gemalto
security to be free

Biometrics for Financial Institutions and the new Gemalto Biometric Sensor Payment card

White paper
October 2017

1- Financial Services go digital: Smartphones set the new user experiences with biometrics on the rise.

The mobile branch revolution

Smartphones are so massively used worldwide nowadays (1.5 billion units will be sold in 2017 according to IDC) that it's hard to realize that they appeared on the market just 10 years ago. Back in 2007, there were no performant broadband wireless networks available and no devices that could let anyone foresee the richness of the apps ecosystem we enjoy today. Back in 2007, mobile phones were not designed for secure services such as financial services. There was no NFC support by major handset makers and the only security framework available was the UICC and the SIM toolkit.

Consumers' interaction with their financial services has now massively migrated to the "mobile branch". Smartphones displaced desktop PCs for day to day banking services such as online access to accounts, money transfer, P2P payments and at store payments with NFC. In a near future, all banks services will be available for enrolment directly via mobile devices, using ID self-verification technologies. All of these anytime, anywhere, using a personal smartphone. Banks are in the process of repositioning their physical branches to prepare for this massive migration to the mobile branch.

This mobile wave comes with an interesting question: what is the future of banking cards on the long term? For the foreseeable future and very likely beyond the next decade, we have good reasons to see cards and mobile co-exist and share various payment scenarios. In fact, in the very near terms, we observe that smartphones advances such as biometrics will come to EMV cards.

Trust is key for the success of digital services

Money is at stake as well as very private data about our purchases, where, when, for how much... Like all digital services, establishing trust between a service provider and its customer is crucial for the adoption of payment services. Consumers have yet to trust their mobile devices. They trust their banking cards because they get issued by a Bank and also because they can see the secure chip on the card body. They want to know what will happen in case they lose their smartphone or if it gets stolen, the same way they know today that losing a banking card is harmless.

Establishing trust starts by a mutual authentication between a service provider and its customer. Both parties want to be sure they connect with the right party. Once authentication is performed, digital transactions can occur. Mobile services inherited at first from authentication technologies coming from the desktop PC and the worldwide web: the use of username and password combination (U/P) dominated the market for the last decade as it is fairly simple to deploy and interoperable across PCs and mobile. With the raise of financial services and the explosive growth of fraud attempts such as phishing attacks, the industry quickly looked for stronger, better ways to perform user authentication than U/P.

Strong authentication: the search for more security without too much impact on user convenience

U/Ps solutions were designed for a mainly dominant PC world and the use of the World Wide Web as the platform for services. It's interesting to observe that despite known security flaws, many service providers never replaced U/P authentication as they were concerned to create "frictions" with their users by introducing more complex solutions. In fact, what triggered the post U/P era was a convenience issue: when most consumers got to manage tens of online accounts, they ended up either getting confused with those tens of passwords or even worse: they used the same U/P for all their accounts.

Early two-factor authentication solutions did not really take into account usage convenience. Priority was to stop massive security flaws with one factor authentication solutions that can easily be phished. The goal was to replace those by two factor authentication solutions combining "What I know" and "What I have" i.e. using out-of-band technology. Security improvements were tangible, but at a cost of convenience for users. Each service provider has its own approach to 2FA and that resulted into some level of complexity for users as well as little to no interoperability among services.

2- Biometrics: a new "What I am" authentication factor that fits very well into mandated multi-factor authentication strategies.

What is biometrics and how does it fit into multi-factor authentication strategies?

