WHAT'S NEXT FOR PAYMENT CARDS?

An introduction to *biometric authentication* and *Fingerprint on Card* technology

NXP

New payment cards, equipped with ***Fingerprint on Card (FPoC)*** technology, use ***biometric authentication*** to make payments safer and easier, but for FPoC cards to succeed, they need to deliver three things: a ***proven-secure architecture, seamless operation,*** and ***cost-effective production and deployment.*** Here's a look at how to deliver all three of these success factors and ensure that FPoC cards deliver the positive experiences that consumers look for in a new technology.

CONTENTS

ARE BIOMETRIC CARDS THE FUTURE OF PAYMENTS?

A big change is coming to the payment industry. ***Biometric payment cards,*** equipped with Fingerprint on Card (FPoc) technology, will use your fingerprint as a biometric to verify your identity and protect the payment transaction.

A sensor, integrated in the card, will scan your fingerprint while you hold it in the machine's reader slot or you tap it against the machine's display. Biometric algorithms will then extract data from the scan and compare it to the reference template securely stored on the card. If the comparison yields a match, the transaction will be authenticated and the terminal will complete the purchase.

Biometric authentication happens in an instant, so the transaction goes quickly, and there's no need to enter a PIN code or sign a receipt. It's a sleek, easy-to-use way to bring a new level of security to the transaction, so there's less risk of payment fraud or identity theft.

But, as with any new technology, FPoC is unfamiliar to end users and adds another dimension to the transaction. Some people may be reluctant to make the change and may be slow to adopt using the FPoC format for payments. The question, then, is whether FPoC cards will catch on. Will consumers, retailers, and banks welcome this new way of doing things?

We think FPoC cards will, indeed, become the norm – as long as they deliver three things:

High-level Security
so everyone trusts that private information, including fingerprint data, is stored safely on the FPoC card and protected from theft or manipulation

Seamless Operation
to prevent frustration at the payment terminal

Cost-effective Production and Deployment
to make the card itself affordable to deliver

There are several approaches to implementing FPoC technology and they vary in their ability to deliver all three of these criteria. There are different hardware architectures, different approaches to power management, different requirements for handling components and connections during production, and different methods for registering (or enrolling) fingerprints prior to putting cards to use. Before investing the time, money, and effort required to add FPoC technology to a card, it's important to know how these differences can impact a design and how they can either improve or detract from the consumer experience.

This paper offers insights into the success factors of a biometric card and shows how FPoC cards can be designed so they ensure increased security, fastest performance, and highest integration. We also look at how best to generate the positive consumer experiences needed for widespread adoption.

WHY PUT A FINGERPRINT SENSOR ON A PAYMENT CARD?

Biometric authentication, which refers to using a physical or behavioral characteristic unique to each person to confirm an individual's identity, has become a ***mainstream part of everyday life.***

Smartphones let us use our fingerprints to unlock the screen, investment brokers let us use our voice, over the telephone, to authorize transactions, and the ePassport gates in many international airports use facial recognition to know who we are. What used to happen only in science fiction now happens in reality, on a daily basis.

The number of fingerprint sensors embedded in devices is projected to reach over a billion units in 2020.

[Source: IHS Markit, 2016]

Biometric authentication is a highly secure way to confirm that the person claiming your identity is, in fact, you.

Biometric authentication is quick to execute and hard to falsify, so using it as part of the identification process adds an extra level of security and convenience. Also, because authentication requires that the person being identified be physically present to supply a biometric sample, the likelihood of fraud is even lower. These features make biometrics a compelling option for authenticating sensitive transactions of all kinds, including payments.

Fingerprints are a Solid Choice

So what makes a biometric good for authentication? There are lots of different characteristics that qualify as biometrics. Along with fingerprints, palmprints, voices, and faces, the veins in your hand, the way you walk, the way you sign your name, and even the way you type are unique to you. But some biometrics are easier to deal with, in a digital sense, than others.

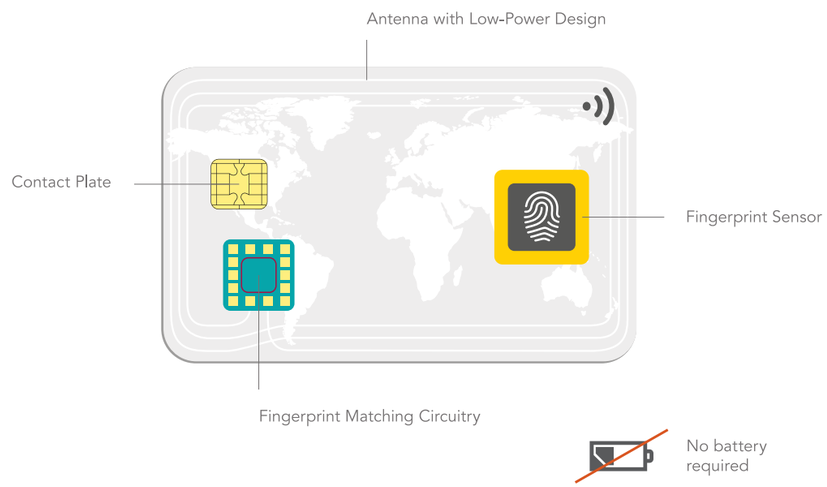
When it comes to payment cards, fingerprints are an excellent choice. They're relatively easy to capture and analyze using available sensor and processing technology. They're as unique as DNA and, for the purposes of identification, they're good because they remain pretty much the same from infancy to old age.

FPoC Technology

As mentioned in the previous section, the technology used to bring fingerprint-based authentication to payment cards is called, appropriately enough, Fingerprint on Card (FPoC) technology. The components used in an FPoC setup are so thin that the card itself looks much like any other bank card.

On one end of the card, there is the usual contact plate, currently used in today's "chip" cards, and on the opposite end is an ultra-thin, low-power fingerprint sensor for reading your fingerprint during a transaction. In between the contact plate and the fingerprint scanner there is circuitry for processing the fingerprint scan. This circuitry extracts the necessary data from the scan and compares the scanned fingerprint to an original, previously saved template of your fingerprint (known as the reference template), and then reports the results to authenticate the transaction.

