Trust issues? The need to secure contactless biometric payment cards

Henrik Nilsson

Henrik Nilsson, Fingerprints

Fingerprint authentication is a mature and trusted technology, refined through a decade of mass adoption across the mobile world. With biometrics now in over 80% of smartphones, it is also a preferred technology that has rapidly overtaken PIN authentication as the means to secure access to devices, make payments and secure applications.

The extensive R&D and market advances made during the smartphone world's mass adoption of fingerprint authentication has readied the technology for integration into new form factors. In line with this, fingerprint biometric-based payment cards are the latest big tech now hitting consumer wallets – with major French banks BNP Paribas and Crédit Agricole recently announcing more commercial rollouts.

The business case is clear. With a fingerprint sensor on-card, banks can add strong customer authentication to contactless verification, removing the hassle of PINs and the need for contactless payment limits. Billed as 'the biggest development in card technology in recent years', this promised boost to the contactless experience is hard to ignore.

But just how secure are these cards? The world of payment cards is complex. So before bringing biometrics to any new payment form factor, it is vital to ensure the technology can be seamlessly integrated into the existing infrastructure, while maintaining the highest levels of security.

Adoption success

Over the last decade, contactless payment cards have enjoyed rapid adoption, especially across Europe – enabling users to simply 'tap' to pay, without the need to enter their PIN code. In markets where contactless technology is highly used, 59% of consumers want to use their contactless card more, but are prevented by the payment limit.

However, fraud remains a significant consumer concern too. Without additional authentication, research shows that 38% of users feel contactless cards are not secure, and around half (51%) are very or extremely concerned about fraud. The result is that 30% of all users with contactless cards still don't use them[1].

In an effort to increase trust and reduce fraud, in 2018 the EU launched its Payment Services Directive 2 (PSD2) which implements new strong customer authentication (SCA) requirements. The directive states that an individual user can be authenticated by three types of factors: 'Possession' – something they have such as a payment card, physical keys, smartphone or security token; 'Knowledge' – something they know and remember, such as a password or PIN code; and 'Inherence' – something the user is or does, for example their fingerprint, signature, voice, etc.

SCA requires two of these authentication factors to be used – which means that when it comes to payments, the user needs to present the card itself, and must provide either a knowledge or inherence factor. In practice, this reduces the number of contactless payments, as it requires PIN-entry to be used more frequently as the default second factor of user verification. Yet the security of PIN-entry is limited, and its user experience is poor.

"With a fingerprint sensor on-card, banks can add strong customer authentication to contactless verification, removing the need for PINs and payment limits. But just how secure are these cards?"

Threat factors

A contactless payment card with on-card biometric authentication offers an opportunity to replace PINs with a solution that provides a better user experience and enhances security. With the added trust this brings to 'tap' card payments, banks could also finally remove the contactless payment limit, helping to increase transaction numbers.

Fingerprint sensors can now be manufactured in high volume at low cost, are compact and robust. Performance has been optimised too. This can be largely measured by the false acceptance rate (FAR) – the rate at which a third party is misidentified as a legitimate user. In modern payment card fingerprint sensors, the FAR rate stands at just one in over 20,000. However, nothing is ever 'un-hackable'. So while biometrics address some of PIN's most important fraud challenges, such as 'shoulder surfing' and shared PINs, the security of biometric payment cards also must be considered carefully before launch.

Essentially, a biometric system on-card (BSoC) is a contactless smartcard that also incorporates the fingerprint sensor needed to capture the user's biometric features, combined with the algorithms and processing power required for the matching process. It is worth noting that before a user can use a biometric system, they need to be enrolled. During enrolment, a template that represents the user's biometric features is created and stored on the card. This template is then utilised to match against the user features captured during subsequent authentication attempts.

In a BSoC, the on-card data flow during authentication can be divided into a number of key steps (as shown in Figure 1, next page). First, the image of the fingerprint is captured by the sensor. This is then processed and the feature, or relevant part of the image, is extracted to be matched against the biometric template stored on the card's processor chip – also known as the Secure Element (SE). If there is a match, authentication has been successful.

