WHITE PAPER

Biometrics at the ATM

Improving the User Experience — While Ensuring Transactions are Trusted and Secure

Executive Overview

In the quest to secure our identity in an increasingly connected digital world, biometrics is flourishing throughout the worldwide banking infrastructure. In many banking services markets, biometrics is successfully authenticating millions of users at the ATM while improving the user experience, increasing transaction security and delivering trust in transactions. Accelerated adoption of biometric authentication at the ATM and related banking solutions (such as securing government pension payments, teller transactions and the opening of new accounts) is in large measure because biometrics is the only authentication method that “binds” a user’s digital credentials to a person. As such, biometrics is playing an important role in eliminating digital identity theft in today’s increasingly complex and vulnerable environment.

Increasing security can create barriers to legitimate access. But biometrics can bring security and convenience together, simplifying authentication while making it more robust and reliable. The technology has now advanced to the point that today’s fingerprint sensors can distinguish between legitimate and counterfeit biometric characteristics, a capability known as liveness detection. Another innovation allows the deployment of intelligent encryption-enabled and tamper-resistant fingerprint devices that further strengthen secure authentication and protect user privacy.

Biometrics authentication will only grow in importance moving forward. We live in an environment where each of us has a growing list of digital identities for an expanding set of applications, stored on a variety of ID cards, tokens, smartphones and other mobile smart devices. Again, biometrics has the unique ability to bind this multitude of digital identities to an individual’s single, true identity. The challenge is how to verify this true identity in a manner that is private, secure and non-intrusive. Biometric authentication solves this challenge, creating a more satisfying and convenient user experience while ensuring that transactions are trusted and secure.

The Challenge of Authentication at the ATM

ATMs in the U.S. and other parts of the world have generally validated the identity of bank customers with something the user has (a card) and something the user knows (a PIN). This decades-old approach is increasingly vulnerable to fraud from a variety of methods. Worse, there are a growing set of digital credentials and identities being stored on ID cards, tokens and smart devices. Without biometrics, these digital identities are not securely bound to the actual person. Additionally, every new digital identity that is created represents yet another element to manage and, as such, becomes a threat to an individual’s one, true identity.

The banking industry continues to look at a number of measures to shore up security, and some measures, such as EMV cards, do address some aspects of the fraud problem. But only biometrics can answer the question of “who” is actually transacting, and determine whether it is a legitimate bank customer or a fraudster. When a biometric solution includes the ability to distinguish live fingerprints from fakes through liveness detection, concerns about loss of user privacy and identity fraud are assuaged.

Those charged with protecting an individual’s true identity and real assets have the responsibility of strengthening user authentication during transactions, without making ATMs impossibly hard to use or increasing the vulnerability of an individual's true identity. Biometrics with liveness detection solves this problem.

By binding a unique individual to his or her true identity, biometrics goes beyond what the user has and knows to provide the only means of determining “who” is actually using the system. It eliminates the hassle and security risks of PINs and passwords while simultaneously making it easier to know if someone is who he or she claims to be. With nothing to carry or remember, biometrics is also inherently more convenient for the user, allowing access with the touch of a finger.

In short, biometrics is the only true means of making security more convenient while also linking or binding digital identities to the individual, determining who is actually using the system and verifying whether he or she is a legitimate user for a myriad of new mobile and on-line applications. And, with liveness detection, biometrics authentication further eliminates the problem of fake fingerprints and concerns about fraud or biometric identity theft.

During 2016, countries like Brazil will see the number of ATMs with biometric authentication overtake those relying only on conventional approaches. Brazil has an extremely high rate of adoption along with other South American countries. With 190,000 ATM terminals throughout Brazil, 90,000 utilize biometric technology and at least 60,000 are multispectral imaging sensors. HID Global’s Lumidigm biometrics solutions are a big part of this adoption curve, with more than 1 billion ATM transactions being biometrically secured each year in Brazil, alone.

Moving forward, using biometrics to authenticate mobile payments and other bank transactions will likely become a very big market driver. Gartner has predicted that by 2016, 30% of all organizations will be using biometrics on mobile devices and has long upheld the conviction that biometric solutions are the must-have for enterprise mobile authentication. With applications like Apple Pay and initiatives from the FIDO Alliance and others, biometric authentication is becoming more prominent in consumer-facing applications.

