SMART PAYMENT ASSOCIATION

shaping the future of payment technology

Biometrics for Payment Applications

The SPA Vision on Financial Match-on-Card

November 2013

Table of Contents

1. **Introductory Remarks 3**

2. **The Use of Biometrics for Personal Authentication 5**

 2.1. **What is an ideal biometric trait? 5**

 2.2. **The card as a processor of biometrics information 7**

  2.2.1. Off-card comparison: pros and cons 7

  2.2.2. On-card comparison: pros and cons 8

  2.2.3. SPA recommendation 8

 2.3. **Technical decisions to design a biometric system 9**

  2.3.1. General Considerations 9

  2.3.2. Design trade-offs and the SPA proposal 11

  2.3.3. Designing the enrolment process 12

3. **Use Cases for biometrics in payment cards 14**

 3.1. **Opening Payment Accounts 14**

 3.2. **Authorization of Payment Transfers 14**

 3.3. **Simplifying the use of payment cards in developing countries 15**

 3.4. **Contactless Payments 16**

 3.5. **Generation of non-repudiable electronic signatures 16**

4. **Interoperability & Biometrics Standards 17**

5. **Addressing data protection concerns 18**

6. **Conclusions 19**

1. Introductory Remarks

In this paper the Smart Payment Association (SPA) reviews the case for implementing a biometric cardholder verification mechanism for card payment applications – examining the challenges and benefits this would deliver. Biometric authentication is a mature technology that has been used for many years in other markets/sectors. However, biometrics has not been frequently used for payment/finance applications.

This paper sets out a framework of the guiding principles, specifications and best practices that are required to underpin the expansion of biometrics into financial applications, and provides:

- A general presentation of the technology
- A comparison of the strengths and challenges of various approaches – including Match-On-Card and Off-Card matching
- A non-exhaustive list of use cases for biometrics in financial services
- An outline of the key design challenges for an efficient biometric system
- A brief review of core ISO technical standards
- A brief discussion on the biometric data protection case

To date, biometric technology has largely been driven by public sector applications to demonstrate identity in the areas of travel documentation, citizenship or residency status, or to grant access to secure locations. The SPA considers that a lack of interoperability and standards has hampered the adoption of biometrics by the finance sector.

During the last decade the biometric industry has undertaken substantial effort to establish a collection of international standards for the development of efficient, interoperable and safe components to sustain biometric authentication and identification systems.

These standards cover different biometrics modalities (or identifiers) – from fingerprint and facial imagery, to iris and vein recognition. SPA members have invested significantly in this standard-setting process.

Today, however, one thing is clear: at a time when extensive work is already taking place on all fronts to address the issues of standards and interoperability, scalability, privacy and security, the financial services sector must not be left behind.

The SPA believes the introduction of biometrics authentication would deliver significant benefits in terms of tackling card payment fraud by extending the cardholder verification methods available with the introduction of a third factor for identification (in addition to a PIN code or password). Furthermore, consideration could also be given to using biometrics to replace PIN-verification in order to increase the convenience aspect (not having to remember a PIN) and facilitate card use in developing regions.

Biometrics technology also provides the security required to better manage identity for a range of other finance services - including cross border e-banking (remote banking), contactless payments, online payments – as well as facilitating the delivery of banking services to populations previously underserved. This document also includes some use cases that illustrate the potential application of biometrics in the financial world. The list of use cases offers a representative sample of typical transactions, and does not provide an exhaustive set.

2. The Use of Biometrics for Personal Authentication

2.1. What is an ideal biometric trait?

The first decision to be taken when designing a biometrics system is to determine the biometrics trait that will be used. A biometric modality refers to a system built to recognize a particular biometric trait, along with the corresponding digital representation. A biometric modality is the combination of a biometric trait, sensor type, and algorithms for extracting and processing the digital representations of the trait. Biometrics modalities are standardized by ISO JTC1 SC37 technical committee.