Within this approach, the image processing and feature extraction processes can be implemented either on a separate processor or the card's SE. The biometric match and storage of

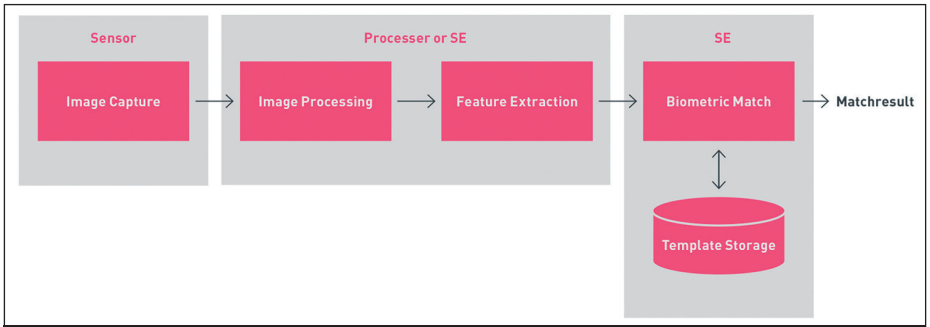


Figure 1: On-card data flow with the steps mapped onto on-card features.

templates is always implemented on the SE, due to its robust security levels. But several risk points emerge during this data flow: in the initial image capture at the sensor, during processing, and in the matching process.

"With card security, the key principle is to ensure attacks are too expensive or too complex to be feasible at scale, and to understand the threat actors. These are thieves looking to use the card to make fraudulent payments, or to attack the payment system itself"

Major threats

When developing any security solution, the key principle is to ensure that attacks are either too expensive or too complex to be feasible at scale. It is also crucial to understand the threats and threat actors aiming to exploit the key risk points.

For payment cards, these are thieves looking to use the card either to make fraudulent payments or as an entry point to attack the payment system itself. An individual thief may have some experience, but will normally lack the expertise and resources to develop advanced attacks. An organisation, however, can have both the expertise and resources needed to develop advanced attacks which can then be performed by individuals.

The primary threat in this area is the exploitation of cards that have been lost or stolen. The PIN protects against fraudulent payments for larger sums but, as mentioned earlier, the PIN is vulnerable to shoulder-surfing attacks, where a person is looking over the shoulder to see the PIN that is entered. This kind of physical attack is limited and not scalable, however, as the thief must learn a new PIN for each card. So while such attacks are troublesome for the individual, what thieves really want are attacks that are general and can be applied directly to all cards; or attacks that do not even require a physical card. The potential monetary gain here is much larger, and an organisation is therefore more prepared to spend resources finding such vulnerabilities.

So in terms of attacks on biometric systems, it's a major security benefit that any spoof attempt is a 'one shot' only – the thief only has one attempt to try and compromise a biometric system, unlike attempting to guess a PIN code which can be done numerous times. But while biometrics offer an answer to some of the vulnerabilities of PIN, careful consideration is still needed to mitigate the vulnerabilities they present – in order to make attacks either too expensive or too complex to be feasible at any scale.

The key attacks that can be made on biometric payment cards (shown in Figure 2) are as follows:

1. Biometric spoofing, also referred to as presentation attacks. This involves using something other than the user's finger on the sensor, to try and trick the matching operation into accepting the spoof as the correct finger.

