WHITE PAPER
BIOMETRIC PAYMENT CARDS
- How to secure contactless payments
SUMMARY

Biometric payment cards are expected to grow significantly in the coming years. The first market trials of biometric payment cards were initiated in 2017 and this year several commercial pilots of contactless biometric cards have started across the globe. Biometric payment cards provide a more convenient and secure alternative to PIN code-based payment cards and are set to gain acceptance due to the following factors:

- **Fingerprint biometrics provide a high level of security and prevent fraud, which is a concern for many users of contactless payment cards.**
- **Biometrics open up the opportunity to lift or raise purchase caps on contactless payments, which would further increase cardholder convenience, while ensuring the required security for card issuers.**
- **Retailers can benefit from higher in-store throughput without making additional investments.**
- **Banks and payment providers can reduce payment card fraud.**
- **Consumers are used to the convenience of using fingerprint authentication instead of PIN codes through their smartphones.**

Contactless payment cards have an advanced architecture and are characterized by constrained computing environments. To enable commercial mass deployment of biometric payment cards, solution providers need to offer cards that provide efficient and secure authentication in such highly constrained and power-lean environments, while meeting the requirements for biometric performance, speed and cost-efficiency set by the payment card industry. Precise Biometrics’ algorithm solution for biometric smart cards, Precis BioMatch Card, meets this challenge.

Precise BioMatch Card uses an innovative “split architecture” solution, which makes it possible to run the critical matching of fingerprint data within a Secure Element, SE, which is an on-card secure chip providing the necessary protection against hacking. However, the SEs that are currently used in biometric smart cards are not powerful enough to run the entire fingerprint authentication process within its confines. Precise Biometrics’ algorithm solution solves this by managing the extraction of fingerprint data within a separate chip on the card, and runs a separate process for the fingerprint matching inside the SE, which ensures a high level of security.
REPLACING THE PIN CODE WITH ON-CARD FINGERPRINTS

There is a great interest in biometric smart cards, which is expected to grow in the years ahead. The growth is expected in several application areas, such as access control and solutions for passports and ID-cards. The largest commercial interest, however, is in biometric payment cards and several of the leaders in the payment ecosystem have communicated a strong commitment to biometric payment cards.

The major payment card providers, such as VISA and Mastercard, as well as many payment card issuers, are driven by the increased convenience and security contactless biometric cards bring, allowing swift tap-and-go purchases while reducing fraud.

In 2018, many of the major payment providers are conducting or are planning to conduct commercial market trials of biometric payment cards together with local banks in Europe, Asia and the US (2). The goal is to evaluate these new cards’ potential as an alternative to or complete replacement for PIN code-based payment cards. One example is VISA’s first pilot with biometric payment cards in the USA, carried out in cooperation with Mountain America Credit Union, with Precise Biometrics supplying the fingerprint software solution.

MARKET-GROWTH DRIVERS

The adoption of fingerprint technology as a secure and convenient standard for authentication on mobile devices has paved the way for the adoption of biometric smart cards.

Fingerprint authentication was ranked the highest compared to other biometric modalities for both in-store payments as well as online scenarios. The consumer bias towards fingerprints is also supported by a survey conducted by Mastercard and Oxford University (4), in which 93 percent of consumers preferred biometrics over passwords for validating payments.

Hundreds of millions of consumers are accustomed to a swift and convenient experience of contactless low-cost purchases where PIN codes are not required. ABI Research considers fingerprint authentication within the card the next natural step in contactless cards (5), maintaining a high level of convenience while increasing security. Contactless cards allow consumers to spend less time in line, while improving in-store throughput for retailers. Adding biometrics in the contactless cards would increase customers’ confidence and trust, while not requiring any additional implementation costs for retailers, since biometric payment cards are designed to function within the existing infrastructure. Adding biometric authentication would reduce the need for today’s purchase caps on contactless payments, which would further increase the convenience of contactless payments.

For banks and payment providers that have seen costs for payment card fraud rise year after year, biometrics come as a welcome feature to tackle skimming and other fraud.

Replacing PIN codes with fingerprint technology closes the door on PIN code theft, which is carried out for instance by looking over the shoulder or using small undetectable cameras near ATMs or payment terminals.
BIOMETRIC PAYMENT CARDS

All the processes - fingerprint enrollment, data extraction, storage and matching - are completely performed within the biometric card. This goes together with the development of data protection legislation. Today national and transnational legal frameworks are moving away from allowing biometric data to be stored in centralized databases for reasons of security and data integrity.

Developing biometric payment card solutions for commercial mass deployment is a tightly performed balancing act. For Precise Biometrics, along with other players in the ecosystem for biometric payment cards that is currently forming, this means balancing tough restrictions on the fingerprint solution in terms of power, clock frequency and sensor size with the payment industry’s performance requirements for convenience and security. The challenge is to produce biometric payment cards that can perform efficient and secure authentication in a highly constricted and power-lean environment.