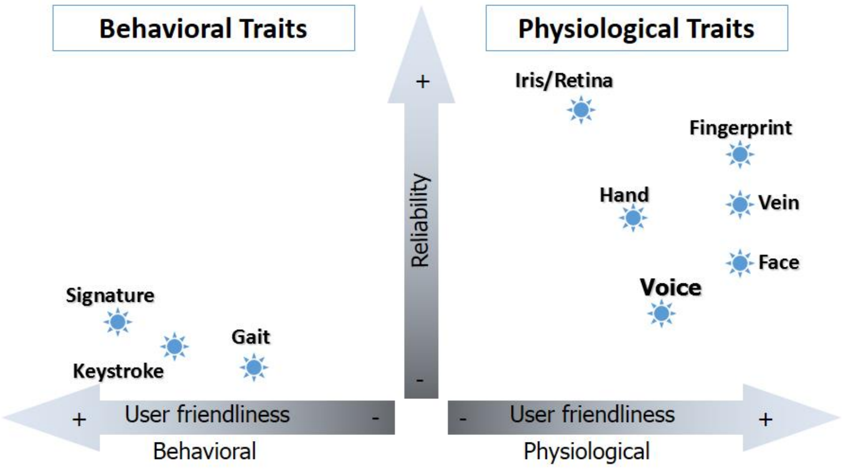
In practice, biometrics traits are only practical if the selected trait meets the five key criteria below:

1. Universal - every user must have the biometric trait
2. Unique - no two persons can have the same biometric trait
3. Permanent - the biometric trait must remain consistent over time
4. Credible - the biometric trait should be measurable
5. Socially acceptable - the biometric trait should not be perceived as invasive or as a risk for the person's health or privacy

While universality, uniqueness and permanence are intrinsic properties of biometric characteristics, collectability and social acceptability are subject to sample acquisition technologies, enrolment practices, subsequent processing and the storage of the biometric data. Convenience for the end-user is, of course, a critical component of success.

Should all above conditions be met, the biometric-based authentication system creates a strong link between the card where the enrolled reference is stored and its legitimate cardholder. For a given cost and transaction time, the strength of the link depends on the intrinsic accuracy of the biometric trait as well as other parameters like the quality of the enrollment process.

Figure 1 compares the most frequently used biometric modalities - behavioral and physiological - with respect to accuracy and user convenience.



2

Figure 1: Comparison of physiological and behavioral biometric modalities

- Physiological biometric traits are personal physical characteristics measured at some point in time. They include the face, the fingerprint, the hand geometry and the iris. In the early days DNA, ear shape, retina, skin reflectance and facial thermograms were also trialed.
- Behavioral biometric traits depend on the way an action is carried out by a person. In other words that they are learned or acquired over time. Hand signature, voice, gait, keystroke and lip motion can be used - and commercial products supporting these are available.

Intrinsic accuracy refers to the capacity of the biometric trait to avoid false matches. Accuracy is the very central security attribute of the biometrics system and, as Figure 1 shows, the iris is best in terms of intrinsic accuracy. Using the iris verification approach has very few false acceptances, meaning that an impostor has little chance of impersonating a legitimate user. However, when selecting a biometric trait for a given application, other criteria matter as well. For instance, the development of an iris capture sensor that is both convenient and unobtrusive is costly. Thus, different factors and attributes need to be carefully evaluated, including the social perception, the required cooperation, the acquisition time and the intrusiveness of the biometrics. All these factors are considered in Figure 1, aggregated as a "user convenience" unique attribute.

When considering the individual attributes for biometrics traits, the table in Figure 2 provides a more exhaustive comparison that does not take cost aspects into consideration.

As mentioned in Chapter 1, it is also important to understand that biometrics can be used as a stand-alone personal authentication methodology or combined with additional biometric and non-biometric authentication methods (for example, a PIN code) to increase security.

	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability
Face	High	Low	Medium	High	Medium	High
Fingerprints	Medium	High	High	Medium	High	Medium
Iris	High	High	High	Medium	High	Low
Retinal Scan	High	High	Medium	Low	High	Low
Voice Print	Medium	Low	Low	High	Low	High

Figure 2: Comparing biometric modalities (system cost is not considered)

Fingerprint is a biometric trait that represents a good trade-off in terms of security/cost ratio, benefiting from a relatively good social acceptance and not being invasive. Public testing implementations of card matchers for fingerprint minutiae are regularly undertaken, enabling future issuers of biometrics technology to compare on common grounds the performance of the different products on offer in the market. Last but not least, fingerprint minutiae specific encoding for storage and comparison in the smart card has been standardized.

