FINGERPRINTS

BRINGING SECURITY TO CONTACTLESS BIOMETRIC PAYMENT CARDS

WHITE PAPER

CONTENT

1. BIOMETRICS IN CONTACTLESS PAYMENT CARDS

1.1 Improving the user experience of contactless

In the last decade, contactless cards have seen rapid adoption, especially across Europe, enabling users to simply 'tap' to pay without the need to enter their PIN code. In markets where contactless is highly used, 59% of consumers want to use their contactless card more but remain prohibited by the payment limit. However, fraud remains a significant consumer concern too. Without additional authentication, research shows that among users of contactless cards, 38% say contactless cards don't feel secure and over half (51%) are very or extremely concerned about fraud. The result is that 30% of all users with contactless cards don't use them[1].

In an effort to increase trust and reduce fraud, the EU launched Payment Services Directive 2 PSD2, implementing new strong customer authentication (SCA) requirements.

A user can be authenticated by three types of factors:

OWNERSHIP
Something the user has, for example a payment card, physical keys, smartphone or security token.

KNOWLEDGE
Something the user knows and remembers, such as a password or PIN code.

INHERENCE
Something the user is or does, for example a fingerprint, signature, voice etc.

SCA requires two of these authentication factors, meaning when it comes to payments the user needs to present the card itself plus must provide either a knowledge or inherence factor. In action, this reduces the number of contactless payments, requiring PIN-entry more frequently as the default second factor of user verification. But the security of PIN is limited, and its user-experience is poor.

1.1.1 THE PIN PROBLEM

Consumers are overwhelmed and frustrated by the number of PINs and passwords to remember in today's digital age. And, if they forget their code, there is the added inconvenience of needing to issue a new card – a significant cost to banks, too.

20% of European users have the same PIN for more than one payment card, while 16% share their PIN with family and friends[1], heightening the PIN's vulnerability to fraud. The PIN is also susceptible to over the shoulder or 'shoulder surfing' attacks, where an attacker gleams the PIN when it is being entered by the user. In light of the COVID-19 pandemic, the PIN code also creates hygiene concerns. With the WHO encouraging contactless payments where possible[2], consumers are keen to avoid interaction with shared payment terminals wherever possible.

A contactless payment card with on-card biometric authentication offers an opportunity to replace forgettable and insecure PINs with a solution that not only offers a superior user experience, but enhances security and reduces fraud. With added trust to 'tap' card payments, banks can also feel empowered to finally remove the contactless payment limit, increasing transaction numbers.

With biometrics, contactless cards can meet SCA requirements and alleviate consumer fraud fears, without impacting the seamless UX.

1.2 Technology for biometrics system on-card

Biometrics in its simplest sense is capturing unique physical features to identify the user, such as the iris, face, and fingerprint. It has been immensely successful in the mobile phone market – over 70% of all shipped smartphones now include biometrics[3], with fingerprint commonly replacing the PIN to unlock devices, make payments and secure applications.

The extensive R&D and market advancement during the smartphone world's mass adoption of the technology has readied the technology for integration into new form factors. Fingerprint sensors can now be manufactured in high volume at low cost, are compact and robust.

Performance has been optimized too. This can be largely measured by the False Acceptance Rate (FAR) - that is, misidentifying a third party as a legitime user – which, in modern sensors for payment cards standards at a rate of misidentification of one in over 20,000.

The world of payment cards is complex, however. Bringing biometrics to cards requires careful consideration and innovation to integrate biometrics seamlessly, and with the highest levels of security, into the form factor.

1.2.1 BRINGING BIOMETRICS TO PAYMENT CARDS

A smartcard for payment is a standardized card with a payment application running on an on-card, highly secure processing platform called a Secure Element (SE), also known as the card's 'chip'. The card is inserted into a payment terminal or Point of Sale (POS) 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), that the card then harvests the energy from to power the SE and other electronics on-card. The field is also used by both the terminal and the card to send commands and responses, the communication uses Secure Channel Protocol (SCP03). Typically, a PIN entered by the user on a terminal is sent via the field to the SE on-card to verify the user by comparing the received PIN with the PIN stored in the SE.

Figure 1. A contactless biometric smartcard.

Figure 2. The universal smartcard reader symbol indicating readers and cards that support contactless payments.
The Contactless Symbol is a trademark owned by and used with permission of EMVCo, LLC.

A BSoC, or biometric system on-card, is a contactless smartcard that also incorporates the fingerprint sensor needed to capture the user's biometric features, 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 enrollment, a biometric template that represents the user's biometric features is created and stored securely on the card. This template is then utilized to match against the user features captured during subsequent authentication attempts.

