash or purchasing mobile phone pre-paid minutes. Several countries around the world are already using biometrics-enabled ATMs. Japan has been an early adopter of this technology, deploying it widely, with more than 80,000 biometrics-enabled ATMs in the country and more than 15 million customers using them.

Chip and pin-based ATM authentication presents security exposures. Biometrics provides the proof of identity lacking from using a payment card alone. Customer identification at the ATM can be achieved solely through biometrics, or in conjunction with the payment card, as a second form of authentication. In some countries, the biometrics templates are stored on the card itself. In this case a biometrics match-on-card can be performed, providing the bank with a multifactor authentication method: “what you have” (the card), “who you are” (the biometrics), and even “what you know”, if the PIN is used. No matter the number of authentication methods used, the outcome is positive for both the customer and the bank, by providing ease of use, speed, and simplicity to the customer, and additional security to the bank.

Biometrics for mobile banking

Similarly, biometric authentication for mobile banking greatly enhances internet security, eliminating vulnerable passwords, and dramatically decreasing the possibility of identity theft. Fingerprint authentication is already used in-branch at many large banks, including Bank of America, where customers authorise transactions by placing a finger on a fingerprint reader, which matches the fingerprint to one stored in the bank’s databases. This decreases both the possibility of financial fraud and the time taken to process transactions.

Mobile biometric authentication can be applied in a variety of ways. A huge development in biometric mobility was Apple’s decision to make its fingerprint scanning technology, Touch ID, available to banks, retailers and any other companies that develop apps for its hand-held devices.

There have been several adopters of this new technology. For example, Canadian digital bank, Tangerine (a revamped ING Direct), has an iTunes mobile app that allows users to log in using their fingerprint. Once identified, clients can ask questions and issue commands with their voices, including requesting balances and transaction details, ordering money transfers and paying bills. Tangerine anticipates allowing users to log into the app using voice verification. Combining authentication and command in a single customer prompt has exciting implications, both in terms of decreasing the number of input methods required from the customer, and increasing the ways that their biometric information can be used.

Layered authentication

Part of biometrics’ appeal within mobile banking is its contribution to layered authentication. With internet banking, this has traditionally involved the user entering a password, plus an additional form of personal information, such as a social security number or mother’s maiden name, or a code from a security token. However, static identifiers are vulnerable to discovery and security tokens can be lost. Mobile banking has often had a slow take up, due to a perception that the devices used are not secure. It is somewhat ironic, therefore, that using biometric identifiers as part of layered authentication on a mobile device actually results in a more secure connection than through internet banking.

Serving the wealthy – and the unbanked

A key benefit of biometrics is that it greatly enhances convenience. This is likely to be very appealing within private wealth management, where the speed of identification will assist in creating a VIP service for the wealthy.

At the other end of the scale, biometric authentication is also ideally suited to a very large demographic that has no access to traditional banking services – the world’s 2.5 billion unbanked. While this demographic present an incredible opportunity for financial institutions, until recently, they have been seen as unbankable, being unable to comply with the identification requirements posed by most financial institutions. In fact, about 60% of the world’s citizens do not have national ID cards, passports, driver’s licences or other government-issued identity credentials. Distance from banking locations and illiteracy have also been strongly-inhibiting factors.

Keeping microfinance overheads low

However, microfinancing organisations are dealing with this by keeping overheads to a minimum, through moving away from the branch-based model. Instead, they are opening low-cost kiosks at multiple locations, greatly improving customer access. Customers can visit these contact points and register for basic banking services. And biometrics is an ideal method of capturing their information, solving the issues of a lack of proof of identification.

As well as operating through kiosks, some banks have given customers mobile fingerprint
readers, allowing them to take advantage of secure internet banking for many of the same transactions, including transferring funds to other financial institutions.

Here, biometrics becomes a double winner, both providing a solution to the ID issue, and offering a far more secure form of verification than existing methods.

Emerging market governments are also seeing the benefits. Offering access to banking services is seen as positive, since it strengthens the economies. Accordingly, governments are partnering with banks, supplying them with biometrics-based identity files already created for purposes such as national ID, benefits delivery, healthcare access or travel documents.

Achieving true mobility

Using the model of multiple, low-cost access points and biometric authentication, microfinancing institutions have already reached almost 150 million of the world’s unbanked. But, for this to be achievable on a greater scale, banks need to exploit the full capabilities of biometrics.

All of the above methods of recording biometric data rely on the customer initially making a visit to a branch for their measurements to be captured. But how about when no branch is available? It's hugely beneficial that biometric data is a unique part of each individual, but for this benefit to be realised, it needs to be truly mobile and not tied to a branch.

A few, highly innovative institutions have taken biometrics a step further by taking it out of the branch. Employees of these banks already use their iPads to make loans and sell goods. When they're visiting remote villages to enrol new customers, they're also using them to capture biometric data.

Biometrics has a bright future in microfinance, for financial institutions and unserved customers alike. Financial institutions get access to large numbers of new customers, while the unbanked get access to financial products and services previously not afforded them. From an institutional perspective, biometrics allow for the creation of a trusted identity file. Biometrics-based solutions are also cost-effective, being less expensive than issuing and managing smart cards or other tokens to widespread populations.

Future potential

So far, biometrics take-up has been higher in smaller banks with the agility to introduce new authentication systems. But, with security and compliance top of mind for banks of all sizes, the impetus for developing a more secure identification process is high. With all the positives that biometrics offers, as well as the recent technology advances, it won't be long before large incumbents adopt this very secure, highly mobile form of authentication.

Vinod Raghavan is Security Architect at Temenos. To discuss any aspect of this viewpoint or to arrange a meeting please contact sales@temenos.com

Michel Nerrant is Business Development Manager at Crossmatch, a Temenos complementary solution provider, specialising in biometric products. To discuss further please contact michel.nerrant@crossmatch.com

www.temenos.com