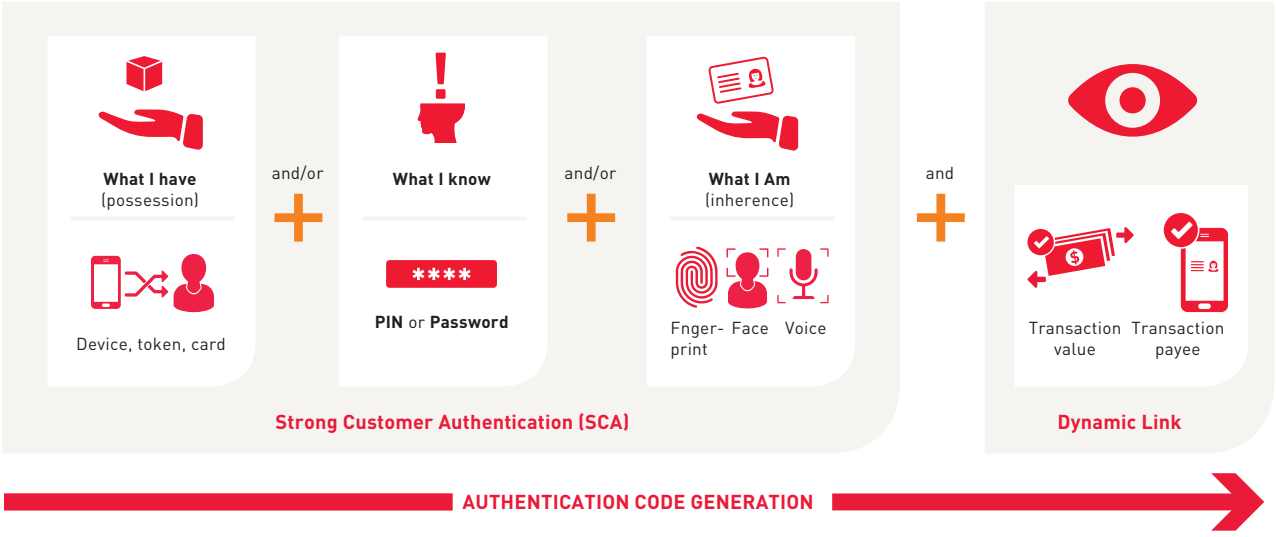
Multi-factor authentication can be defined as the use of at least two "factors" to verify a given user's right to be granted access to a service. Such factors are techniques that usually belong to three main families:

- What I know" i.e. a secret that the user memorizes, such as a password for example.
- What I have" i.e. a device that remains in the user's possession and that will be mandatory to be present when trying to complete the authentication challenge.
- What I am" is something very unique about the user, inherent to the user and always available to him/her.

Biometrics fits exactly that "What I am" family of techniques as it is defined as the measurement and analysis of unique physical or behavioral characteristics of individuals.

Biometrics such as fingerprints verification or facial recognition are massively used today by government bodies for electronic ID and ePassport border control for example. Biometrics sources such as DNA are also used for criminal investigations as they allow accurate identification and can't be forged.

Since 2013 with the introduction of the first iPhone 5 with TouchID fingerprint verification, commercial biometrics entered into a new dimension with hundreds of millions of smartphones equipped with fingerprint sensors. The very first use case for fingerprint was to unlock the phone. It is also used to login onto mobile apps and perform mobile NFC payment at the store.



Authentication vs identification

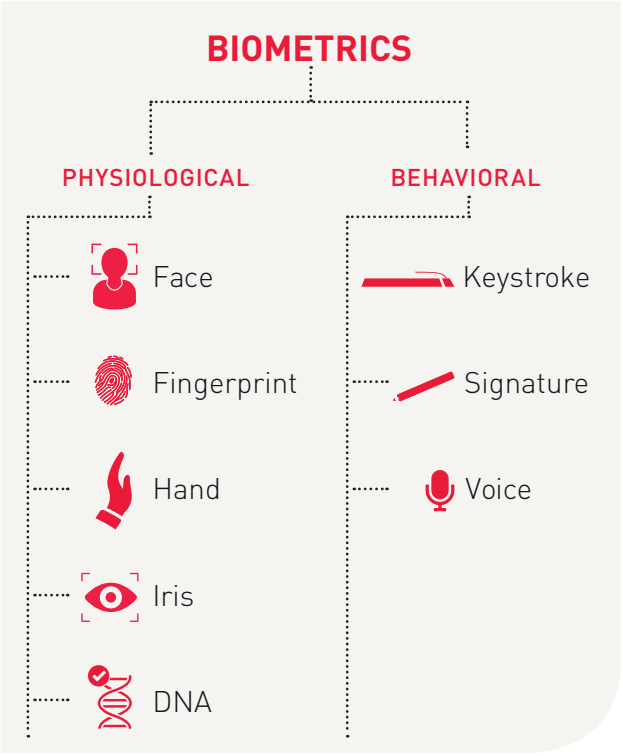
"What I know" and "What I have" factors can prove that a given user has access to the right credentials but does not prove the identity of that user. Secrets can be shared by the genuine user to family and friends as well as devices that belong to the genuine user can be used by third parties. Most Service Providers consider today that user authentication is sufficient to grant access as terms&conditions of their services will bind all liabilities to the genuine user. The genuine user is responsible for any issue that may occur if he/she shares access rights with other parties. For example, when using an EMV banking card, the use of the PIN code authenticates but does not identify the cardholder as the 4 digit PIN may have been shared by the genuine user. Most card issuers will specify in their services terms&conditions than PIN sharing is prohibited, but there is no solution nor mandate to control that at the Point of Sales Terminal.