FPoC cards are dual-interface cards, with support for contactless communication and the same form factor as a conventional chip card. They can be used in the existing infrastructure of payment terminals, wherever EMV payment cards are accepted.



The thin, battery-free form factor is compatible with the current infrastructure

A Compelling Approach

High-level, certified security

Seamless customer experience

Cost-effective production

Quick and Simple

Using the card is straightforward.

01

Initial Storage

When you receive your newly issued card, you begin by storing your fingerprint in the smartcard's memory. This initial fingerprint, called the reference template, serves as the basis for your identity and is later compared to the fingerprint captured during the payment transaction. This step is also called enrollment.

02

Capture and Extraction

When it's time to make a purchase, you press your finger to the card sensor while either inserting it in the payment machine's reader slot or tapping it to the machine's display. The card uses its embedded fingerprint sensor to capture your fingerprint, then uses algorithms to extract the data needed to compare the captured fingerprint to the reference template.

03

Matching

If the captured fingerprint matches the reference template, then you're good to go – you've confirmed your identity and authorized the payment terminal to complete the purchase.

Fingerprint authentication takes place so quickly that it's almost imperceptible, and there's no need to enter a PIN code or sign a receipt.

II. SECURITY

THE BEST ARCHITECTURE FOR PROTECTING DATA AND PREVENTING MANIPULATION

Using an FPoC card may be fast and simple, but just how secure is it? ***Can an FPoC card be trusted to ensure privacy and protect sensitive data?***

The short answer is yes, but it depends on the implementation. The process of storing, extracting, and matching fingerprints needs to be protected. How that protection is designed can influence the security of the solution. A quick look at each step in the FPoC process (initial storage, extraction, matching) highlights where security is most important and how best to ensure high-level protection.

Initial Storage: Secure the reference template

The first task is to store the reference template, the basis of your identity, in such a way that it remains protected at all times. The approach that offers the highest degree of protection is to store the reference template in a secure location on the card and, once it's written into memory, never let it leave the protected location. Storing the reference template in a secure, tamper-resistant IC, called a secure element, is a proven way to do this. The secure element acts as a vault, hiding the reference template from view and protecting it from attack.

Secure elements are designed from the ground up to protect against a broad range of attack categories and can be equipped with dozens of security mechanisms that defend data in different ways. Because they're tailor-made for security, secure elements offer a level of protection that's simply not available with other on-card storage options, including general-purpose microcontrollers.

In fact, secure elements are so widely recognized for their ability to protect private information that they've been used in the payment industry to store PINs and other sensitive data for many years. The same applies to secure ID applications, such as government-issued IDs and electronic passports. For more than a decade, secure ID cards have stored fingerprint templates in a Common Criteria-certified secure element.

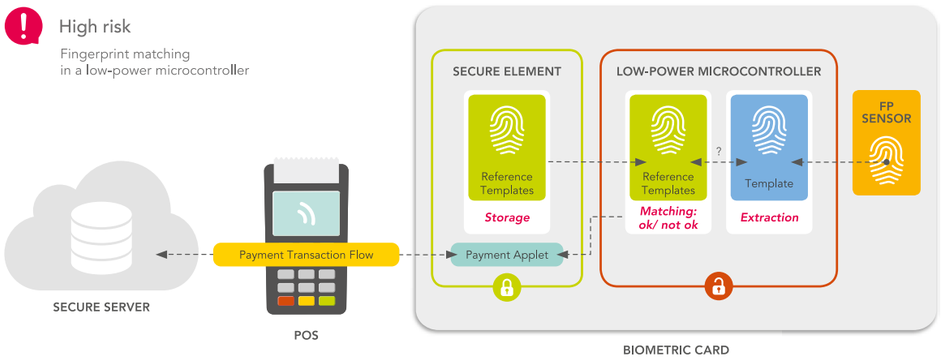
Extraction: Process data quickly

At the time of payment, processing the captured fingerprint requires strong calculation capabilities, to ensure quick extraction, but the security requirements are much lower. Extraction is essentially a format change – converting the image captured by the sensor to data that can be used for a match – and doesn't need the same level of protection as other steps in the FPoC process. The microcontroller receives the fingerprint captured by the onboard sensor and then extracts the data needed to do a match against the reference template. A low-power microcontroller is a cost-effective solution for extraction, since it does a good job with calculations while needing fewer security mechanisms.

Matching: Only in the secure element

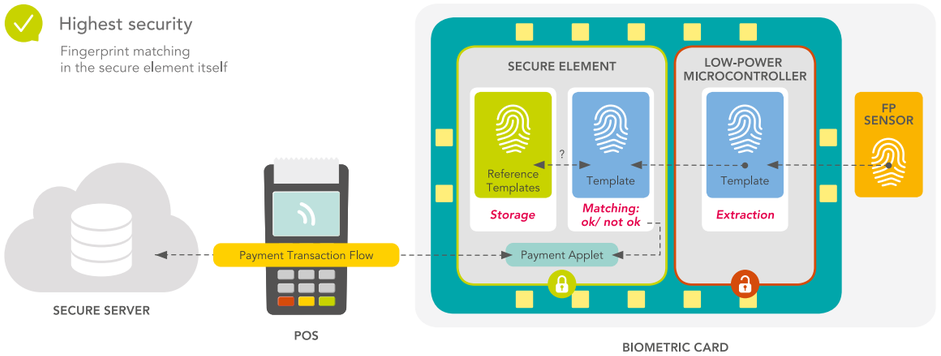
This is a critical step. The data extracted by the microcontroller is compared to the reference template to see if there is a match. The data associated with the reference template needs to be available for the match to take place. If the match happens in the microcontroller, then the reference template must leave the secure element and go to the microcontroller each time a match takes place. This is risky, since as soon as the reference template leaves the secure element, it's vulnerable to attack. The template loses its protection and can be either manipulated or stolen. The results produced by the match need to be protected, too, since they include information needed to verify payment. To maintain the right levels of protection, the best place to perform fingerprint matching is in the secure element. The secure element receives the extraction data from the low-power microcontroller, performs the match, and reports a simple "ok" or "not ok," without releasing the reference template or the data produced by the match.