Meanwhile, with new technology adoption comes new risks: as biometric applications become increasingly widespread, and are relied upon for securing personal transactions, deployed solutions are likely to be targeted for attack. Consequently, it will be increasingly important for those deploying biometric authentication to understand that not all biometric devices and solutions are created equal.

How Biometric Authentication Works

Banking at the ATM requires robust and reliable authentication of authorized individuals to prevent fraudulent system access. There are also two important concepts to understand: identification and verification. The former answers the question “Who am I?” while the latter answers the question “Am I who I claim to be?”

Biometric identification is often used in government and commercial applications to validate the uniqueness of an individual by comparing his or her name and biometric information against others that have been enrolled. In the absence of any other information provided by the user, the system must search a large database of biometrics data to identify this one individual. This computationally intensive process requires an automated fingerprint information system (AFIS) to conduct this search and see if there is a match.

Biometric verification, on the other hand, is simply a confirmation of a person’s identity claim, made through a second factor such as an account number, a card or even a smart device, and match to his or her biometric record. In simple terms, combining fingerprint authentication with a second (or multiple) factors is a very good way of providing a very high level of security in real time.

Biometrics as part of a multi-factor approach is becoming more and more interesting given the availability of an expanded set of intelligent personal devices including smartphones, wearables, watches and cards. These are all convenient second factors that are becoming part of an ever-expanding access management ecosystem. Regardless of which additional authentication factor is presented by the user, when it is combined with the biometric data associated with the identity claim, it is possible to quickly determine a definitive “yes” or “no” to the user’s identity claim. Strong authentication, by means of two or more factors (with one being a biometric) is substantially more secure than outdated username/ password alternatives.

Enrolling and verifying individuals with today’s biometrics technology has become fairly routine. Chips on cards can securely hold biometric templates that can be matched at the point of verification. Smartphones or other mobile devices could also contain secure digital credentials. The benefit of this architecture, and today’s technology, is that a person can match his or her fingerprint data with the information carried on the card, phone, wearable or other digital personal device — there is no local database or network connection required. So as mobile banking rises, applications could allow users to store their biometric data on their own devices for privacy, portability and convenience.

Requirements for Successful Implementation

While many biometric modalities have been tried at the ATM, fingerprint biometrics has become one of the most widely used, partly because of its long history, but more importantly for its ease of use, performance, interoperability, ability to thwart imposters and low cost. And contrary to many claims or what has been depicted in movies, fingerprint characteristics cannot easily be transferred, socially engineered or guessed. Biometrics is quite simply the simplest and most universal form of personal identity. There are also no literacy, language, race, gender or other barriers to biometrics’ widespread adoption or deployment. User authentication is completed with the simple touch of a finger.

That said, best practices should be observed for the most successful implementation of a secure, convenient and trusted authentication solution. Key focus areas should include the following:

Biometric Sensor Reliability

Sensor reliability is essential. It is critical that sensor technology be capable of working reliably under the broadest range of real world conditions. To solve this problem, HID Global uses Lumidigm multispectral imaging technology to ensure that unique fingerprint characteristics can be extracted from both the surface and subsurface of the skin. More data and better images yield superior and reliable matching performance. Key features include:

- Uses multiple sources and types of light along with advanced polarization techniques to capture information from deep within the finger — all the way down to capillary beds and other sub-dermal structures.
- Includes field-updatable liveness detection capabilities to prevent spoof attacks — the use of fake fingerprints or “spoofs” to impersonate a legitimate user and gain unauthorized access. Lumidigm liveness detection is built from advanced machine learning algorithms that can be updated as new threats and spoofs are identified, enabling multispectral imaging sensors to very quickly respond and adapt to new vulnerabilities.

Optimized Data Security

Biometrics data must be handled like all sensitive and identifying information. Properly architected system designs will always consider and protect against both internal and external threats and attacks. Beyond the encryption of the data itself, there are now many good alternatives available for building highly secure and well protected systems. For instance, for strong and reliable user authentication, organizations should consider, where practical, multi-factor and even multi-modal authentication to maintain security even if some identifying data is compromised. Today's authentication technologies enable solutions that can enhance security while replacing passwords and improving convenience in a seamless way that is non-intrusive to the legitimate user.