"What I am" factors, when biometrics, are determining a true user identification. There is no way to share my biometrics information (despite attempts made by fraudsters to use "fake skin" for fingerprints) for example. Therefore when using biometrics, authentication becomes identification and brings a all-new security level.

Different source of biometrics today and tomorrow for commercial use cases

There are five main biometrics sources today at work for commercial use cases, mostly driven by the fact that the device of choice for biometrics measurements is the smartphone: fingerprint, finger or palm veins network, facial recognition with liveness detection, voice recognition and iris scan. An additional technique will emerge in the near future for connected watches: Infra-red imaging (and recognition) of blood veins networks at the wrist.

On a broader perspective, Biometrics can be categorized into two families: Physiological biometrics are body attributes that are unique to each person and that do not require any specific action by the user to be measured (beyond interacting with a sensor). Behavioral biometrics are attitude patterns that can be measured and differentiate from person to person in a way that can be measured and compared back to a reference data.



Biometrics	Accuracy	Cost	Size of template	Long term stability
Facial recognition	Low	High	Large	Low
Iris scan	High	High	Small	Medium
Finger print	High	Low	Small	Medium
Finger vein	High	Medium	Medium	High
Voice recognition	Low	Medium	Small	Low
Lip recongnition	Medium	Medium	Small	Medium

Multimodal biometrics

Consistently with the Multi-factor authentication strategy, solutions to measure and verify multiple biometrics sources can be deployed. For example fingerprint and facial recognition.

This is a growing trend for Public Sector applications such as border control. For commercial applications such as Banking services and payments, the foreseeable future is single source biometrics.

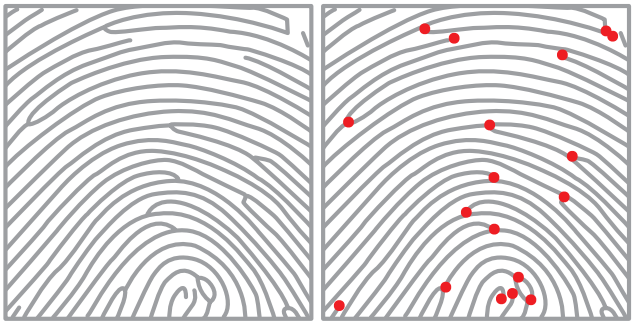
Biometrics implementation core technologies: Analog to Digital transformation

The use of biometrics for financial services on mobile devices today and on smart card in the near future will imply two steps to go through for the user:

- **Enrolment:** performed once per device. This is the process of creating a reference data to be securely stored in the device and then used for comparison purpose each time a verification request will be performed.
- **Verification:** performed each time the user wants to identify him/herself. This is the proceed of completing a biometric measurement to be then compared with the reference data

The enrolment process can be performed either on a sensor provided by the service provider, or on a smartphone owned by the user (self-enrolment). The first method will result either in adding a given user's biometric credentials in a global users' database, either in loading the biometric reference data in a user owned device. The second method will result in a local secure storage of the user's biometrics credentials in a device that remains in his/her possession. Self-enrolment (or assisted enrolment with the help of a teller at the branch) leads to dispersed credentials into individually owned devices and is currently the preferred method for commercial use case with biometrics, as it appears to protect the user Privacy and also protect the Service Provider from handling its customers' biometrics data.