Fingerprint matching in an external microcontroller introduces risk



Using software security to protect matching is NEVER as secure as using hardware security.

Using the secure element to perform fingerprint matching guarantees highest security



What happens in a microcontroller is vulnerable to manipulation.

What happens in a secure element remains hidden and protected.

The Safest Setup

The setup just described, with the reference template stored in a secure element, extraction performed by a low-cost microcontroller, and matching taking place in the secure element, represents the best combination of security and protection. The reference template remains hidden and never leaves its secure vault and matching takes place only in the protected environment of the secure element, minimizing the chances for manipulation. The payment transaction remains protected and trustworthy.

Going back to the question we asked at the beginning of this section, whether FPoC technology can be trusted to deliver a high level of security and privacy, the more precise answer is still yes – as long as a secure element is used to store the reference template and perform matching.

With this setup, the FPoC product is compliant with the General Data Protection Regulation (GDPR) and ensures the highest security and best protection of private biometric data. The biometric data never leaves its secure environment and, as a result, prevents its manipulation by an unauthorized party.

Fingerprint matching is only safe in the secure element

III. SENSORS

THE RIGHT SENSOR ENSURES SCALABILITY AND A CONSUMER-FRIENDLY EXPERIENCE

It's important ***to find the right sensor*** to use in an FPoC solution. The best choice creates a good trade-off between size, accuracy, and cost. Compared to other sensor technologies, active capacitive technology is the best option for integration onto a smartcard. Recent advances in active capacitive sensors, enabled by extensive R&D, are making it possible to integrate a fingerprint sensor into a payment card.

Active capacitive sensors generate an image by measuring the variations in electrical capacitance created by the ridges and valleys in the fingerprint. They are more robust than passive capacitive sensors and work with a broad range of skin types and conditions. Also, compared to thermal sensors, which generate an image by measuring the variations in temperature that ridges and valleys create, active capacitive sensors use much less power.

	ACTIVE CAPACITIVE	PASSIVE CAPACITIVE	THERMAL
Cost efficiency	High	Medium	Medium
Design flexibility	High	Low	Medium
Technology maturity	High	High	Medium
Security	High	Low	Medium
Convenience	High	Medium	Low
Power efficiency	High	High	
Mobile device adoption	High		

High Medium Low

Capacitive versus thermal sensor technologies

Active Sensors Are the Best Choice

Active capacitive sensors are the number-one choice for smartphones, in part because they deliver the necessary image quality and also because they enable a positive user experience. In creating an FPoC solution, the goal is to optimize an active capacitive sensor such that it can translate that combination of quality and convenience to a smartcard.

Software Makes the Difference

The hardware used to create the sensor provides the right foundation for fingerprint authentication, but the software behind the sensor is where the "magic" really happens. Higher-quality software can reduce the amount of processing power and memory needed on the device, and that can dramatically reduce the time it takes to read a fingerprint, known as the touch time. High-end software capabilities also make it possible to use a smaller sensor, thereby cutting the cost of solutions and giving device makers even more flexibility for design and integration.

IV. PERFORMANCE

SPEED, EFFICIENCY, AND ACCURACY

Consumers are only going to accept FPoC cards if they're easy to use. That makes ***performance an essential aspect*** of FPoC operation, since faster performance means fewer hassles or retries at the payment terminal.

There are three things that define FPoC performance: speed, efficiency, and accuracy. Speed refers to the time it takes to perform a fingerprint verification, efficiency refers to the amount of power required to run the verification process, and accuracy refers to how frequently the FPoC operation correctly confirms your identity.

Together, these three performance characteristics have a direct influence on how you, as a consumer, perceive the transaction. If the card falls short in one of these areas, your experience with FPoC cards can quickly turn sour.

Speed: Aim for a fast contactless fingerprint verification time

Operational speed is fundamental to the convenience of fingerprint biometrics. The verification process has to happen so quickly that it's almost imperceptible. Minimizing execution time means streamlining the three extra steps that biometric authentication adds to the payment process:

Capture

The card's embedded fingerprint sensor captures an image and transfers it to the card's low-power microcontroller.

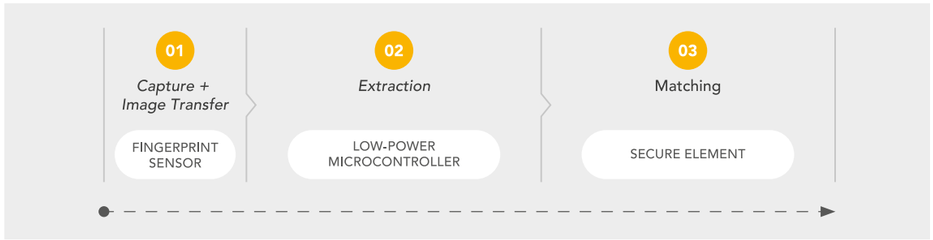
Extraction

The low-power microcontroller extracts the relevant data needed to match the fingerprint to the one stored in the reference template in the secure element.

Matching

The extracted data is sent to the secure element, where it is matched against the fingerprint stored in the reference template.

Separating the extraction and matching steps helps improve performance. This is partly due to the amount of data associated with the fingerprint image and partly due to the limited computing capabilities of a smartcard powered only by the PoS terminal.



The goal is to keep the FPoC transaction time as short as possible

The extraction process, which is more compute-intensive but does not need the highest security protection, executes in the card's microcontroller, a low-power IC specially chosen for the task. This lets the extraction process make use of the microcontroller's accelerated computing capabilities and reduces the time needed to complete certain mathematical operations.