For all these reasons, the SPA recommends the use of fingerprint minutiae as the base biometrics modality for payment cards. In order to develop the biometric system, other technical and organizational decisions have to be made. These are described in Sections 2.2 and 2.3 below. We begin with a discussion on the use of the smart card during the biometrics processing. The key point here is to compare Match-Off-Card implementations (where the card stores the biometrics reference, but the matching is implemented off-card) versus Match-On-Card (where the card stores the reference and compares the reference with the captured biometrics sample).

2.2. The card as a processor of biometrics information

To use a biometric system, individual persons must be first enrolled. During the enrolment stage, the reference biometric is captured, processed, associated with other identity attributes in a biometrics template and finally stored in a card issued to the enrolled person, who becomes the cardholder.

When using a biometric authentication system, a new sample of the cardholder biometrics is captured. A comparison (often referred to as 'matching' or 'verification' depending the sources) between the 'fresh' captured sample and the corresponding enrolled reference is then performed.

At present there are two ways to use the card in a biometrics processing system: Match-Off-Card and Match-On-Card. The next sections presents the pros and cons of both approaches and provides an SPA recommendation.

2.2.1. Off-card comparison: pros and cons

The off-card comparison (off-card matching) process takes place in the terminal or back-end system. ePassports are a good example of off-card matching. In this approach, because the terminal offers powerful computing resources with advanced comparison algorithms, the biometrics authentication is faster. However, other considerations have to be taken into account.

Off-card matching requires that the biometrics reference template is retrieved from the card. For security reasons the terminal should be authenticated by the card first. Moreover, such sensitive information is sent using a RF channel, where specific attacks (skimming, eavesdropping) are possible. As a result, a secure channel must be established between the terminal and the card prior to the transmission of biometric data. It should be noted that EMV specifications at present don't feature these two security services. The implementation of the off-card comparison process will therefore require a significant investment on the terminal side.

2.2.2. On-card comparison: pros and cons

In a Match-On-Card process, the enrolled biometrics reference data never leaves the card. The captured biometric is processed off-card and then transmitted down to the card encoded as a template for comparison with the biometric reference stored in the chip memory. The card compares both templates using a matcher - a high-performance algorithm. This means that the card must feature enough computational power to perform an accurate comparison calculation in very short transaction times (several hundreds of msec).

Not so long ago most available solutions were proprietary, creating a lack of interoperability that impaired large scale deployments and discouraged investments. Match-On-Card products proposed by biometric companies were not interoperable due to the fact that the algorithm in the card (verification device) needs to match another part of the same algorithm in the acquisition biometric device.

In order to overcome this unsatisfactory scenario, SPA members have undertaken a substantial standardization effort. ISO/IEC 24787 and ISO/IEC 7816-1 now provide the interoperability mechanisms and data structures to execute the biometric comparison on card. In addition, ISO/IEC 19794-2 has standardized a COMPACT CARD format for fingerprint minutiae template. With this compact format a single short APDU command is enough to convey the biometric template to the card for comparison. The card performance is therefore much improved and the results of the US MINEX II program prove that the Match-On-Card process can be implemented with a reduced transaction time.

2.2.3. SPA recommendation

The SPA recommends a Match-On-Card process for the fingerprint verification implemented in payment cards. Match-On-Card presents definitive advantages in terms of security and data privacy, a central concern for payment applications. For instance, the fact that the reference never leaves the card means that the attacker has no prior knowledge of the stored biometrics. This way, if an attacker manages to get a legitimate card, he/she has no hints on the particular fingerprint template (spoofings) that if presented to the card would result in a successful comparison.

In terms of performance, different marketed solutions are able to make secure on-card comparisons in less than 500 ms, which is compatible with transaction time requirements. Finally, the adoption of ISO standards for interoperability of Match-On-Card solutions should facilitate a good user experience.