Biometrics sensors are devices transforming an analog information into a digital map (minutiae) that can be compared digitally with a reference minutiae. For each biometrics sources, there are multiple technologies for minutiae extraction. For example with fingerprint sensor, solutions like capacitive coupling or ultra sounds can be used, resulting in different quality of results such as liveness detection or fake skin detection. The choice for one particular technology will depend on the use case specifications for False Acceptance Rate (FAR) i.e. the number of times a wrong user will succeed the biometrics comparison with the reference data and the False Failure Rate (FFR) i.e. the number of times a genuine user will fail the match comparison.



Minutiae Extraction by a fingerprint sensor

As an example today for an EMV banking card using a 4 digit PIN code as the preferred Card Verification Method (CVM), FAR = 1 for 10000 and FFR =0 for a match-on-card comparison time perceived as instantaneous.

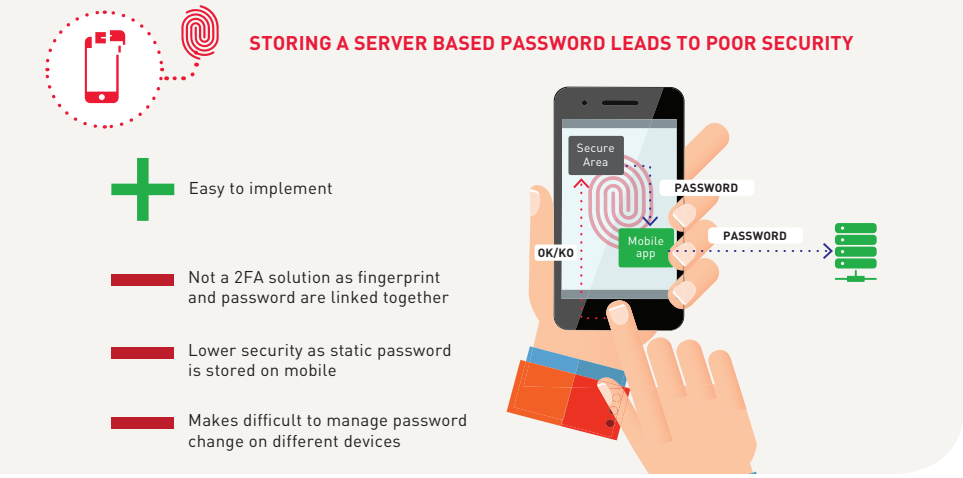
Typical fingerprint sensors today for EMV banking card perform at FAR = 1 for 50000 and FFR = 1 for 10 with a match-on-card time of approximatively 2 seconds. Increasing performance on FAR requires a more stringent Minutiae extraction and will likely translate into a longer time to perform a match-on-reference comparison.

Gemalto differentiators when using biometrics for online banking and NFC payment

Current commercial deployment of biometrics (mainly fingerprint) on smartphones were designed not for security improvement but rather exclusively for convenience improvement: an objective clearly achieved given the popular demand for fingerprint, facial recognition or iris scan for simple day-to-day actions such as unlocking a phone, accessing mobile apps in lieu of using a password and paying at stores using NFC. For online banking, most banks use a simple API provided by the OEM to store locally the user's password and release it to the app when the match test results in a success. This is a popular technique bringing biometrics in lieu of passwords management popular mobile apps, storing all the user's passwords.

This is still a One Factor authentication solution and, because of the risk of not being able to measure the fingerprint (wet fingers, cut on the finger, etc....) a password fallback is always available bypassing the entire biometrics test procedure. Bottom line this approach has zero impact on security. It's a great usage comfort and an elegant way to replace hard to remember passwords by biometrics, but it does nothing about security. Consumers mistakenly perceive this as a security improvement.

Given the constraints driven by the OEM that controls the API and the usage of the securely stored (typically in a TEE or a Sand Box) reference data, Gemalto is leveraging on that resource to turn it into a real 2FA solution with PKI:



OEM implementation of fingerprint to secure access to a mobile App: 1FA with passcode bypass

Gemalto implementation leveraging the OEM API: 2FA with no possible passcode bypass.