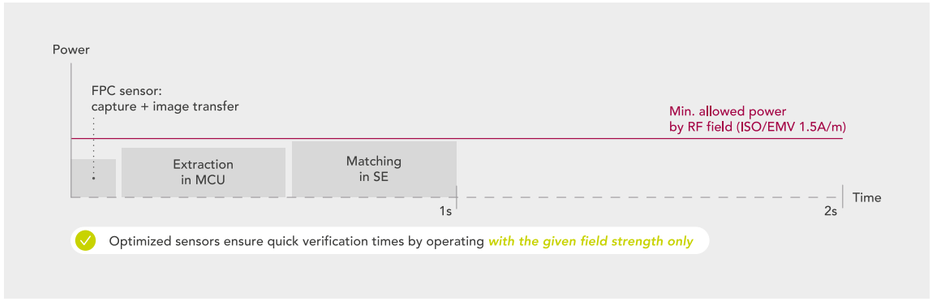
The matching process, which is less compute-intensive, executes in the secure environment of the secure element. From a security perspective, using a secure element for matching is the best approach because the final results are kept hidden in a secure area of silicon.

Choosing a sensor that quickly captures and transfers the image, and then dividing tasks, by placing extraction in the microcontroller and matching in the secure element, creates a solution that delivers both speed and security.

Efficiency: Choose low-power operation that doesn't need a battery or super capacitor

To reduce the cost of manufacturing and deployment, and to save retailers from having to upgrade their payment terminals to support biometric authentication, the FPoC format is intended to work with the existing terminal infrastructure. Today's in-place terminals are designed for lower-power operation and are specified at a minimum field strength of just 1.5A/m. As a result, a fingerprint sensor must be optimized to work only with the power provided by the payment terminal, without assistance of a battery or super capacitor.

Some FPoC solutions may be able to work with the available field strength, but are not fast enough to ensure a seamless payment experience. Some FPoC systems add a battery or super capacitor to the design to increase the power budget, but this adds cost and can impact the robustness of the design. Super capacitors are particularly tricky, since they need to be up and running for a certain amount of time before being able to power the card system, and this increases transaction time. An optimized, power-efficient sensor, in combination with optimized extraction and matching processes, ensures that the FPoC solution runs on the existing field strength.



Power efficiency versus processing time for fingerprint verification

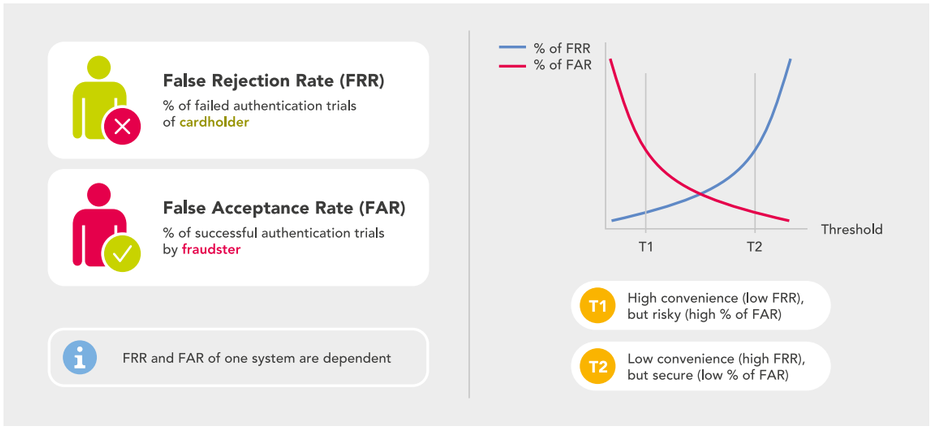
To operate in the existing infrastructure, the card needs to operate at 1.5A/m (the minimum allowed field strength of payment terminals), without using a battery or super capacitor

Accuracy: Balance the False Acceptance Rate (FAR)/False Rejection Rate (FRR) trade-off

When configuring the match parameters to be used with biometric authentication, there is always a trade-off between security and convenience. Focus only on security, and define parameters so tightly that it's difficult to get a positive match, and you risk compromising convenience, since the system is more likely to refuse an authorized user, even if the user tries repeatedly to verify the biometric. On the other hand, put too much emphasis on convenience, and define parameters too loosely, so it's easier to get a positive match, and you risk compromising security, since the system may allow too many fraudsters to gain authorization.

To balance this trade-off, and create a system that delivers acceptable levels of both security and convenience, developers perform tests involving thousands of attempts to access the system. They then use two metrics to track how often the system gets it right. The first metric, the False Rejection Rate (FRR), indicates how often the system wrongly rejects an authorized user, and the second metric, the False Acceptance Rate (FAR), indicates how often the system wrongly accepts an unauthorized user.

Comparing the FRR and FAR results makes it easier to find the area where there's an acceptable balance between security and convenience. As shown in the graphic, the parameters that yield results between T1 and T2 offer a reasonable trade-off.



The security/convenience trade-off between FRR and FAR

To create an FPoC card that delivers accuracy high enough to satisfy the strict requirements of payment transactions, developers typically aim to produce a FAR/FRR trade-off that is at least as good as present-day payment cards that use a 4-digit PIN. To do this, the biometric performance of an FPoC function is trimmed and optimized to reach 3% FRR at a FAR of 1 in 10,000, meaning three in every 100 genuine fingerprints are falsely rejected and one false fingerprint in 10,000 attempts is successfully accepted.

In general, the FAR/FRR trade-off is complicated by the fact that fingerprints, like other biometrics, can vary due to age, gender, origin, profession, and other factors. With FPoC technology, one of the biggest challenges in this regard is the size of the sensor and, as a result, the amount of data captured with each image capture. A large sensor, sized big enough to capture every aspect of the fingerprint on even the biggest of fingers, is cost-prohibitive, and requires more power than is readily available on a contactless card. These cost and power constraints mean the FPoC function has to use a sensor that is much smaller than the average finger.