The on-card data flow during a customer verification operation can be divided into four main steps:

1. **Image Capture**
2. **Image Processing**
3. **Feature Extraction**
4. **Biometric Match against stored template**

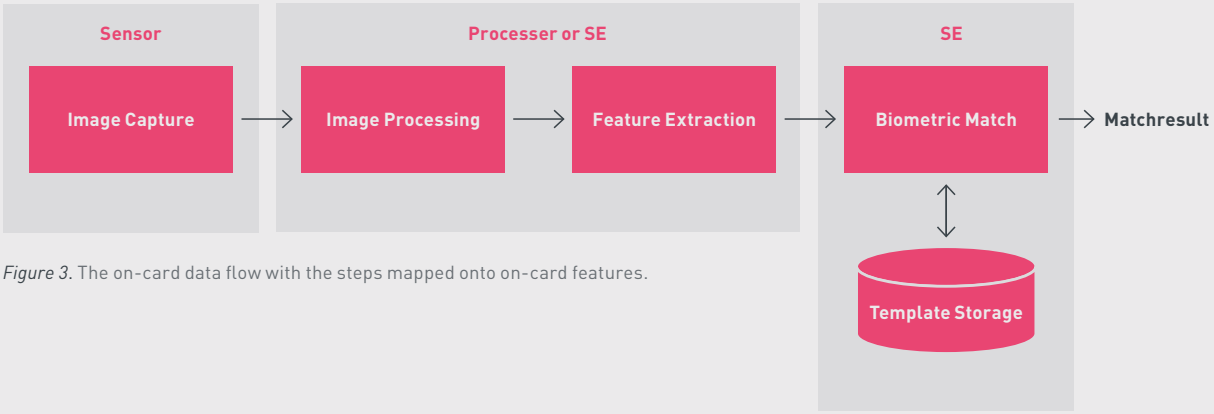

Figure 3. The on-card data flow with the steps mapped onto on-card features.

The image processing and feature extraction can be implemented either on a separate processor or the card's SE. The biometric match and storage of templates is always implemented on the SE, due to its robust security levels.

2. THREATS AND THREAT ACTORS

When developing any security solution, it is crucial to map the threats and threat actors. For payment cards, these are thieves looking to use the card either to make fraudulent payments or as an entry of attack on the payment system itself. An individual thief may have quite some experience, but normally lack the expertise and resources to develop advanced attacks. An organization however can have both the expertise and resources to develop advanced attacks which can then be performed by individuals.

The primary threat is to use 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. Although 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 that do not even require a physical card. The potential monetary gain is much larger, and an organization is therefore more prepared to spend resources finding such attacks. Considering attacks on biometric systems, it's also 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 a traditional door lock that can be tried several times or attempting to guess a PIN code.

The threat actors are after monetary gain. And while biometrics offers an answer to some of the vulnerabilities of PIN, careful consideration is still needed to mitigate the vulnerabilities any new security solution has.

Nothing is ever 'un-hackable', but the goal of any security solution is to make attacks either too expensive or too complex to be feasible at any scale.

2.1 Attacks and scenarios

Looking at the on-card data flow again, there are several attack vectors that can be identified where a threat actor can try and influence the operation of a BSoC.

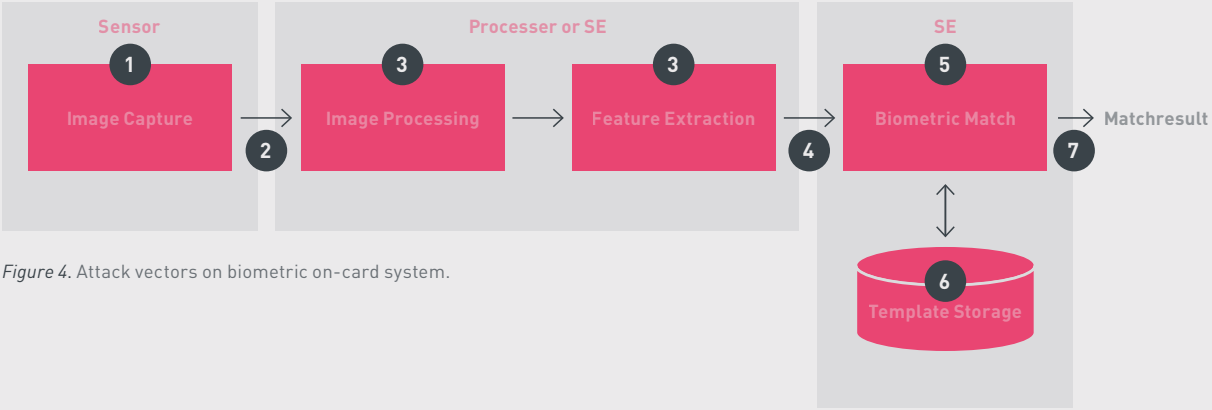

Figure 4. Attack vectors on biometric on-card system.