For mobile NFC Payments, most solutions deployed today use card enrolment in the cloud and a tokenized representation of such card, store in the mobile device, to complete the EMV flow at the POS terminal.

Gemalto supports all types of security frameworks to securely handle the tokens in the mobile device as well as biometrics as an identification method for payment.

3- The EMV card use case: Biometrics as an identification method for payment

Revisiting the CVM strategy

Chip&PIN EMV banking cards support 4 different types of Card Verification Method (CVM) today:

- PIN offline
- PIN online
- Signature
- No CVM

EMVco has expanded this list in 2017 by defining a biometric CVM (see EMVco Specifications Bulletin 185 at https://www.emvco.com/specifications.aspx?id=23).

There is a very broad diversity worldwide, from issuer to issuer, regarding the CVM of choice for each payment application. The raise of contactless payment for cards for low amounts increased the number of scenarios where no CVM is the choice. When introducing the idea of Biometrics fingerprints in lieu of a Pin Code for CVM for an EMV banking card (biometrics CVM being already standardized for sensor-on-terminal use cases, or sensor on smartphones), the product design strategy must cope with one of the existing 4 CVM standardized methods: One solution leveraging CVM =no CVM required emerges quickly: it consists in executing all transactions in 'no CVM' mode if the biometrics test using math-on-card to the reference data, securely stored in the card's chip, is passed successfully.

The 'no CVM' approach applies to transactions using the contact mode. For contactless transactions, CVM must be either CD CVM (Consumer Devices CVM) or OD CVM (On Device CVM).

ISO standards constraints and implications

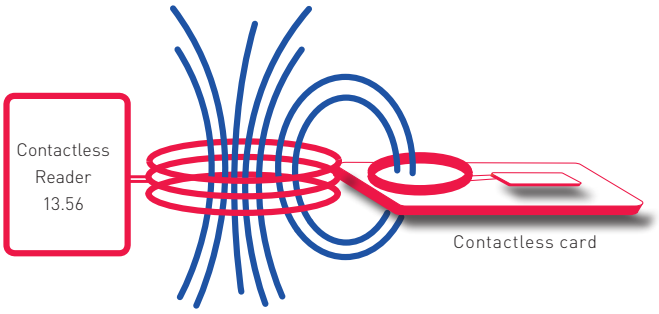
The addition of a fingerprint sensor on a card body for at POS contact and contactless payment, using biometrics fingerprint in lieu of a 4-digit PIN code, must be done in full compliance of the ISO standards for card dimensions for size, flexibility, life time.

Size: the card must still be used at the ATM – a fall-back to PIN code entry may be authorized when the biometric sensor is not accessible as the card is totally inserted inside the ATM. A fingerprint sensor which is typically a 1 by 1 cm device must not affect the overall thickness of the card body which is standardized at 0.76mm.

Flexibility: The card expected life time of 3 to 5 years comes with ISO specifications on how much flex it must be capable to handle. A fingerprint sensor which is typically a 1 by 1 cm square at the surface of the card body must comply with typical flexions that the card will deal with during its life time.

Life time: a fingerprint sensor is an electronic device that requires power both for enrolment and for day to day measurements and match-on-card. Two strategies can be used.

- A battery in the card can be used to power the fingerprint sensor. Gemalto has developed EMV cards with embedded batteries for other applications like LCD displays for Dynamic Code Verification for example (DCV). The DCV use case allows a precise energy consumption forecast over the complete life cycle of the card: with the code changing every 20 minutes, the battery will need to support 3x24x365x3 write cycle on the e-Ink display for a 3 years life cycle. That type of precise energy forecast is not applicable to a biometric sensor as the cardholder can perform a large (and unpredictable) amount of transactions per day.
- Power for the sensor can be delivered by the POS via the ISO14443 wireless bearer properties whereby the POS is magnetically inducing power into the card when with 4cm distance. Gemalto hold patents covering powered devices without the use of a battery.