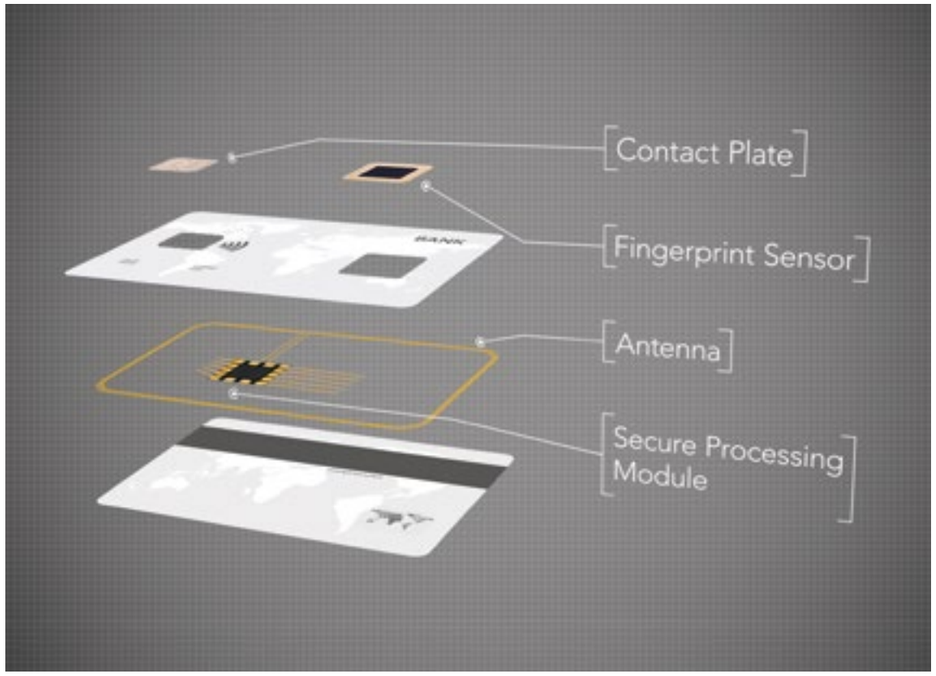
To address this, the biometric algorithm for fingerprint capture makes use of multiple image samples collected from the sensor. The algorithm then sorts, combines, and optimizes different image samples to produce the most efficient and most secure matching process. To optimize the statistical FRR and FAR settings of the system, the system needs to depend on large databases of fingerprints. These databases are carefully collected to take into account a variety of external factors, such as temperature, humidity, gender, age, and more. Complex machine-learning methods are then used to train and adapt the algorithm to meet the required system performance in all expected user scenarios.

V. PRODUCTION

COST, SCALABILITY, AND ROBUSTNESS

Miniaturization, in the form of increasingly small electronic components, is one of the things that makes it possible to put biometric authentication onto a payment card. ***FPoC technology is an excellent example of miniaturization,*** since it places several complex components, including a fingerprint sensor, a secure element, and a low-power microcontroller, onto a standard smartcard.

To create an FPoC card, you start with a standard payment card, which already has integrated circuits onboard to support digital authentication and the payment transaction. Then you add the necessary components and connectors for biometric authentication.



Design for Manufacturability

Present-day payment cards are produced using manufacturing techniques that enable very high volumes, with minimal yield loss and at a reasonable cost. This kind of high-volume scalability is key to meeting strong market demand while keeping payment cards affordable.

Since FPoC cards involve more circuitry than conventional payment cards, they will always be more expensive to manufacture than their conventional counterparts. But there are ways to minimize the extra expense. The goal is to design an FPoC card that's compatible with existing manufacturing techniques, so there are fewer changes to be made to the manufacturing line before starting production. By making a few important choices in the design phase, developers can create cards that can be manufactured using a standard production line and standard production processes.

Prepare for Hot Lamination

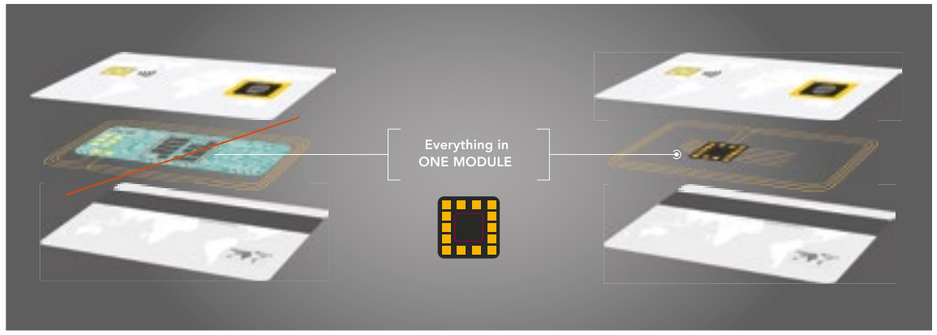
The manufacturing process is likely to use one of two lamination processes, hot or cold. Hot lamination uses heat to merge the PVC layers as they pass through the laminator. Hot lamination is the less expensive approach, and the one most commonly used for manufacturing payment cards, but it's only an option if the components used in the card can withstand the heat and pressure of the lamination machine. Cold lamination uses a pressure-sensitive adhesive that doesn't need to be heated, so it's safer for use with a wider set of electronic components, but it's a more expensive process.

Most components used for biometric authentication are compatible with hot lamination. Batteries and super capacitors are the exception. A design that uses batteries or super capacitors to increase the amount of power available for biometric authentication is likely to be too delicate for use with hot lamination, so the manufacturer is likely to recommend using cold lamination instead. As a result, adding batteries and super capacitors not only increases the cost of the components involved, it also necessitates a more expensive production process. Choosing a solution that doesn't require extra batteries or super capacitors is likely to be a better option from this standpoint.

Look for Integration

Another reason to eliminate extra components such as batteries and super capacitors is to simplify the design and reduce complexity in the manufacturing process. Using fewer components means there are fewer items to keep track of, fewer connections to make on the card, and fewer opportunities to break or damage something on the card during production, stress tests, or when the card's put to real-world use.

Using an FPoC solution that houses all the necessary components in a single module can lower production costs quite a bit, since the module can be delivered in a production-ready format and there's only one item to place on the card.