The attack vectors from one to seven are:

1. Biometric spoofing. This means something other than the user's finger is used on the sensor to try and trick the matching operation to accept the spoof as the correct finger, called presentation attack. The spoof could be a latent fingerprint on the sensor that is reactivated or an artificial fingerprint, for example.

2. Replay or manipulation of sensor image data. Replay or manipulation of sensor image data requires the ability to inject a sensor image instead of an image from the sensor. The image could 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. The sensor image is processed, and biometric features are extracted. The attack attempts at disturbing the processing and extraction in such a way that the biometric match accepts features it receives from the extracted image of the user's fingerprint.

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

5. Manipulation, disturbance of biometric match processing. The attack tries to influence the biometric match processing to produce a positive match 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 template in storage. The biometric template, the asset created during user enrollment and used to match the features, is either modified or replaced to allow payments using the user's card.

7. Replay or manipulation of biometric match result. The final match result is modified or replayed to fool the rest of the payment system that the legitimate user was verified for a payment.

3. SECURITY FOR BIOMETRIC PAYMENT CARDS

3.1 Mitigating the threats

3.1.1 PROTECTION AGAINST SPOOFING

Spoofing involves the forgery of faces, voices, fingerprints etc. to try to authenticate fraudulently. Many advanced technologies have been developed to minimize the risk of spoofing. In fingerprint authentication, for example, spoofing risks have been significantly reduced by the introduction of active capacitive sensors. This meant conductive 3D prints would be needed that resembled the texture of a real finger to trick any system – a far trickier task to achieve.

Discriminating between the user's finger and someone else's – or indeed, 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 now make creating a successful spoof require considerable time, money, skill, and care. A sophisticated biometric algorithm paired with a state-of-the-art sensor for payment cards is able to provide better than 1/ 20,000 FAR - far harder to achieve than guessing a PIN which, by comparison, has a rate of 1/10,000. Additional security can also be achieved by use of more than one biometric identifier to authenticate the user.

The opposite of FAR is FRR – False Rejection Rate, which means that the authorized user is misidentified as a non-authorized user. For the user, a false rejection is an inconvenience. The ideal biometric authentication system has minimal FAR and FRR, but 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.

3.1.2 PROTECTION AGAINST INJECTION AND REPLAY OF SENSOR IMAGE DATA

Injection and replay mean replacing the sensor itself with a device that provides an image instead of the sensor. The image provided can be the image of the user's finger captured at an earlier payment, and now replayed to trigger more payments.

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.

The inherent privacy of on-device biometric systems also provides protection against leakage of biometric information needed for a subsequent replay attack. All biometric data is stored and processed on the device in the case of personal authentication, and the biometric template that is created is entirely unique to that device. As such, the same finger would create a different template when enrolled on another consumer device. This means attacks are considerably harder to scale and the ability to attack a secondary system that the user is enrolled on are 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. Privacy is crucial to consumers – especially in the modern age of data protection. The consumer's data stays with them at all times on their device and is kept secure, never leaving the card.

3.1.3 PROTECTION AGAINST MANIPULATION OF BIOMETRIC PROCESSING AND TEMPLATE STORAGE

These types of attacks target the execution of the biometric software. Attacks can consist of fault injection attacks, or inversely measure effects such as variance in time, power consumption or in electromagnetic fields caused by the execution. These are types of side channel leakage that are then used to optimize fraudulent inputs. This process is known as a hill climbing attack.

The robustness of the processor execution and protection mechanisms against fault injections, as well as the protections against leakages, provides the necessary defenses against these types of attacks. Again, high quality biometric algorithms and how the algorithms are implemented also impacts how sensitive the biometric processing is to these attacks.

The perfect combination of hardware and software is key. A high-quality sensor combined with an advanced algorithm finds the sweet spot between security and convenience.

3.2 Meeting the demands of payment cards

The requirements on a security solution to be embedded in payment cards and launched commercially are plentiful and complex:

1. Low cost. The security solution cannot drive cost by requiring more memory, processing power in the sensor host etc.

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

3. Real-time performance. The time from the user holding up a contactless card against the reader until a match operation has completed and the user has been verified in less than a second. Any security solution cannot add latency that disrupts this convenient user experience and the less-than-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.