2.3. Technical decisions to design a biometric system

2.3.1. General Considerations

The use of biometrics for personal identification/authentication raises the technical concern of the intrinsic variability of the capture process.

1. The SPA recommends the use of fingerprint minutiae for payment cards. As pointed out in Section 2.1, fingerprint minutiae offers a good level of interoperability, are processed efficiently by card technology and have a good level of social acceptance.
2. A second design choice is the type of card biometrics comparison to implement. At present two processes are used: Match-On-Card and Match-Off-Card. For security and privacy reasons, the SPA advocates the Match-On-Card option. With Match-On-Card, when the cardholder presents his/her biometrics to the sensor, the captured biometrics data are sent to the card for comparison with the stored reference. This way, the biometrics reference is never exposed, a good point for security.

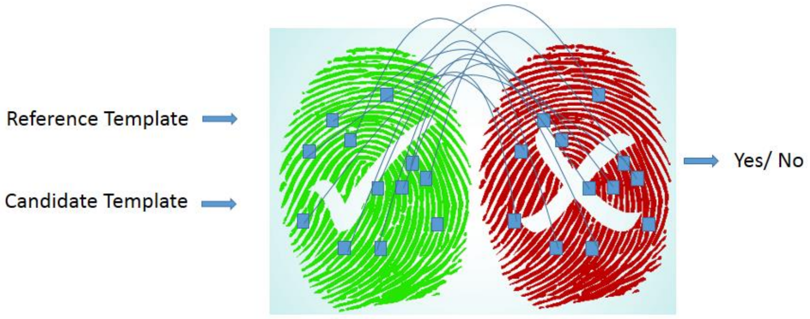


Figure 3: Point set matching between the enrolled reference and the captured sample

3. The third criterion is to set the biometrics system performance parameters, and in particular the thresholds serving to make the decision as to whether the compared biometric data match well enough or not. The comparison process measures 'similarity' – with 'similar measures' being considered to come from the same cardholder. This choice is fundamental because it is going to set the error rates and subsequent opportunities for circumvention when the objective is to reduce fraud and offer access to sensitive financial services.

4. The introduction of biometrics requires careful consideration of a number of practical issues, starting with the initial capture of the cardholder biometrics trait during the enrolment process. This digital representation of the enrolled biometrics will be the biometrics reference that is to be personalized into the payment card. The way the biometrics reference data is processed, stored and safely protected during the enrolment prior to the card personalization raises important design decisions.

5. The biometric data capture has a major impact on the system accuracy because it introduces significant variabilities; for instance, the environmental conditions at the point of capture (such as ambient light), the variable human interaction with the sensor and the lack of regular calibration of a sensor adds "noise" to the captured information. This variability of the captured biometrics is detrimental for the performance of the system. Standard stable conditions for enrolment and capture should be set out early.

6. The system should be designed to facilitate performance testing. The US MINEX II program provides a complete framework for testing the performance and interoperability of Match-On-Card fingerprint implementations. Thanks to MINEX we've seen a steady improvement in terms of the performance and interoperability of fingerprint minutia standards implemented in smart cards. This, in turn, has acted as a driver for more powerful card chips. The success of MINEX has led to its adoption as an ISO standard (ISO/IEC 19797-7).

7. The biometrics system should fit into the highly interoperable context of retail payment systems. In order to propose a biometric profile for interoperability that would be appropriate for the financial industry, the SPA has reviewed the core ISO technical standards that relate to biometric system properties, data attributes and data exchange as well as societal and legal issues. From this analysis we have selected those mechanisms required to develop a profile for biometrics to be implemented in a new generation of standard biometric match-on payment cards.

2.3.2. Design trade-offs and the SPA proposal

It is, of course, impossible to guarantee faultless operation. Inaccuracies are possible when capturing and representing the biometrics sample. Similarly, biometric data belonging to different users cannot always be differentiated by verification systems. At the same time, biometric data only exhibits unique characteristics if analyzed in sufficient detail.