Tamper Protection and Trusted Connections

The chain of trust is only as strong as the weakest link. The biometric used to authenticate the user for each transaction must interoperate with trusted devices at each point of verification. An example of this approach is HID Global's Seos™-based solutions, which create a device-independent, trusted physical identity verification process. Additionally, the physical devices themselves must be tamper resistant to ensure that all transaction integrity is preserved. The HID Global Lumidigm V4xx fingerprint sensors and modules provide a good example of how to take this approach with a biometric authenticator, which is implemented as follows:

- The device can be encryption-enabled with various tamper resistance and detection capabilities that protect the integrity of the communication between the client and the sensor.
- The chain of trust must be preserved end-to-end if the goal is, for example, to simplify financial transactions for users while eliminating fraud for financial institutions.
- The end-point device must connect to the institution's systems through a cryptographically secure channel protected by hardware tamper detection and response, which establishes trust between the device and the institution's systems independent of intermediate systems and networks.
- The trusted biometric device must be able to perform a live scan of a finger with strong liveness detection to ensure that the person making the transaction is who they claim to be (that is, the same person that enrolled their biometric fingerprint).
- If a card, smartphone, PIN, or other authentication factor is used, each must also be confirmed by the biometric — a biometric that is associated with a specific individual through a robust identity-proofing process at enrollment. This ensures that true identity verification has been performed in a trusted manner.

HID Global Lumidigm biometric solutions that support this combination of tamper protection and trusted endpoint connections have been successfully deployed in ATMs worldwide. This includes Brazil, where one billion annual transactions are authenticated using this approach.

Deploying biometrics solutions with tamper protection and trusted endpoint connections results in fraud reduction and other cost savings for a strong ROI. Many banks report that measurable reductions of fraud levels have met or exceeded expectations. Some banks allow their customers to self-enroll at the ATM, a cost-saving system design that works because HID Global Lumidigm liveness detection technology functions unattended. Further, the ease of the process and attractiveness of biometric authentication has enabled banks to accelerate their enrollment initiatives, securing more transactions against fraud with biometric authentication. Finally, some banks have shown an authentication service rate for HID Global Lumidigm sensors to be higher than that of the typical card-plus-PIN authentication model.

Scenario Testing

Scenario testing is always recommended in order to evaluate biometric technologies in specific environments and applications. Any well-designed system must provide a very positive user experience while maintaining required levels of security and reliability. Systems that make access difficult are frustrating for legitimate users, who then take their business elsewhere. Usability can be ascertained through scenario testing.

Smart Implementation Policies

Effective authentication solution deployments are supported by appropriate business policies. Well-designed systems can significantly reduce risks and vulnerabilities. However the best system deployments are those that employ effective business policies to control or otherwise ensure the proper use of these systems. Enrollment policy, number of allowed attempts before lockout and basic exception handling are good examples of workflow considerations that will significantly impact security, convenience, and the anticipated return on investment.

Mobile Credentials Linked to a Biometric Identity

Because digital credentials are simply aliases for one's true identity, it is critical to authenticate credentials stored on a user's personal device and link those credentials back to a true identity with biometrics. When credentials and digital aliases are bound to a unique individual's true identity, a rich set of new trusted applications and services are enabled. No single security technology is 100 percent reliable; making multi-factor authentication more seamless and non-intrusive with biometrics improves and protects the user's true identity and business transactions. And unless and until all systems are designed to support biometric authentication, both the user and vendor are exposed.

More Robust Biometric Templates

It may be desirable in some application-dependent situations to construct and enforce the use of enhanced biometric templates. The use of a "super template" that uniquely combines biometric data with other information — perhaps even an OTP or other out-of-band data — enables the system to recognize and reject a biometric template that was created from a stolen fingerprint image. Templates can reside on a card or on a chip or in a smartphone or personal wearable. A bank could deploy this approach to protect user identity. As some do today, banks could enable multi-factor authentication and require that both the biometric and some other data be provided. Alternatively, they could enroll biometric data and then "sign and encrypt" the template with unique or closed-system data.

The creation of a guaranteed unique "super template" might combine standard (interoperable) and proprietary data. This is the approach that HID Global takes with its Secure Identity Object™ (SIO), which is a data model for storing and transporting identity information in a single object. SIOs can be deployed in any number of form factors including contactless and contact smart cards, smartphones and USB tokens, and ensure that any of these items and the data associated with them are, in turn, only associated with the owner's identity. The SIO is digitally signed using proven cryptographic techniques as part of a seamless and secure process. Various data objects can be added, encrypted, and signed, i.e., biometric data, as well as data for computer log-on and other secure identity applications. Then, all content is secured with a wrapper and bound to the device with another signature.