3.3 Fingerprints' solution

Fingerprints™, the leader in biometrics for contactless smartcards, provides a solution that can be totally integrated into the card itself. This means that all steps in the biometric verification, from sensor image capture to final match, are performed on-card and in real-time. This allows the system to be used with any payment terminal that accepts contactless cards. This also means that all sensitive information is contained in the card and not accumulated in the terminals or in the cloud. For the user, the experience remains just as convenient, only with added security.

Fingerprints FPC SafeTouch® feature is a collection of functions designed to maximize the security. Fingerprints' updated version of this feature is integrated into a selection of its latest sensors to offer a flexible and cost-efficient security solution. It provides two security modes. The MAC mode provides sensor image origin authentication, as well as integrity and replay protection. Additionally, the ISO compliant[4] EtM mode provides sensor image confidentiality.

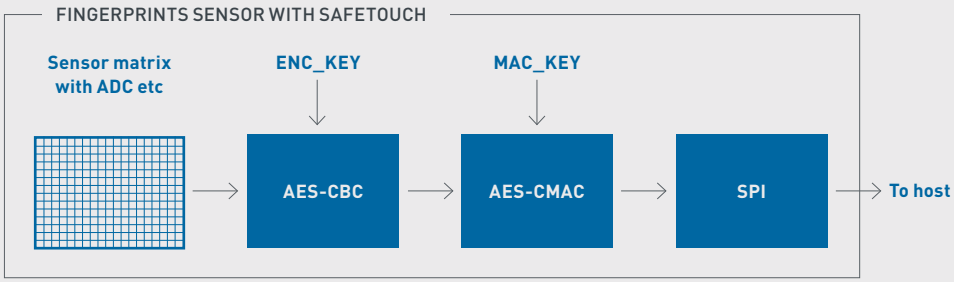

Figure 5. Fingerprints sensor with latest FPC SafeTouch® functionality.

The security solution uses separate keys for encryption (ENC_KEY) and authentication (MAC_KEY). The ENC_KEY can be either 128 or 256 bits. The MAC_KEY is 128 bits.

Sensors with support for the latest FPC SafeTouch work exactly as sensors without earlier SafeTouch functionality, improving the efficiency of testing during card manufacturing and assembly. Only when pre-shared keys have been established, and the desirable security mode has been selected is the security functionality enabled. Once enabled however, the security mode is irreversible and cannot be disabled in any way. The pre-shared keys (PSK) ENC_KEY and MAC_KEY can be established during production, personalization or even during user enrollment, allowing for an ease of production and user experience.

The security solution is based on well-established trusted industry standards[5] and proven technology to ensure that the solution is compatible with existing components in the ecosystem and interoperates seamlessly. Authentication, integrity and replay protection are provided with AES-CMAC[6] in combination with a random challenge from the host when requesting a sensor image. If enabled, AES-CBC[7] provides confidentiality protection of the image data. AES is also used internally as part of the generation of initial vectors (IV) for AES-CBC.

The solution requires the host to use a single crypto primitive, AES[8]. This makes the solution easier to integrate and cost efficient. AES is commonly supported in MCUs (microcontrollers) and SEs, which further cuts the cost and power consumption required to support the solution. The solution can also be performed in streaming mode, further reducing memory requirements and minimizing latency. The Fingerprints' sensor provides image protection without any loss of bitrate performance or lagging.

Replay protection is based on a 128bit random challenge (CR) provided by the host when requesting a new image. The challenge is used to initialize the CMAC tag for the image captured and sent to the host. This allows the host to verify that the image received is not a previous image being replayed but sent as a response to the request to the sensor with which it shares the authentication key.

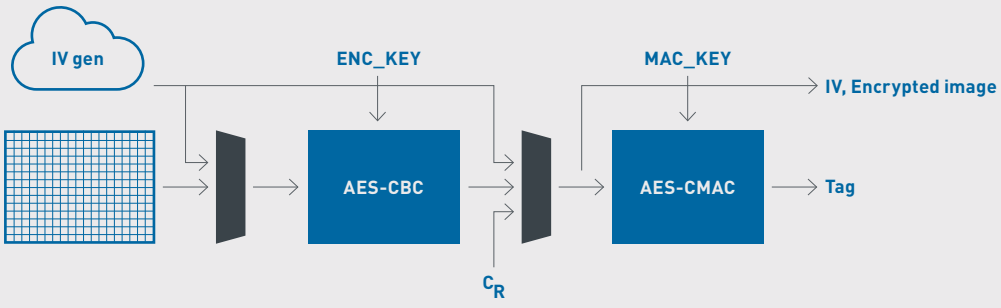

Figure 6. Sensor security processing in detail with IV generation and random challenge supplied by the host.