Whatever the final solution adopted, the comparison process between the biometric template enrolled and the random biometric templates captured afterwards is a probabilistic one. In practice, this problematic comparison procedure introduces two types of errors quantified using two standard parameters: these are known as the False Rejection Rate (FRR) and False Acceptance Rate (FAR) rates. The FFR and FAR rates together are used to measure the performance of the biometric system, as explained below:

1. Two biometric samples from the same person may appear dissimilar due to random low quality adverse capture conditions. And as a result the legitimate person will be mistakenly taken for an impostor. This condition is referred to as a False Rejection Error and is quantified by the False Rejection Rate (FRR), which is a measurement of the probability that the legitimate person is not recognized as such by the system.
2. If an impostor is trying to impersonate a legitimate person, it may happen that a high similarity score is calculated if the two biometrics samples are close enough. As a result, the impostor might be mistakenly considered by the system as a legitimate user. This scenario is referred to as a False Acceptance and is quantified by the False Acceptance Rate, which measures the probability of an impostor being successfully authenticated.

In an ideal system the FAR and FRR should be very low, but both parameters are not independent. As is often the case with commercial applications requiring high security levels, the final design decision of which parameter to prioritize will be a trade-off between security and convenience as Figure 4 illustrates. The optimal system configuration can only be identified in relation to the specific financial operating conditions and of the assets to be protected.

It’s clear that payment applications must be highly secure. Therefore, when designing a biometrics system, the parameter to be minimized should be the False Acceptance Rate. On the other hand, it is evident that for commercial reasons an upper limit needs to be set for the False Rejection Rate since a biometric system frequently rejecting a legitimate user is unacceptable.

The SPA proposes the following tradeoff: a False Acceptance Rate of 0.01% should be achieved, with a maximum False Rejection Rate of 2% on one finger. A lower FAR could be achieved by comparing more than one fingerprint, or with biometrics multi-modality. The rationale for this proposal can be summarized as follows:

1. The proposed FAR/FRR settings represent a good level of performance for current levels of technology, and are comparable to what is going to be required in the US PIV card program.
2. Lowering the FAR further means increasing the FRR, which will itself then become random and highly dependent on the individual characteristics.

3. Utilizing a FAR of 0,01% offers the same level of security as a PIN comparison and ensures that cardholders not eligible for minutiae enrollment could continue to use the PIN with the same level of risk.
4. The processing time for a Match-On-Card with the error rates set above is less than one second with available commercial products.

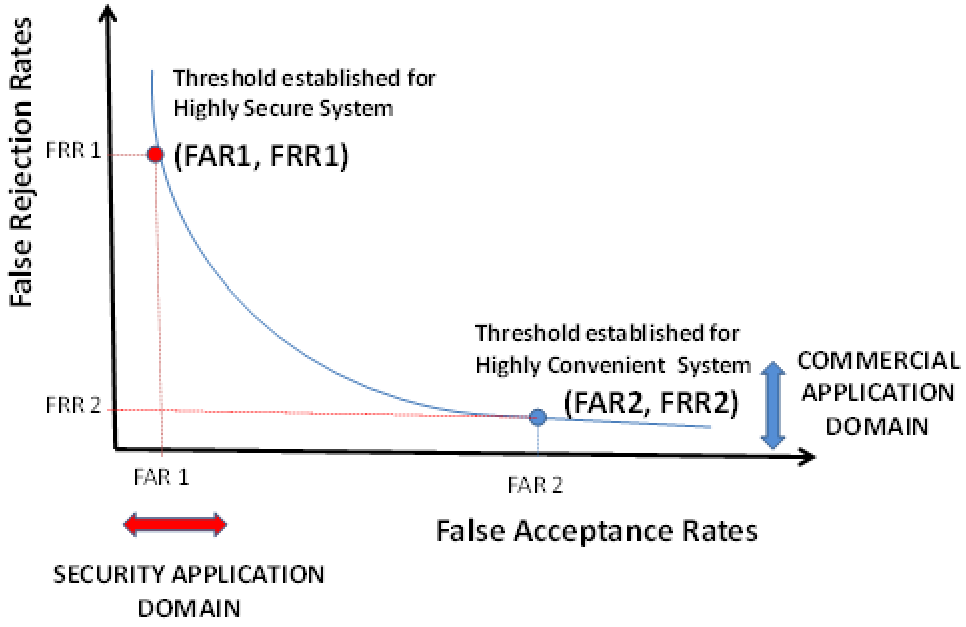


Figure 4: Different approaches for setting the comparison threshold for the application