4- Fingerprint sensor technology used for the Gemalto EMV card with a fingerprint sensor

Rationale for the no-battery approach

The DCV use case was perfect for an embedded battery approach for 2 reasons: First it is possible to set a maximum limit to the number of cycle changes of the dynamic code as the time between DCV changes is a specification set at design. Second the amount of energy used by a 3 digit e-ink display is very small.

In the case of a fingerprint sensor, the need for energy is more significant than an e-ink display and the number of usage cycles is unpredictable. Some card holders may need to perform tens of transactions a week during the several years' life cycle of their card. It is impossible to size a battery without over-sizing it to insure no interruption of service.

That is why the approach of using power by the POS magnetic induction is the preferred choice by Gemalto. It also adds one layer of security as no fingerprint reading is possible without the vicinity of a POS.

Sensor position

As biometrics is expected to deliver more convenience to the user by not requiring the need to enter a password, it is important that such card does not introduce a new burden due to a complex finger position on the card body to measure biometrics.

Bottom line the gesture is intuitive and natural for both contact and contactless modes and we believe users will not have to deal with any specific learning curve to start using such a product.

CVM completion time

The specified levels of FAR and FFR translate into a potentially longer CVM completion time. With FAR = 1 for 50000 and FFR = 1 for 20, CVM completion time can be kept under 2 seconds.

Red/green LEDs for a better user experience

CVM completion or failure can be materialized on the card body by the use of green and red LEDs. When the biometric verification is completed successfully, the user will be reassured by a green light displayed on the card body while the transaction will be processed positively. In case of a biometric mismatch, a red light will inform the user about the unsuccessful CVM attempt.

Impact on POS

All existing POS terminals are ready to accept contact and contactless payments using the biometric sensor card. There is no software kernel modification to be performed. PIN code entry may still be used as a fall-back solution for a given user who may not be in a position to use the biometric sensor – for example after a finger injury.

5- Enrolment using a secure tablet

Self-Enrolment for dispersed credentials – no central database

The use of a fingerprint sensor on the card body and the local match on card approach implies that when receiving a new card, the cardholder must go through an enrolment process. That process will be performed only once for good, for the entire card life cycle. When using the card, the biometric data measured will be compared with the reference data. It is possible to enroll multiple fingerprints: the product specifications and the issuer requirements will set that number.

The experience from Smartphones makers such as Apple and Samsung demonstrates that commercial biometrics got successful when the notion of self-enrolment appeared, and when the reference data got stored no longer in a central database but locally in a device than remains in the possession of the user. That is easy to perform on a smartphone as it is equipped with a fingerprint sensor. For EMV cards, the use of an additional equipment for the "write" step will be necessary.

The Tablet approach chosen by Gemalto tries to get as close as possible to the proven self-enrolment model that is very well accepted by consumers on Smartphones and very compliant will privacy protection regulations such as GDPR.

For present times, all foreseeable enrolment procedures must happen at the Bank branch or at approved premises by the bank as it requires a read/write equipment to install the minutiae inside the chip of the card. That equipment remains property of the bank and must be handled under its control.

- The cardholder must go to the branch and be assisted by a trained teller.
- The teller is presenting a secure tablet to the cardholder. This tablet is equipped with a card reader and with a fingerprint sensor. The UI is a very intuitive walkthrough process that is designed to be completed with a few minutes. Gemalto brings the benefits of a tablet designed for government applications such as eID and ePassport enrolment and field control. The EMV card use case is a subset of this features-rich tablet and the adaptation of the UI was the main redesign effort.
- The Cardholder provides his/her fingerprint via the fingerprint reader on the tablet and the tablet securely writes the minutiae inside the chip of the EMV card.

The crucial point about this tablet is that the cardholder biometrics data is solely measured to be then copied inside the secure chip on the card: at no point in time, the biometric data is kept inside the tablet, nor sent to a bank server or to a remote personalization bureau. This is a crucial privacy-friendly commitment from the bank to its cardholder.

24/7 kiosks at the branch as an alternative to the secure tablet

The use of the secure tablet requires the assistance of a teller at the branch. The tablet UI is self-explanatory so the role of the teller is mainly to control who is using the tablet and make sure the tablet is not lost or stolen.
A 24/7 kiosk version is possible as such a kiosk cannot be taken away as easily as a tablet. Gemalto has developed a multi-service kiosk initially focusing on card instant issuance at the branch. A foreseeable evolution of that kiosk is to perform more service for all aspects of ID verification for services enrolment. One service being the personalization of the biometric CVM for EMV cards.