The sensor data size only marginally expands when security has been enabled. With authentication and replay protection, the data expands by 16 bytes. If confidentiality has also been enabled, the data expands with 32 bytes in total. As such, for a sensor image of 10 kilobytes, the expansion is less than 5%.

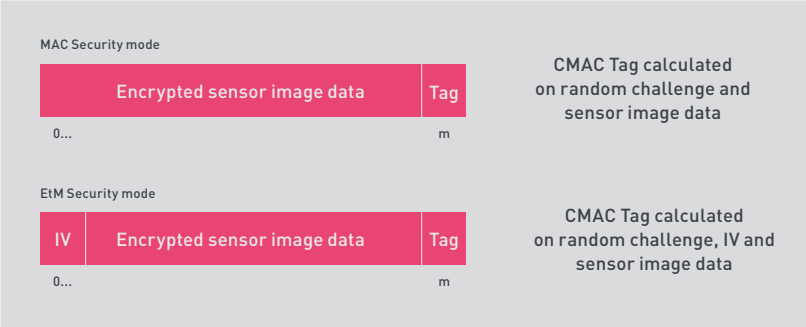

Figure 7. Sensor image data when MAC mode or EtM mode is enabled.

4. CONCLUSION

Adding biometric authentication on-card is the natural evolution of contactless card payments. It offers an answer to fraud fears and security requirements, without impairing the convenience of paying with a 'tap'. By adding strong authentication to contactless, the financial world can also finally eradicate the need for PIN entry by removing contactless payment limits, enabling a consistent, simple and hygienic payment experience.

Compared to PINs and traditional contactless, cards with integrated, fingerprint-based biometric authentication offer a superior solution on multiple fronts. However, biometric solutions rely on the quality of the biometric processing itself, and how assets such as the sensor image and templates are protected. Robust security and privacy protections are fundamental for the launch, and indeed mass adoption, of any new technology relating to sensitive financial data.

Fingerprints' sensor and its image protection features meet these demands. With extensive and considered R&D, we have created a solution that delivers multiple attack mitigation functions that can be layered and implemented throughout the manufacturing and personalization process.

Our solution has been carefully developed to meet stringent technical, market and user requirements. Created in line with existing card standard requirements, the technology can enter the market seamlessly, with simple manufacturing processes and no update required to existing payment infrastructure.

The next generation of contactless cards is ready to roll. To learn more about Fingerprints' biometric payment card offering, *visit our website*.

5. REFERENCES, INDICES, KEYWORDS

References

[1] Fingerprint Cards. ***Biometrics – The missing piece of the payment card puzzle?*** **2018.**
https://www.fingerprints.com/uploads/2018/05/fpc-smartcards-ebook-en.pdf

[2] The Telegraph. ***Dirty banknotes may be spreading the Coronavirus, WHO suggests.*** **2020.**
https://www.telegraph.co.uk/news/2020/03/02/exclusive-dirty-banknotes-may-spreading-coronavirus-world-health

[3] Fingerprint Cards. ***Banking on Biometrics.*** **2019.**
https://www.fingerprints.com/uploads/2019/08/fingerprints-banking-ebook-3.pdf

[4] ISO/IEC 7816-4:2013
https://www.iso.org/standard/54550.html

[5] ISO/IEC. ***Information technology -- Security techniques -- Authenticated encryption.*** **19772:2009**
https://www.iso.org/standard/46345.html

[6] NIST. ***Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication.***
SP 800-38B. 2005.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

[7] NIST. ***Recommendation for Block Cipher Modes of Operation: Methods and Techniques.*** **SP 800-38A. 2001.**
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[8] NIST. ***Advanced Encryption Standard (AES).*** **FIPS-197. 2001.**
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Abbreviations

AES – Advanced Encryption Standard, see [4]
BSoC – Biometric System on Card
CC – Common Criteria
CMAC – Block Cipher Based Message Authentication Code
CVM – Customer Verified Method
EC – Elliptic Curve based PKI
ETM – Encrypt Then MAC
FAR – False Acceptance Rate
FRR – False Rejection Rate
MAC – Message Authentication Code
PKI – Public Key Infrastructure
PSD2 – Payment Service Directive 2
PSK – Pre Shared Key
SCA – Strong Customer Authentication
SCP3 – Secure Channel Protocol
SE – Secure Element
UX – User Experience