2.3.3. Designing the enrolment process

Enrolment consists of collecting and formatting biometric, personal and payment account data for the issuance of the payment card. Enrolment is usually a prerequisite to operational use and enrolment for biometric services can be undertaking using a number of approaches. Enrolment is usually undertaken at fixed location sites where there is an attendant available who supports the applicant in effecting a successful enrolment.

There are four main objectives to consider when designing an enrolment subsystem:

1. Capturing high-quality fingerprints at the enrolment stage is essential to ensure the best matching rates. Early quality verifications during enrolment will ensure fewer rejection rates during the operational use of the card. However, if the quality of the capture at enrolment is not maintained consistently, the verification system is likely to experience unreliable performance. Responsibility for ensuring the quality and the security of biometric enrolment processes usually lies with contractual requirements. A performance management program should be put in place to monitor enrolment performance, applying corrective measures when required, and reporting enrolment performance to the issuer bank where enrolment is subcontracted to a third entity. As part of this program, the enrolment entity should develop metrics for measuring the impact of poor quality

enrolments (e.g. refer to ISO 29794-4). The design of the biometric enrolment service should allow for the right metrics to be collected.

2. The cardholder experience at enrolment is likely to impact the perception of the operational system and the acceptance of the technology. Indeed, the enrolment session may be the first time that the enrollee is in contact with biometric equipment. Actions to improve the enrolment quality or cardholder experience will have a cost/time impact on the enrolment service: the ease and speed of biometrics capture at enrolment and later verification is therefore important.

3. Fraud arises when falsified applicant declarations are made at the enrolment phase in order to obtain false identities. At enrolment the document that proves an individual's identity is created – therefore it is imperative that there is no room for error. The identity verifications employed during enrolment have to guarantee the applicant's identity as well as avoiding the duplication of applications by the same individual.

4. Specific data protection mechanisms should be designed for the enrollment process. Indeed sensitive personal data is likely to be stored for a certain period of time in a central database prior to personalization in the card. The mechanisms used for the transfer, storage and later retrieval of this data, including but not limited to the biometric reference, must guarantee the data's confidentiality and integrity.

3. Use Cases for biometrics in payment cards

Biometrics can replace a PIN code, or be used in combination with the PIN code or other knowledge-based authenticators. There is, however, a fundamental difference. The PIN is a knowledge-based authenticator and requires exact matching by the card. There is no ambiguity: either the PIN is known or not. When using biometrics, the notion of similarity appears. Error rates are therefore an inevitable consequence and must be defined to an 'acceptable level' for a given financial service.

Combining multiple authentication methods into an authentication protocol offers a higher confidence level and decreases the chances of repudiation and fraud. For instance, the individual in possession of a legitimate card who knows the card PIN code is able to produce a biometric sample that is similar to the one stored in the card can be assumed – with a high degree of confidence – to be the legitimate user.

As remote banking becomes increasingly important for the delivery of financial services to customers, it is important that such services are delivered in a safe and secure manner. Financial institutions should authenticate registered customers as the first step in a remote banking session.

The mechanisms used to authenticate the registered customer should be appropriate to the risks identified. In a more general way, financial institutions have to take appropriate measures to identify and register customers with whom they conduct business. Biometrics is a natural way to do this.

Next we'll offer an overview of use cases for EMVCo cards supporting biometric authentication for financial related operations.

3.1. Opening Payment Accounts

Financial institutions and other institutions providing payments services should be compliant with national requirements to execute 'Know your Customer' (KYC) processes, and to verify the customer's credentials in the opening and operation of an account. KYC processes are set out by national regulatory authorities and are based on robust identification and authentication processes during customer registration. By introducing biometrics for the identification of individuals, a bank proves their governance commitments and their willingness to implement rigorous KYC rules.