Eliminate the Flex PCB

A Flexible Printed Circuit Board, or Flex PCB, is a popular choice for assembling a biometric design during development and prototyping, but keeping the Flex PCB format when transitioning to mass production can cause problems. To begin with, the Flex PCB format most frequently used with biometrics, a polymer reinforced with glass fiber, isn't usually used with standard payment card manufacturing and is likely to require special handling, especially since it can be damaged by hot lamination. Even cold lamination can be tricky with a Flex PCB, though, since the PVC typically used with cold lamination doesn't always make a good connection with the Flex PCB. Using a Flex PCB may also create difficulties passing the usual stress tests, since the bending and twisting actions performed in these tests can be more than the Flex PCB can handle.

This is another instance where integration can help. Replacing the Flex PCB with a single module, which combines all the necessary components in one element, creates a more robust design. The module requires a very small PCB and serves to protect components since the IC housing acts as a mold cap. Using a mold cap for protection is a technique that has been widely used with contactless cards for several years now. It has helped make smartcards of all kinds more robust, since cards that use this approach are better at withstanding the mechanical challenges of production and everyday use.

VI. DEPLOYMENT

SECURE, COST-EFFECTIVE ENROLLMENT

We've alluded to it earlier, when talking about storing the reference template used to verify your fingerprint during a payment, but it's time to look more closely at the ***initial configuration of an FPoC card.***

Today's payment cards are equipped with an electronic circuit that secures the transaction. The card is essentially ready to go as soon as you get it. Your bank may assign a PIN code to use with the card but, beyond that, once you've notified the bank that you've received the card, you can usually start using it right away to make purchases.

With FPoC technology, it's a little different. Your new card is issued as a blank of sorts, with nothing stored on it for use with biometric authentication. Before you can use it to make purchases that are authorized using your fingerprint, you need to configure the card so it knows what your fingerprint looks like. This configuration step, which essentially teaches the card who you are so it can recognize you during a payment, is called enrollment.

How Enrollment Works

During the enrollment process, you store (or enroll) multiple views of your fingerprint on the card, so the card has biometric data to refer to when authorizing a payment. The biometric data associated with your fingerprint is called a reference template and is stored on the card's secure element.

High-Touch Enrollment Improves Performance at the Payment Terminal

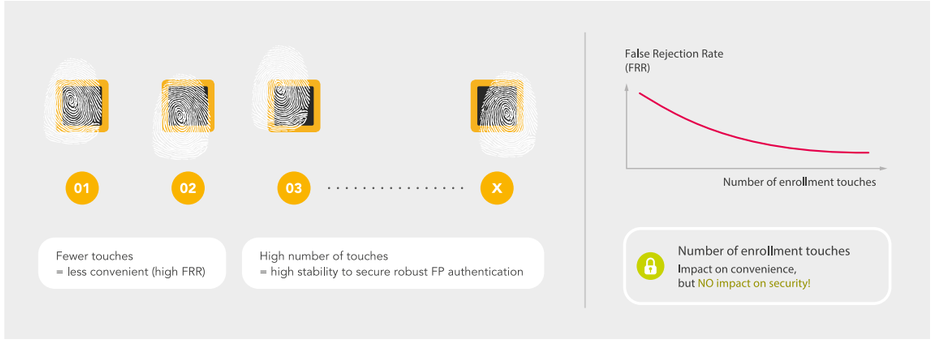
There are two main reasons why the card needs to store multiple views of your fingerprint. First, the sensor on the card isn't big enough to capture your entire fingerprint. The sensor is only large enough to read portions of your fingerprint and needs to have those various portions described and stored as individual reference templates that reside in the secure element. Second, you're unlikely to hold the card in exactly the same way each time you make a payment, so having multiple views of your fingerprint helps the card work with whatever way you happen to be holding the card while you're at the payment terminal.

To make sure the card has enough biometric data to perform a reliable match, the enrollment process involves saving more than one version of your fingerprint. The card does this by having you move your finger up and down on the sensor with slightly different placement each time. Storing multiple views creates a fuller description of your fingerprint, so the card does a better job of verifying your identity during a transaction. That translates into greater convenience because there are fewer errors or retries at the point of sale.

Deciding just how many touches are required for enrollment involves making a trade-off in convenience. For example, having to enroll too many views of your fingerprint can be seen as a nuisance. On the other hand, the upfront time spent enrolling views can save time (and thereby increase convenience) when the card is put to use, since the card performs more reliably if it has more reference templates to work with.

More touches = more stability and convenience

A high-touch enrollment process may be more time-consuming to complete, but it makes the card better at recognizing the authorized user, resulting in greater convenience. Another way to say this is that a full enrollment process, involving many views of your fingerprint, improves the performance metric we mentioned earlier, the False Rejection Rate or FRR. With a lower FRR, the card does a better job of knowing that you, the authorized user, are requesting the payment. The enrollment process doesn't, however, change the False Acceptance Rate or FAR. That's because the card will refuse to make a payment if there's no match, regardless of the number of reference templates stored.



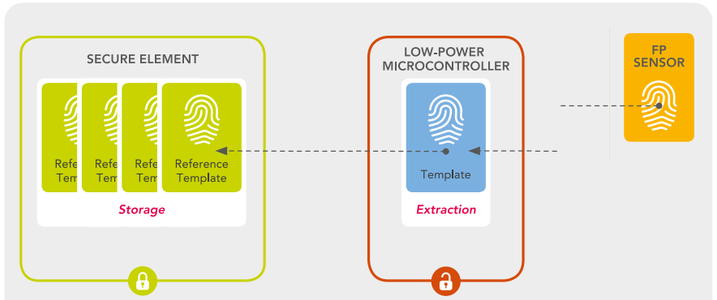
High-touch enrollment means less frustration at the payment terminal

A little extra time at enrollment ***reduces time*** at the terminal and ***greatly increases consumer convenience***

Direct Enrollment on the Card is Safest

It's important to note that we're describing an enrollment process that takes place directly on the card. This ensures the highest security and the best protection of biometric data, and also complies with the General Data Protection Regulation (GDPR). When you press your finger onto the card, the onboard sensor takes the image and transfers data associated with your fingerprint to the card's onboard microcontroller. The microcontroller then extracts the fingerprint data to be stored as a reference template in the card's secure element. The biometric data never leaves the secure environment of the card, thus preventing its manipulation by an unauthorized party. Aside from a power supply, there's nothing else needed for direct on-card enrollment.