Privacy Protection

System design must provide for end-user privacy. The ability to store biometric data on a personal device eliminates the need for a local database or network connection and is one way to ensure privacy. Encryption and tamper resistant devices prevent the interception of private biometric, biographic, and transactional data. Finally, while biometric characteristics are not themselves inherently private, well-designed biometric solutions prevent fraudulent access and allow individuals to control their true identity.

Use Cases

There are a number of use cases for biometric authentication at the ATM and self-service kiosks that offer significant value to the financial institution and to its customers:

PIN Replacement at ATMs

One common approach used today at biometric ATMs is to use the fingerprint in place of the PIN for the ubiquitous card-plus-PIN transaction. Fingerprint authentication is generally easier for the customer than remembering a PIN and it also brings a higher level of certainty about who is transacting. To be a successful component of a transaction, the biometric technology chosen must deliver the highest possible levels of reliability and performance.

- With the fingerprint-plus-card approach at the ATM, the customer simply inserts the card and touches a finger to the reader to conveniently withdraw funds. Widely used today in Brazil, the card-plus-fingerprint solution is used in the more than one billion ATM transactions annually referenced earlier.
- With multispectral fingerprint technology, one institution has enabled customers to enjoy card-less processing, eliminating the need for a PIN while offering the convenience of making the bank customer's finger the only “key” or “wallet” necessary for accessing cash and conducting other transactions at an ATM. Users simply enter their account number and confirm the transaction with a fingerprint. The bank that took this to market established a competitive advantage over its peers who did not offer the service, which resulted in the successful acquisition of new bank customers who made the switch specifically to enjoy this level of convenience.

Proof of Life for Benefit Distribution

For banks that administer citizen benefit programs, the assurance that a recipient is alive and present is critical. This was important for Argentina’s Banco Supervielle, whose kiosks are used to distribute pension benefits from the Administración Nacional de la Seguridad Social (ANSES). The bank had a significant problem with fraudsters trying to claim their deceased relatives’ pension benefits. To combat the problem, the bank began rolling out fingerprint authentication with multispectral imaging technology as part of a “proof of life initiative” in October 2013. The bank’s investment in biometric kiosks has resulted in considerable savings due to fraud reduction. In addition, 170 human cashiers have been retrained as commercial advisors, allowing the bank to increase the level of attention to its customers.

Authentication Extended to New Applications

A bank’s greatest investment in biometrics solutions is in the enrollment database. The availability of interoperable authentication devices enables banks to purchase from multiple vendors, permit cross-bank usage, and pave the way for many new applications in the future. We have seen fingerprint authentication used for mobile payments, and it can also be used to secure mobile banking by requiring a user to provide biometric credential before accessing information or proceeding with a transaction. If interoperability is ensured, then fingerprint authentication on mobile devices could be used in conjunction with enrolled information that the bank uses for authentication at the ATM.

Multi-Transaction Sessions

Placing a finger on a sensor takes less time than keying in a PIN. When multiple transactions are desired in a single session, this time benefit is multiplied to provide a quick and easy way for a bank customer to authenticate each transaction. In this way, the bank can enforce per-transaction authentication for greater security without compromising the user experience.

Biometric Information Incorporated into a Smart Device

As banks migrate to chip-based EMV cards for higher security, there is the opportunity for incorporating a user's biometric template on the card. This is currently being done in some large-scale national identity programs. Alternatively, in countries where national IDs already exist, commercial customers could leverage these programs to ensure that both the card itself is genuine and that it indeed is associated with that known user. The ability to intelligently manage digital credentials on cards, phones, and wearables — and bind those credentials to the legitimate user with biometrics — improves overall security and user convenience.

Conclusion

The goal of any transaction at the ATM is to conveniently provide a service while ensuring the identity of the individual to whom the service is being provided. Managing risk is a matter of balancing and, ideally, combining security and convenience. Biometric authentication provides this capability with the highest level of certainty, which is why it is increasingly popular for securing ATM transactions.

We all have only one true identity, and this identity must be protected in an sensible, balanced and efficient way. Nothing in life is without risk but there are no longer valid technical or business reasons to rely on outdated security systems and practices. Biometrics offers us the ability to make productive use of the myriad of digital credentials that we use and manage today — and to do so in a manner that is more secure and convenient, and actually protects our true identity. We no longer should have to choose between greater security or convenience, when with biometrics we can get both.

hidglobal.com

2016-04-13-hid-biometrics-atm-wp-en PLT-02817