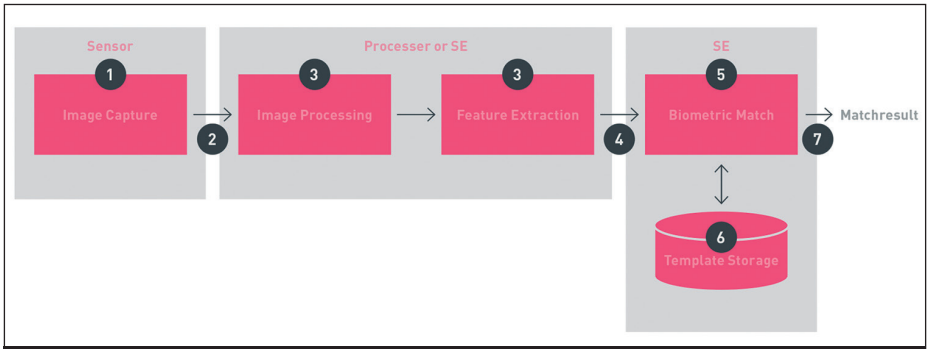


Figure 2: Attack vectors on biometric on-card system.

The spoof could be an artificial fingerprint, for example, or a latent fingerprint on the sensor that is re-activated.

2. Replay or manipulation of sensor image data. A replay attack requires the ability to inject a sensor image, instead of an image from the sensor. The image may have been captured from the same sensor at a time when the legitimate user used the card, but is replayed later.

3. Manipulation, disturbance of image processing and feature extraction. Here, the sensor image is processed and biometric features are extracted. This attack attempts to disturb the processing and extraction in such a way that the biometric match accepts the features it receives from the extracted image as the user's fingerprint.

4. Replay or manipulation of biometric feature data. If the attacker can gain entry to the interface between the feature extraction and biometric match, a replay or manipulation attack is possible.

5. Manipulation and disturbance of biometric match processing. This attack tries to influence the biometric match processing to produce a positive result, even though the extracted features are not from the user's finger. This can even happen when no features have been extracted.

6. Injection or manipulation of the stored template. Here the biometric template – the asset created during user enrolment and used to match the features – is either modified or replaced so that the hacker can make payments using the victim's card.

7. Replay or manipulation of the biometric match result. In this attack, the final match result is modified or replayed to fool the rest of the payment system into accepting that the legitimate user was verified for a payment.

"Biometric payment cards prevent spoofing or 'presentation' attacks using active capacitive sensors. These increase the image quality and use sophisticated matching algorithms to discriminate between the real user's finger and someone else's (or a forged) finger"

Mitigating the threats

Biometric payment cards have been developed to counter this range of threats. In the case of spoofing or presentation attacks, a move to active capacitive sensors has significantly mitigated the threat. It means that three-

Technology behind biometric cards

A smartcard for payment consists of a standardised card, and a payment application running on a highly secure on-card processing platform called the Secure Element (SE) – also known as the card's 'chip'. The card is inserted into a payment or point of sale (POS) terminal, and the card and POS communicate via electrical connectors on the card.

A contactless payment card is both powered by and communicates with the payment terminal. The terminal generates a field (typically at 13.56 MHz), from which the card then harvests the energy to power the SE and other on-card electronics. The field is also used by both the terminal and the card to send commands and responses. This communication uses its Secure Channel Protocol (SCP03). Typically, a PIN entered by the user on a terminal is sent via the field to the on-card SE to verify the user, by comparing the received PIN with the PIN stored in the SE.

A number of complex demands need to be addressed to make a payment card with embedded biometric security a commercial success:

1. Low cost. The security solution cannot push up cost by requiring more memory or processing power in the sensor host.

2. Ultra-low power consumption. ISO 7816 Class C cards – the standard card utilised in the payment world – have to power all electronics inside the card on the available magnetic field from the PoS, typically four to five mA. The power budget is very limited, so any security functionality integrated in the sensor can only draw a tiny fraction of the power.

3. Real-time performance. The time lag from the user holding up a contactless card against the reader until a match operation is completed and the user has been verified must be less than a second. Any security solution cannot add latency that disrupts this convenient user experience, and the under-one-second response time expected by consumers.

4. Ease of production. Smartcards are manufactured in the billions. The security solution cannot require complex, time-consuming production steps to establish the on-card security.

