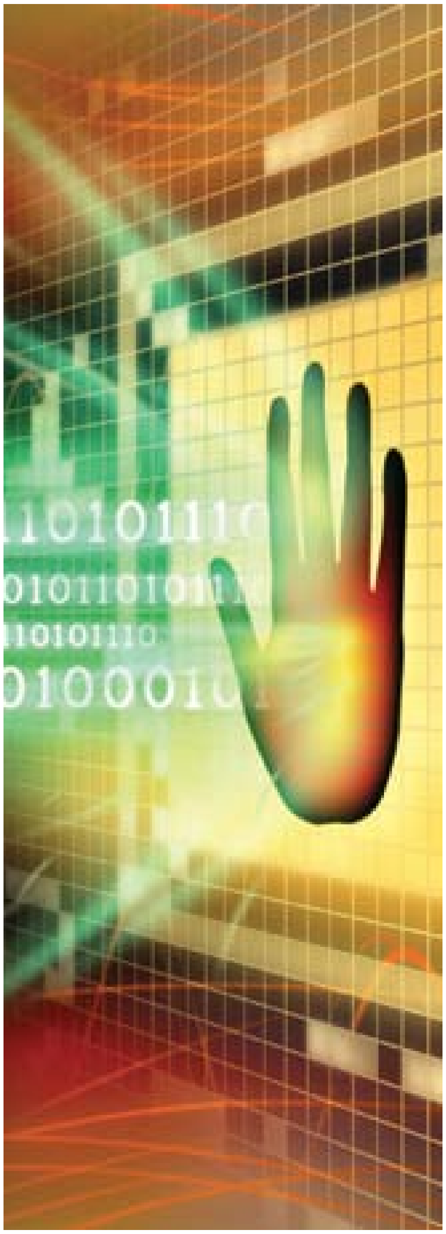
Biometrics for payments

The use of biometrics in banking

Biometrics for payments

The use of biometrics in banking

The use of biometrics for authentication is nothing new. But historically, its use has been mostly concentrated in the government sector (such as for electronic ID and passports) and access control. More recently, a whole range of biometric applications are being released by various industry sectors. The number of people that uses some sort of biometry on a daily basis grows steadily; some analysts even predict that the size of the biometrics market will triplicate in the coming five years. One of the reasons of this popularity is the price. While in the past biometric systems were prohibitively expensive, technology has improved to the point that for less than $7 it is possible to install fingerprint scanners on a mobile phone – such as in Apple's iPhone 5S. In particular, the mobile and payments industry are paying more attention to biometric solutions.



Many banks around the world have already implemented biometrics for customer authentication, in most cases in the form of fingerprint reading. Countries such as Brazil, India, Poland and Japan already support ATM cash withdrawals by means of biometrics, many other countries intend to follow the trend in the near future, especially in Asia and Africa. While security experts are cautious about the use of biometrics in the (extremely regulated) banking industry, banks are rolling-out biometric solutions as a countermeasure to two commonly faced problems:

1. Identity theft, mainly in the form of enrollment fraud, where a customer applies for a bank service or a credit line using a fake ID

2. Increasing frauds at ATMs, in particular, card trapping, use of lost & stolen cards or skimming (in regions that have not migrated to chip).

By implementing biometrics systems, banks have managed to reduce losses due to identity theft to a level that quickly justifies the business cases for the implementation. In some cases, the losses could sum up to dozens of millions of dollars. One of the popular methodologies used to ensure that no applicant is registered twice is the Automated Fingerprint Identification System (AFIS), originally implemented by the FBI for criminal cases; nowadays it has been adapted for the banking industry as well, with a high degree of reliability. Once the bank already stores the biometric data of its accountholders in a database, it can also use biometrics for authentication when authorizing transactions. In this way, banks can not only safeguard against skimming or misuse of lost & stolen cards at ATMs, but also as a protection against legislations that makes financial institutions liable for withdrawals denied by the cardholder.

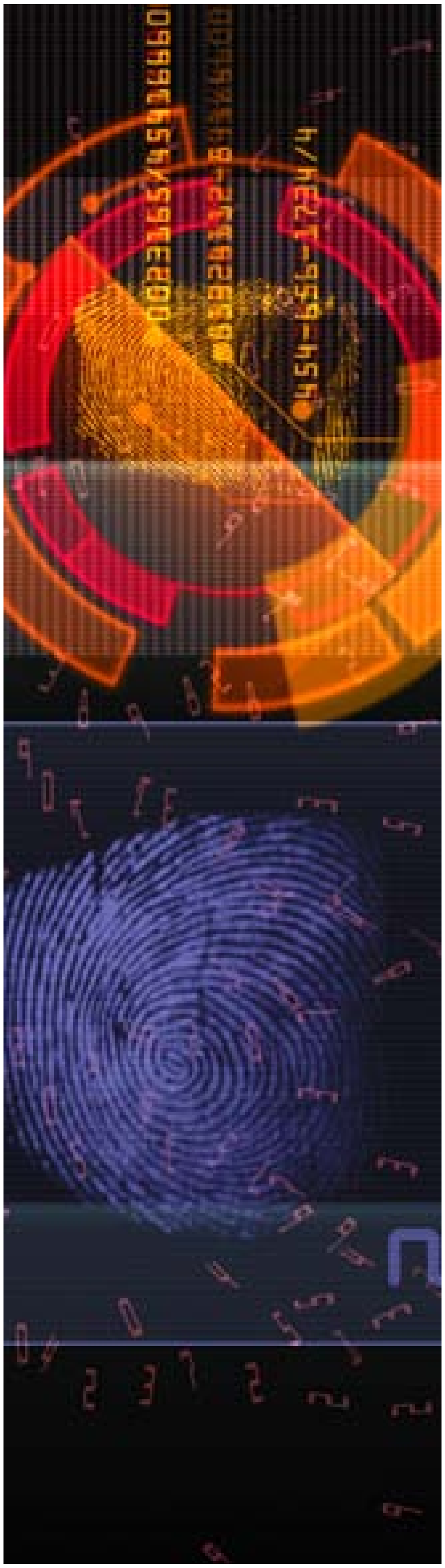
While the above seems to justify the adoption of biometrics in the banking industry, one should be aware that the technology has not yet achieved an adequate degree of maturity. The following factors contribute to that:

- Security and reliability of the device

Shortly after the release of the iPhone 5S it was possible to fool the fingerprint scanner by copying the fingerprint of another person and creating an artificial or gummy finger which could be used to unlock the device. Fingerprint readers at ATMs are usually equipped with more sophisticated modules to perform live finger detection (LFD). Many of them use multi-spectral and multi-polarization analysis to detect whether the material has the physical structure of a real finger. But this is not an exact science. The reliability of a fingerprint is always a trade-off between the False Rejection Rate (FRR) and the False Acceptance Rate (FAR). Also, the relationship between the FRR and FAR is not unique and depends on various factors, which are still object of scrutiny by scientific experiments and proof of concepts. The false acceptance can, for instance, be increased by ingenuous attacks. Every year, better attacks are published, and better readers and LFD modules are produced. This is good news, but also a warning sign. Although most of the implementations in the banking industry still rely on the fingerprint as the biometric characteristic, the vein structure of hands or fingers is gaining popularity, as it is an equally convenient method, but much more difficult to forge than fingerprints. Also, the vein recognition technology tends to have a much lower FAR then fingerprints. A combination of fingerprint and finger vein recognition may prove to be an even stronger method, but is technologically more complex.

- It is not only the device

Most of the media and academic attention are paid to the "falsification of the biometric trait", such as replicating a fingerprint. But after the capture, this trait is transformed into a digitized data. So, the question is, how is this digitized data protected? If one can make a 'copy' of this data, one can pose as the person providing it. Although there is a strong history and culture of physical and logical security for PINs and card data, it is not the same for biometric data. Furthermore, one of the reasons why the financial industry in developed countries is not ready to adopt biometrics is the need to comply with strict personal data protection regulation, such as the European General Data Protection Regulation (GDPR). The risk of compromise of biometric information stored in a centralized database is real and non-acceptable for the Security Officer of many banks. The liability arising from data leakage due to an attack is also difficult to estimate. Recently there have been repeatedly attacks on payment systems; a recent example is the breach of 70 million customer's credit card data of the American retailer Target.



Besides the financial loss, banks react to such compromise by re-issuing the card. In case of biometrics, the customer fingerprint cannot be re-issued. Furthermore, some banks do store the full biometric data in their databases, and not only the trait or template. This is done in order to avoid vendor-lock in, as the template is vendor-dependent, while the fingerprint is not. Having the fingerprint database compromised, could affect the customers in all government and industry sectors that rely in the fingerprint, which is a threat of unpredictable liability.

- Lack of standardization

Although the standardization of the "representation, interoperability and quality" of biometric data has improved in the last years, there is still no widely recognized standard to validate the security of the biometric data for payments. Although there are some organizations that do provide validation of biometric solutions, the methodology and security requirements do not have the same degree of scrutiny of those traditionally used by the card payments industry. As it is usually the case, a biometric system is just as secure as its weakest link. Therefore security standards and security evaluation should cover the whole chain – including service enrollment, usage, transmission and storage of biometric traits, and all devices that participates in this process. Standardization bodies, such as ISO, NIST and BSI are regularly releasing biometrics standards, but an industry-wide recognition is still to be seen.

Conclusion

Biometrics is easy and convenient to the customer and, when used properly, can be secure as well. One must realize, however, that biometrics is not a remedy for all problems. Understanding how it works, when to use and when not to use is essential. For example, the two problems discussed in this note require quite different approaches: The use of biometrics as a form of identification, such as to prevent the enrollment fraud, requires the comparison of one biometric reference to many biometric references stored in the system (1:N). In this case, the false acceptance rate (FAR) plays an important role. On the other hand, the use of biometrics in order just to authenticate a customer, such as to prevent frauds at ATMs requires the comparison of one biometric feature to just one reference feature stored in the system (1:1), as the customer was already identified by using other means. There are a plethora of different architectures and designs used by the banks that have implemented biometry. However, the banking industry still needs to agree on a comprehensive set of robust standards for security and testing. This will be crucial to leverage the strengths of biometrics for payment processing and customer enrollment.

As it is usually the case, a biometric system is just as secure as its weakest link. Therefore security standards and security evaluation should cover the whole chain – including service enrollment, usage, transmission and storage of biometric traits, and all devices that participates in this process.

Contact details

UL Transaction Security
info@ul-ts.com
www.ul-ts.com