For KYC processes to be efficient, financial institutions should ensure that, during the registration process, the identification of the customer takes place using identity credentials that achieve the highest level of confidence. These identity credentials (national ID cards, e-Passports, e-Visas, residence permit cards, driving licenses) are usually issued by a public authority - and increasingly make use of biometric authenticators. A financial or payment institution may then proceed to capture a biometric sample from the customer, to compare it against the biometric reference stored in the official document. Should both match, the captured biometric data can be used as a biometric reference for a new payment and/or e-banking EMVCo card issued to the newly registered customer.

3.2. Authorization of Payment Transfers

Cross-border e-banking represents a further opportunity for biometrics authentication, due to the increased risk for identity theft and the greater difficulty in conducting effective credit checks on potential customers. Remittances, defined as a financial wire transfer with well established characteristics (relatively low-value, regular cross border payments that are highly concentrated in well identified geographic corridors from developed to emerging countries) is an area of future business development for financial and payment institutions.

As with any other wire transfer, remittances are subject to anti-money laundering/counter-terrorist financing (AML/CFT) regimes. As such, they rate particular attention from national institutions and central banks. A successful biometrics authentication as a pre-condition to a remittance payment creates a strong link between the identity of the payer and the transfer, and as above constitutes a proof of the willingness of the payment provider to comply with these national and international regulations.

3.3. Simplifying the use of payment cards in developing countries

Adding biometric functionality to an EMV card may contribute to making cards more widely accessible in areas with a high illiteracy rates. It also has the potential to facilitate access to financial services for individuals unused to PINs or passwords. In this context, biometrics offers a convenient, easy-to-implement solution to verify the customer identity when no other official credentials by government are available. If the biometrics authentication is based on an interoperable standard solution (refer to Section 4), regional payment cards will enable cash withdrawal and other transaction services at an ATM or self-service bank kiosk.

3.4. Contactless Payments

For contactless payments, the payer positions the card near the contactless reader and waits for the confirmation of the payment. Contactless cards deliver a convenient payment option and reduces queuing - as this form of payment is typically much quicker and, because a PIN is not necessary, can be used with one hand. Unfortunately, should a contactless card be stolen or lost it can be used fraudulently. Similarly, without a personal authenticator, a pure contactless card cannot (or should not) be used in ATM to withdraw cash.

Biometrics capture solves these problems by requiring a conscious action by the user when the card is positioned in front of the interface device (IFD). Here, biometrics capture can intervene even before the card is activated and, upon card authentication, the first command to be executed will be a verification of the biometrics sample just acquired.

However if not implemented correctly, this could have an impact on the throughput speed.

3.5. Generation of non-repudiable electronic signatures

Payment cards can support the provision of services that require use of legally accepted digital signature, such as:

- subscribing a contract for access to a new financial service
- confirming a remittance
- generating an e-Invoice
- proceeding to a mobile commerce transaction
- downloading and transferring electronic money.

Contact cards usually contain an electronic signature application which can be used for electronically signing documents. This signature is generated using a private key in possession of the signatory through public-key cryptography (e.g. RSA or ECC).

In the case of contact cards a PIN authentication usually activates the signing private key. As mentioned, contactless cards were not intended to be used with PIN codes. As a result, a more appropriate way to authorize this type of card is to use biometric verification to release the signing private key.

It is important to note that successful biometric authentication creates a second link between the signed message and the signatory, while reinforcing the non-repudiation due to the intrinsic non-transferability of the biometrics feature.

4. Interoperability & Biometrics Standards

Real life biometrics systems raise a host of interoperability issues. Parts of the same algorithm had to be implemented in distributed processors within the system, while the algorithms themselves, and the communication protocols, are largely proprietary. This is a classic scenario for innovative IT markets, but constitutes a barrier to prompt growth. Not surprisingly, the biometrics industry has collaborated in ISO technical committee structures (ISO JTC1 SC37) in order to enable the coexistence of these proprietary approaches.

Efforts were first focused on developing common encoding rules for biometrics modalities in order to ensure that any biometric sensor, for instance fingerprint images, delivers the same data structure built using common standard rules. This is a condition for the comparison of biometric data generated by different capture devices. The series of ISO/IEC 19792-X standards describe the standard representation of the different biometric modalities.