FINGERPRINT SENSOR SIZE

Today's biometric smart cards use capacitive fingerprint sensors due to their ability to generate a highly detailed image of a fingerprint via electric signals. The capacitive sensor is silicon-based and thus price sensitive; the smaller the silicon area, the more cost efficient the sensor becomes. At the same time the user experience must not be compromised so that it becomes difficult to obtain a match when placing the finger on the sensor. This is naturally easier with a larger sensor area. To find the sweet spot for size versus cost is therefore a critical factor for the success of biometric payment cards. The smart card must have an efficient algorithm solution to perform a fingerprint match, regardless of whether it supports a small sensor that captures limited fingerprint features or meets memory limitations when storing features captured on a larger sensor. Precise Biometrics’ algorithm solution BioMatch Card is optimized to run an effective authentication process on small fingerprint sensors, currently down to 8 x 8 mm in size.

POWER LEAN

The first pilots of biometric payment cards have been powered by contact mode. Recently, pilots of biometric smart cards supporting dual interfaces, i.e., contact and contactless mode, have been initiated. Most of these have been equipped with built-in batteries. But to reach a high-volume market the price must be kept down, meaning a solution without a battery is desirable. A dual interface biometric smart card therefore should be powered by energy harvesting through a wireless radio antenna in the card. The limited power access means that the total biometric solution should be as energy lean and efficient as possible, which puts restrictions on processor clock speed. Precise Biometrics’ algorithm software is therefore highly optimized to run in a very restricted environment. This must be achieved while meeting payment industry targets for convenience and security. This means that a successful payment should be performed within a second, with an FRR of 3% and an FAR at least as secure as a PIN code, i.e., 1/10,000.

BIOMETRIC SMART CARD BASICS

SECURE ELEMENT

The Secure Element, SE, is an on-card secure chip. Performing the matching part of the fingerprint authentication in the SE provides the highest degree of protection against hacking.

1259 5667 8854 569
MONTH/YEAR 04-20

NFC

A contactless biometric smart card is powered by the payment terminal through Near Field Communication (NFC).

FINGERPRINT SENSOR

The fingerprint sensor on a smart card needs to be small due to cost and memory limitations which requires an effective and powerful algorithm solution that can perform a convenient and secure match.
SPLIT ARCHITECTURE SOLVES THE CHALLENGE OF LIMITED COMPUTING CAPACITY

As a self-contained biometric system, the biometric smart card provides a high degree of protection of the cardholder’s biometric data against external attacks. The best possible protection of a biometric smart card against hacking and spoofing is to store all fingerprint data and run the authentication process within the card’s Secure Element, SE, a secure chip where it’s possible to store sensitive data and run dedicated applications. All the major payment providers have certified SEs for payments.

The SE considerably reduces the risk of theft of fingerprint data and makes it extremely difficult to tamper with the payment process, essentially creating bank-grade security around the payment process. But SEs are very restricted chips, with a fraction of the memory and much less processing capability than the processor on a smartphone. The SEs that are currently used in payment cards are not powerful enough to handle both the extraction and matching of fingerprint templates, which demands much more computing power than PIN code matching. Using more powerful SEs would result in increased production costs, which is not a viable solution.

Precise Biometrics has met the challenge by implementing a “split architecture” solution in Precise BioMatch Card, which distributes the algorithm’s tasks in an optimal way: One part of the algorithm runs the extraction of fingerprint data on a separate MCU in the card. The other part of the software runs the storage and the critical matching process within the SE. This makes it possible to use SEs that are currently available on the market, while keeping the manufacturing costs at an acceptable level.

THE FINGERPRINT ENROLLMENT AND VERIFICATION PROCESS STEP-BY-STEP IN THE BIOMETRIC PAYMENT CARD

1. At enrollment the card owner touches the fingerprint sensor several times to capture fingerprint images.

2. Precise BioMatch Card extracts the fingerprints’ unique characteristics from the images and creates a template.

3. The template is stored in the Secure Element (SE) on the card. Once the fingerprint has been enrolled, subsequent fingerprint authentication during a purchase would only require one touch on the sensor.

4. At fingerprint authentication Precise BioMatch Card matches the newly acquired fingerprint template with the stored template of the rightful card owner. If the two templates match, an approval is sent to the payment applet to authorize the purchase. This all takes place in the SE.

5. The authentication is wirelessly transmitted to the point-of-sales terminal. The whole process, from placing the finger on the sensor to the purchase being authenticated, should take no more than 1 second.

FAR (False Acceptance Rate) and FRR (False Rejection Rate) describe the security of a fingerprint solution. A low FAR means a secure solution, where a low rate of unauthorized persons is authenticated. A low FRR means a convenient solution, where a low rate of authorized persons is denied authentication. An optimal solution is a low FRR and low FAR.
ABOUT PRECISE BIOMETRICS
Precise Biometrics is a market-leading supplier of solutions for convenient and secure authentication of people’s identity. We develop and sell fingerprint software that provides the market’s best user experience and security. Our solutions are used hundreds of millions of times every day by people all over the world and are marketed together with strong business partners. For more information, please visit https://precisebiometrics.com. Follow us on LinkedIn and Twitter.
REFERENCES


(4) "Mastercard and Oxford University unveil framework for mobile biometric banking", Biometric Update, June 2017.

(5) "The Payment Card is here to stay", ABI Research, report, Phil Sealy, Q4 2017, IN-4776.