High security

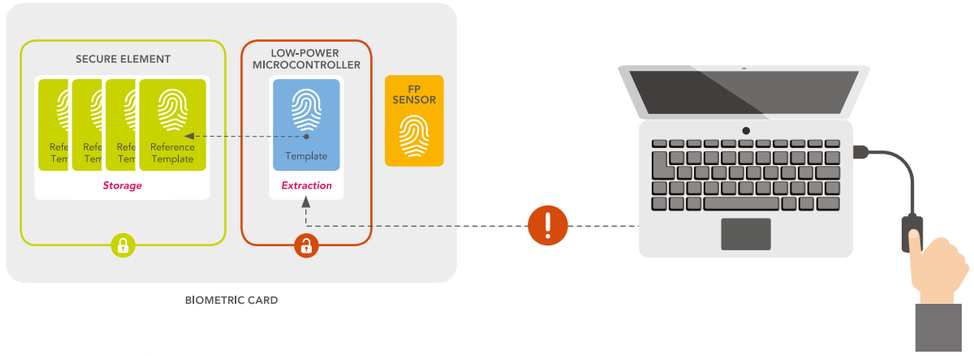


BIOMETRIC CARD

Direct on-card enrollment ensures highest security

Direct on-card enrollment is possible because all the necessary security and intelligence features needed to perform enrollment are already built into the card. There's no need for an external enrollment device, such as a standalone fingerprint sensor, to read your fingerprint. Your fingerprint data goes directly from your finger to the card. This essentially eliminates the risk of someone stealing your biometric data, since your fingerprint isn't stored on a third-party device, and hackers can't copy, manipulate, or steal your fingerprint before it reaches the card.

High risk

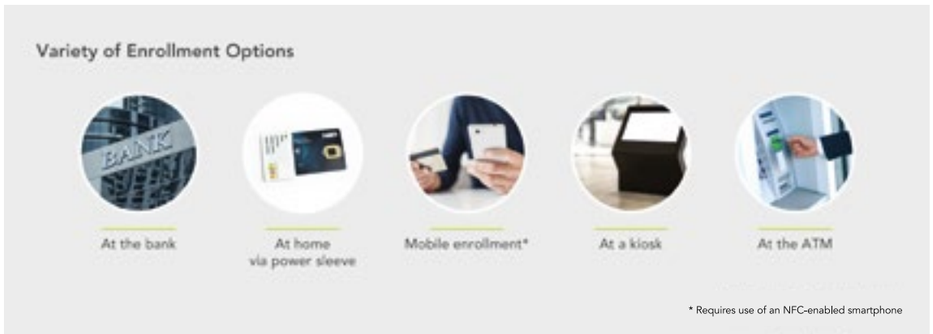


BIOMETRIC CARD

Off-card enrollment opens the door for manipulation and theft

How Banks are Approaching Enrollment

Since enrollment is a new concept with payment cards, banks are discussing how they'll manage the process so their customers accept the idea and get the best possible experience with their cards. There are a number of different approaches being considered.



Some banks are considering in-branch enrollment. The bank retains control over the process and can ensure the highest levels of security, but forcing you to make a special trip to the bank isn't particularly convenient. There may not be a branch nearby, and since so many banks now operate as online-only businesses, it may be difficult to find a physical location where you can do in-branch enrollment. A standalone kiosk or ATM machine can serve a similar purpose, having you interact with a bank-owned machine to do enrollment, but there still has to be a location nearby and you still have to make a special trip to configure the card before you can use it.

The more convenient approach is to let you do enrollment yourself, at home. The bank might, for example, supply you with a smartphone app, so you don't have to find a branch office or ATM machine and you can complete enrollment on your own terms, whenever it's best for your schedule. The drawback of an app, however, is that the smartphone needs to be equipped with Near Field Communication (NFC), so the phone can deliver power to the card the same way a payment terminal does. While a growing number of today's smartphones support NFC, banks can't assume that everyone has an NFC-enabled smartphone.

As an alternative to an app, banks can send you a special device, called an enrollment sleeve, along with your card. The sleeve can power the card and guide you through enrollment. A standalone enrollment device, using an integrated battery to deliver power to the card, can quickly take you through enrollment using optical indicators for feedback and guidance.

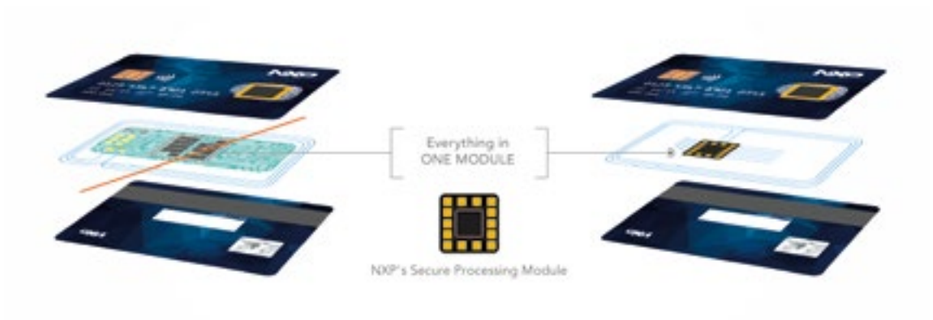
NXP Enrollment Kits are easy, private, and convenient to use

The card's biometric authentication process can be configured so it doesn't activate until the first time you use your PIN code at a payment terminal. That way, even if you lose your card or it's stolen before you complete enrollment, nobody else can configure the card and use it while pretending to be you.