Possible evolution toward self-enrolment using your own smartphone

On a longer term, looking at the smartphone self-enrolment process, one desirable evolution may be to skip the trip to the branch for enrolment and do it at home, on the smartphone. That would require an innovative way to write the biometric minutiae from the smartphone to the EMV card. Today, EMV card can communicate with the external worlds by only two methods: one being by establishing a physical contact with the EMV card chip pins (for example at the POS or at the ATM). The other one by using an ISO14443 short range wireless communication (NFC) . Additional communication methods will emerge in a near future.

6- Contact and contactless usage scenarios

PIN replacement

The main value proposition of such an EMV card with a fingerprint sensor is to remove the need for a 4 digit PIN entry. This can be extremely valuable for consumers using a large number of cards as remembering multiple PIN code can be very difficult.

For EMV payments using the contact mode at the POS terminal, PIN entry is requested today for all amounts – the use of on-card biometric CVM would apply for 100% of transactions and bring a tangible convenience to the card holder.

For EMV payments using the contactless mode at the POS terminal, there are two scenarios:
For low amounts (depending from one country to another), most issuers will allow CVM = No CVM to position contactless as a fast, simple, cash replacement. The use of biometric CVM may still not be activated for small amounts but some issuers may do so as the overhead in term of user experience is minimal.
For high amounts - whose threshold differs from one country to another, some issuers block all contactless payments and others authorized those with a CVM = PIN online. For that use case, biometric CVM brings a huge benefit as it can replace PIN online and bring a superb seamless user experience, even in countries only supporting offline PIN.

Thanks to biometric CVM, contactless can cover all payments amounts range and offer an identical customer experience for contact, contactless, for all amounts.

Identification for Social Benefits cards

Another new and interesting value proposition for Biometric CVM on an EMV card is that unlike PIN code which is an authentication method, biometry is an identification method. A PIN code can be shared by the genuine cardholder, but biometrics data can't be shared. This identification approach brought by biometry can be used by card issuers to ensure that the card usage benefits are really used by the genuine cardholder: that enables social benefits distribution via an EMV payment card. No change on the EMV payment performance, but a very robust identification of the cardholder.

7- Conclusion

Biometrics and Contactless: the ultimate EMV card experience at the store

Biometrics for the EMV card goes beyond convenience as it does for mobile. It brings the final touch that is needed to migrate the entire card experience to contactless, regardless the payment amount. The fact the card keeps its ISO form factor and can be used in contact mode is a long term insurance that EMV payments will remain the only true universal payment device. Contactless payment acceptance is growing fast, everywhere in the world, but it is foreseeable that even 10 or 20 years from now, there will still be places in the world when inserting a card will be mandatory to complete a purchase at the POS.

The Gemalto Biometric Sensor Payment card bridges the future with the entire legacy of EMV. It will bring the ultimate convenient user experience and the trust that is associated to biometrics. In fact, 10 years from now, none of us may want to be requested to remember a secret such as a password or a PIN code. It will be a blast from the past… but it will be a useful safeguard to travel the world. Gemalto is preparing a future in payment where mobile, wearable and card do coexist with areas of excellence for each of these devices. No one will travel the world without an EMV card for the 10 or 20 years to come, because it will be the only possible peace of mind when it comes to payment.

The EMV card has a great future as consumers' favorite payment method and that future starts today with fingerprint biometrics.

BANKING & PAYMENT

The world of financial services is changing fast and consumers look for ever more personalized, convenient, yet secure options to pay, communicate and interact with their banks. Gemalto offers a wide range of digital solutions to meet and exceed these demands. Banking & Payment regroups a broad range of solutions and offers to equip banks with the most advanced digital security and technology available.

Mobile & Apps | eBanking & eCommerce | Cards & Payments | Services for Banks

gemalto.com/financial

GEMALTO.COM

gemalto
security to be free