5. Attacks cannot be scalable. Each card must be unique. No attack should work on multiple or all cards, nor should it be able to work with zero or minimal work effort for each new card. In effect, attacks must be too costly to scale.

The latest contactless biometric cards are equipped with advanced sensors and security features that meet these demands. They provide multiple attack mitigation functions that can be layered and implemented throughout the manufacturing and personalisation process.

dimensional, conductive prints which closely resemble the texture of a real finger would be required – and spoofing such prints is a major (not to mention expensive) challenge, and nigh-impossible to achieve at scale.

Discriminating between the user's finger and someone else's (or a forged) finger directly relates to the quality of the sensor and the biometric algorithm. By increasing the image quality and using sophisticated matching algorithms, modern sensors counteract this threat. As mentioned earlier, an advanced biometric algorithm paired with a state-of-the-art sensor for payment cards is able to provide better than one in 20,000 FAR – more than twice as hard to achieve than guessing a PIN which, by comparison, has a rate of one in 10,000. Additional security can also be achieved by using more than one biometric identifier to authenticate the user.

The opposite of FAR is FRR – false rejection rate, which means the authorised user is misidentified as a non-authorised user. For the user, a false rejection is an inconvenience. So the ideal biometric authentication system therefore has minimal FAR and FRR, though in reality biometric authentication systems are somewhere on a curve where you either have high convenience (low FRR) but lower security (high FAR), or *vice versa*. Striking a balance between these is crucial. A sophisticated biometric algorithm pushes the curve down and provides high convenience while at the same time maintaining high security levels. Modern matching algorithms also include detection and protection against different types of spoof attacks.

The other main type of threat is injection and image replay attacks – where the sensor is replaced by a fraudulent device which provides a falsified image. A sensor-image authentication process provides robust security against such attacks. Authentication of the sensor image allows the on-card host (the processor or SE) to verify that the image originates from the sensor, not another device. Replay protection allows the host to verify that the image received was captured in that moment and a response to an image request from the host, not a replayed image.

More generally, the inherent privacy of on-device biometric systems provides protection against leakage of the biometric information needed for a subsequent replay attack. All biometric data is stored and processed on the device and personal authentication is entirely unique to that device. As such, the same finger would create a different template when enrolled on another consumer device. This means that attacks are considerably harder to scale, and the ability to attack a secondary system that the user is enrolled on is considerably reduced. Better connection between the sensor and the SE is also fundamental to ensuring strong data protection, as it moves sensitive information and processing away from the vulnerabilities of the sensor, to the robust protections of secure chip technology.

Data-conscious consumers can therefore feel reassured. Attacks on these biometric systems are harder to achieve, especially at any scale that would be valuable to hackers, and the consumer's encrypted data stays with them at all times on their device, never leaving the card.

Protecting processing and templates

The final type of attack targets the execution of the biometric software itself. These hacks can consist of fault injection attacks, or they inversely measure effects such as variance

With biometric cards, data-conscious consumers can feel reassured: their encrypted data stays with them at all times, never leaving the card.

in time, power consumption or in electromagnetic fields caused by the execution. This variance is known as 'side-channel leakage' and the data is then used to optimise fraudulent inputs.

Again, sophisticated algorithms form the main point of defence. The trend here is to develop sensors that are capable of conducting the entire feature extraction and matching process within the Secure Element itself, without the need for an additional processor. This progression is a major technical advance. SEs remain one of the most robust hardware security solutions available, and consolidating the process into the SE eliminates many points of risk in the data flow.

Ready to roll

In summary, on-card biometric authentication is a natural evolution for contactless card payments. These cards offer an answer to fraud fears and security requirements, without impairing the convenience of paying with a 'tap'. However, ensuring that robust security and privacy protections are in place is still fundamental to the launch and successful mass adoption of any new technology – especially when it comes to payments!