VII. FPOC BY NXP

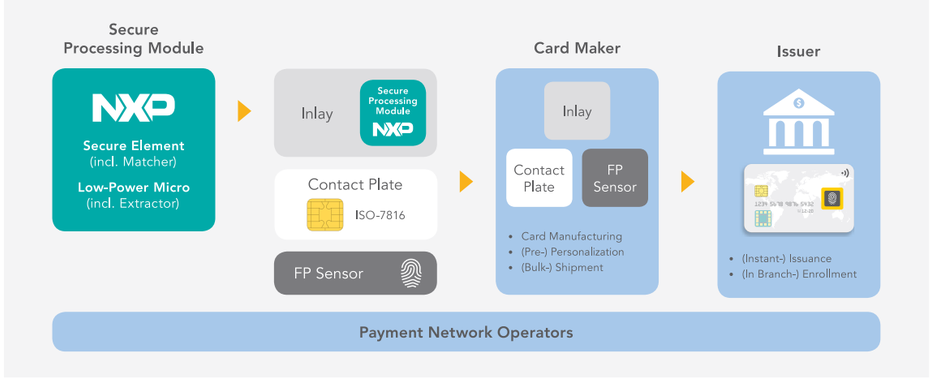
NXP'S SECURE PROCESSING MODULE AND ENROLLMENT KIT

NXP, a recognized leader in identification and smartcard technologies, has designed a ***high-performance, high-security solution for fingerprint cards*** that paves the way for a seamless customer payment experience. As a fully integrated, one-module solution, without the need for battery support, the NXP solution enables easy integration in a card body and uses standard manufacturing processes.



No need for Flex PCB with NXP´s Secure Processing Module

As a result, the NXP approach makes it easy for the whole industry to deliver the most secure, convenient, and integrated biometric solution.



NXP enables the smartcard supply chain for biometrics

High-Level Security

Our FPoC solution securely divides tasks between the secure element and the low-power microcontroller. The microcontroller performs extraction only. The secure element – based on a multi-layered architecture already proven in high-security applications – performs the fingerprint match and never lets the reference template leave its secure perimeter. The reference template and the matching results are protected from manipulation by outside forces, and the sensitive identity information relating to the fingerprint remains private. NXP´s FPoC solution is also GDPR compliant.

Impressive Performance

The NXP solution, based on NXP´s Secure Processing Module, enhances performance in terms of speed, power, and accuracy.

Speed – The added steps required for biometric authentication essentially go unnoticed, by using a fast biometric algorithm that splits extraction and matching into two separate processes so as to optimize speed and security.

Power – Highly efficient use of power means payment cards that use NXP's Secure Processing Module are ready to run on the 1.5A/m field strength supplied by the existing payment infrastructure, without using a battery or a super capacitor.

Accuracy – NXP´s Secure Processing Module delivers a FRR/FAR trade-off that's at least equal to a 4-digit PIN, and delivers a payment experience that is both secure and convenient to use.

Cost-Effective Manufacturing

NXP´s single-module solution is designed for high-volume manufacturing processes. Our solution delivers fast biometric performance using only the power provided by the payment terminal, so it doesn't need a battery or super capacitors. As a result, it withstands the higher temperatures used with hot lamination, requires placement of only one component, doesn't use a big PCB set up, and performs well in stress tests for everyday smartcard use. It is a streamlined, cost-effective solution that is both robust and scalable.

NXP´s Enrollment Kit

The NXP Secure Processing Module is designed to support any type of enrollment setup, and NXP supports customers with whatever's needed to configure enrollment in the setup phase. In addition, NXP´s developers are working on reference designs for various enrollment sleeve formats, so card issuers can configure the enrollment process during the initial pilot phase. Our standalone enrollment devices, called Enrollment Kits, use an integrated battery to deliver power to the card. Our Enrollment Kits are inexpensive to produce and quickly take end users through enrollment using optical indicators for feedback and guidance.

Optimized by Experts

To offer the highest levels of security, integration, and convenience, NXP partnered with other experts in the industry.

- ***Precise Biometrics*** provides the biometric algorithms for matching and extraction that enhance performance in terms of speed, power, and accuracy.
- ***Fingerprints*** provides the FPC T-Shape sensor FPC1321 and its driver, to ensure on-card verification takes place as quickly and securely as possible.
- ***Linxens*** provides a custom-developed, all-in-one biometric inlay that makes it easy to integrate NXP's FPoC technology with existing manufacturing processes.

NXP's Secure Processing Module enables

Highest Security
Fingerprint storage and matching in the secure element

High-Volume Scalability
One-module solution with no need for a battery

Seamless Customer Payment Experience
High-speed contactless fingerprint verification

VIII. FPOC FOR TODAY AND TOMORROW

WE'RE ALL IN

At NXP, we're excited about the ***promise of FPoC cards***. We see the many benefits biometric authentication can bring to payments, especially at a time when security and convenience are more important than ever.

FPoC technology combats card fraud by using fingerprints in a highly secure authentication process and gives consumers the freedom to make contactless payments without caps or having to provide a PIN number or signature. This unique combination of privacy and flexibility makes FPoC technology one of the most exciting payment innovations in a very long time.

Taken as a whole, FPoC technology holds great promise for everyone involved, from consumers to retailers and banks. It creates a card that uses biometric authentication to deliver high-level security and privacy, while ensuring a seamless customer experience. What's more, FPoC cards are cost-effective to produce and compatible with today's in-place manufacturing techniques. They're also quick to deploy because they already work with the global payment infrastructure.

Where We See This Going

Taking a longer-term view, we see FPoC technology enabling a broad range of new use cases. In the payment sector, FPoC technology can reduce fraud by protecting online banking and online payments, and can enable smart retail, with faster transactions in unmanned stores. Add a small display to the card, and you can dynamically create a Card Verification Value (CVV) to secure online payment. FPoC technology also has applications in eGovernment, by adding biometric authentication to secure ID documents, such as drivers' licenses and health cards. This is also true for access applications, where FPoC can help businesses and educational institutions secure access to restricted areas.

As FPoC continues to evolve, NXP will be there, delivering innovative solutions that remove barriers, increase security, and enhance user experiences.

Thanks to our partners, *Precise Biometrics and Fingerprints,* for their contributions to the chapters on Sensors and Performance.

Take the Next Step

To learn more about biometric authentication, FPoC technology, and NXP's Secure Processing Module, visit ***www.nxp.com/FPoC.***

Date of Release: November 2019