With this first fundamental level of standardization achieved, the next step was to solve the integration of the capture device into the larger biometrics system made up of heterogeneous computing devices executing proprietary algorithms. The classical solutions of common data structures for transmission and API specifications were privileged.

The CBEFF (Common Biometric Exchange Formats Framework) and the Bio API are two examples of standard solutions for the integration of the biometric capture device and comparison devices. Interestingly, these standards don’t specify the algorithms themselves but rather the templates used to encode various biometric identifiers. These identifiers enable the recipient of a biometric package of information to properly interpret the received information. In addition, the sender has to specify, in a common language, the kind of process that the recipient of the biometric information has to execute on the data. Thus, a common set of primitives to access biometric data processing services have been specified by the BioAPI standard.

So, should vendors implement proprietary technology, as long as (1) their products comply with the CBEFF standard, (2) the biometric trait is encoded using the standard and (3) the different parts of the system implement a common BioAPI, a first step towards true interoperability can be achieved.

Simultaneously, ISO has developed a complete set of conformance and interoperability mechanisms for sensors and applications. Products and solutions proposed by vendors can be evaluated and eventually certified against a common criteria – facilitating greater choice for issuers and system integrators.

The SPA outlines that the on-going standardization effort is focused on minimizing the variability intrinsic to the capture and processing of biometrics. As a result quality standards, specifying for instance the environmental conditions to optimize capture and comparison of biometrics traits, are under publication.

Additional documentation describing the biometrics standardization context in detail is available on request.

5. Addressing data protection concerns

In terms of privacy, biometrics constitute personal data to be protected in the same way as any other personal data. A payment card is a secure repository for the biometrics reference and may be well considered as a Privacy Enhancement Technology (PET). Let's discuss why:

- With Match-On-Card the biometrics reference never leaves the card. A sensitive personal data such as a biometrics reference should only be transferred to an authenticated entity when encrypted. EMV cards do not authenticate the terminal.
- The storage of the biometric reference in the card avoids the implementation of a central database of biometrics references. A key aspect for privacy is that the person keeps control on the release of his/her personal information. Central databases are out of the control of the individual person.
- The storage of the biometrics reference in the card instead of in a central database means that that only biometrics verification is possible, not the identification. The identification of the individual requires additional card retrieval of identifiers or identity attributes once the biometrics verification has been performed.
- With card-based biometric verification, the only authenticated claim is that the user of the card is the legitimate cardholder (provided that the captured biometric data is fresh). The card then acts as an authorization token without revealing the identity of the cardholder.

From the above it follows that a payment card supporting Match-On-Card can be implemented with the security properties inherent to make the card a Privacy Enhancing Technology (PET).

6. Conclusions

1. The SPA considers that the introduction of biometrics payment cards would represent an important step forward for the finance industry, opening the way to eliminating fraud for issuers and cardholders, reducing costs and providing the additional security and identity verification required to support remote or cross-border transactions.
2. The biometrics market is growing and new areas of application, including finance, should take advantage of the improved functionality and innovation of biometrics components and systems. Match-On-Card targeted bank applications will be available for implementation on any smart card platform – from Java to .NET and native integration in card operating systems.
3. A biometric Match-On-Card authentication solution – using a fingerprint in combination with a smart bank card – will meet new security demands while protecting the individual's privacy. Furthermore, Match-On-Card functionality binds the card to one specific person, removing the possibility of contactless fraud, or transferring or delegating card usage; making the card truly personal and truly secure.
4. Match-On-Card fingerprint recognition fits with EMV architecture - as cardholder verification is performed inside the smart card. It is completely scalable, and can be introduced to any segment of cardholders and activated on specific terminals. Crucially, as the function is integrated on the card and completely local, there are minimal infrastructure costs.
5. The new generation of card platforms makes it possible to simultaneously achieve security and performance when executing a biometric authentication process. Security is achieved by minimizing system error rates. Performance is the result of implementing fast cards whilst keeping error rates low.