Biometric solutions can provide this security both through the quality of the biometric processing itself, and the protection and storage of assets such as the sensor image and templates. The R&D work already done, and feedback from over 20 global trials and commercial launches so far, mean that modern biometric payment card sensors deliver the required high-quality software and algorithms, and more robust protection of sensitive biometric data. By adding biometric authentication to contactless payments, the financial world can finally eradicate the need for PIN entry and remove contactless payment limits, enabling a consistent, simple and hygienic payment experience.

About the author

Henrik Nilsson is the director of product management at Fingerprint Cards, responsible for the company's biometric offering in the payment and access segments. Since joining Fingerprints in 2013, Henrik has collaborated with customers to optimise biometric products across the mobile, PC and IoT space. He holds a BSc in Economics and an MSc in Electrical Engineering from Lund University and has extensive industry experience, having previously held roles at Ericsson and ST Ericsson.

Reference

1. 'Biometrics – The missing piece of the payment card puzzle?'. Fingerprint Cards, 2018. Accessed December 2020. https://www.fingerprints.com/uploads/2018/05/fpc-smartcards-ebook-en.pdf.

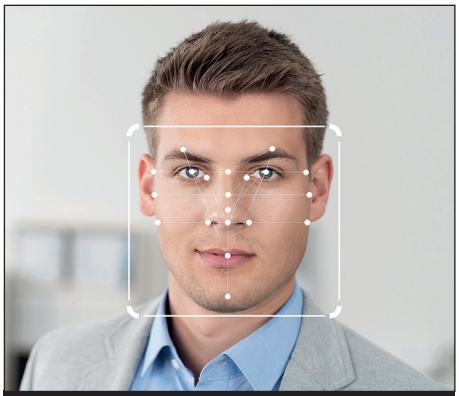
How biometrics can help airlines take off again

Peter Sutcliffe

We speak to SITA director Peter Sutcliffe about the role biometric technology can play, as airlines and airports progressively resume their operations following the Covid-19 pandemic.

BTT: SITA has said that smart biometric technology is fundamental for airports and airlines to safely resume their operations following the Covid-19 emergency. Why is it so vital?

Peter Sutcliffe: Airports and airlines – along with other ports and carriers in the wider travel industry – face an extraordinary challenge.



Biometrically linked identities – where your face is your boarding pass, for example – is one of the fundamental technologies that will support airlines in resuming their activities more efficiently.

Covid-19 has transformed the air transport industry. 9/11 brought security to the forefront of air travel, but with Covid health is the new priority in the return to the skies. We are now seeing some recovery in air travel, but the challenges of implementing shifting travel corridors and the re-opening of borders requires more agile operations that can respond to changing policy, often at short notice. The financial pressures the industry is facing are vast and the need to contain costs – to do more for less – is critical. Greater efficiencies and agility will depend on accelerating automation and technology, to keep air travel attractive and commercially viable.

Biometrically linked identities – where your face is your boarding pass, for example – is one of the fundamental technologies that will support carriers and ports in resuming their activities more efficiently. This will also help build confidence with travellers, and improve identity assurance to support traditional security needs while managing health risks. But the use of biometric technology alone will bring limited benefits for airports and carriers. The benefits are more far-reaching when biometric technology is combined with other technologies to provide greater identity integration, traveller automation and self-service.

BTT: The air industry is under major financial pressure, following the drop in global travel caused by the pandemic. How can airlines and airports be expected, or persuaded, to invest in expensive new biometric tech in these circumstances?

Peter Sutcliffe: It is certainly not an easy time for the industry. SITA is acutely aware of the challenges that airlines and airports are experiencing. However, all industry stakeholders recognise that countries can restart travel safely and efficiently. Real savings can be made in the long term with the right solutions to support the recovery. One of the first steps we recommend is that airlines and airports undertake a cost-benefit analysis and a risk assessment into whether an investment is justified. As part of this analysis, considerations would include the likely scenarios around the industry's direction over the next 10 years.

For example, we know that the International Civil Aviation Organisation