The future of payments with wearables and smart devices

Second edition, September 2021

www.infineon.com

Contents

1. Introduction 3

2. What are wearables? 3

2.1 Types of wearables 4

2.2 Functionality 4

2.3 Market growth 5

2.4 Challenges with wearables 6

3. Wearable use cases requiring a Secure Element (SE) 7

3.1 Payment use cases 8

3.2 Transit ticketing 9

3.3 Physical access 9

3.4 Identification & authentication 10

3.5 Automotive use cases (e.g. keyless entry) 10

3.6 Enterprise use cases 11

3.7 Health tracking 11

4. The evolution of wearables 12

4.1 Security, low power consumption & high-performance NFC transactions 13

4.2 Different SE solutions for wearables 15

4.3 Connected wearables 16

4.4 Service enrollment and security 17

4.4.1 Decentralised SE Management (DSEM) 18

4.5 Security measures for connected devices 18

4.5.1 Strong device identity 18

4.5.2 User authentication 18

4.5.3 Strong device authentication 18

4.5.4 Device Integrity 18

4.5.5 Remote Attestation 18

5. The (near) future of payments in wearable devices and connected devices 19

5.1 The need for hardware-based security 19

5.2 SECORA™ Pay and SECORA™ Connect: Everything is potentially a payment device 20

5.3 Uncovering the right use cases 21

5.4 Standardising across the industry 21

5.5 Looking further ahead 22

1. Introduction

Infineon is the global enabler of efficient and secured transactions using smart devices. This whitepaper will explore the different types of wearables beyond simple electronic gadgets and analyse some of the payments-related current and future use cases.

2. What are wearables?

Wearables are a convenient choice for the modern connected consumer allowing for easy access to the preferred functionality. Wearables are basically mobile products or gadgets worn (often continuously) by the user rather than picked up and carried (like phones or tablets). The fact that the device is worn also allows for continuous interaction – directly or indirectly – between the user and the device.

2.1 Types of wearables

While we continue to see many innovative types of wearables brought to market, we will focus on three key types in this paper, as these are types of wearables often enabled for payments.

- Payment Accessories (e.g. Wristbands and rings)
- Smartwatches
- Fitness/health trackers/smart wristband

These categories have all seen successful products broadly adopted in the market. Another type of wearable that deserves mention is "hearables[1]" – typically wireless earpieces like Google's Pixel Buds or Apple's AirPods. To be classified as a hearable, the devices must have additional functionality beyond basic earphones. This line of products has been the fastest-growing wearables category in recent years[2]. While we see interesting use cases for hearables in health monitoring, voice assistance and others, we have yet to see support for payments, which is why we have omitted this type of wearable from this paper.

2.2 Functionality

Single-use wearables still dominate the wearables market and this trend seems to continue as the barriers to entry for this range of products continues to diminish. In parallel, we see wearables like smartwatches developing into platforms in their own right – albeit often as a companion to the increasingly feature-rich smartphones.

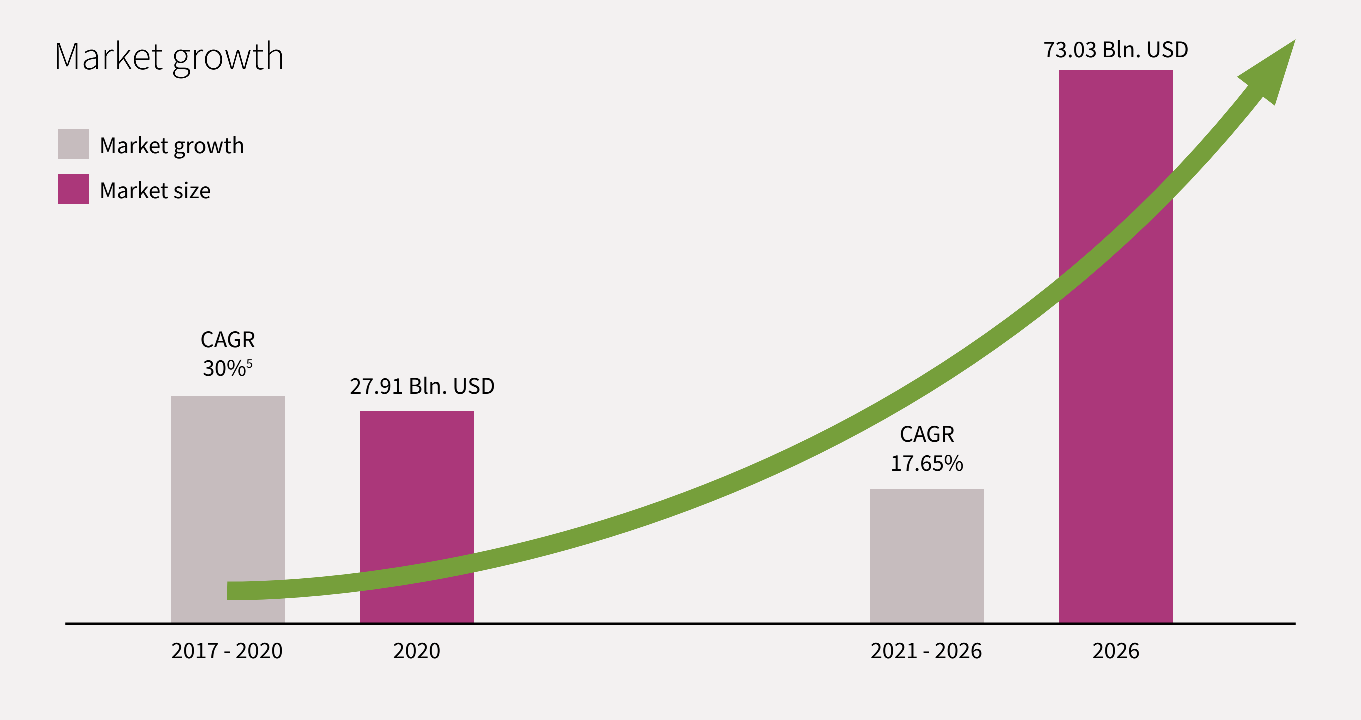
There can be functional overlap between the categories in this white paper, which is only natural as the very core of smart wearables is their diverse functionality, thanks to the sophisticated integrated circuits embedded into the products. As seen with smartwatches, in particular, the ability to deploy apps directly to a wearable allows for individual mix-and-match solutions rather than one-size-fits-all.

It is also important to highlight that the development of functionality in wearables, especially with regard to payment, has meant that smart devices increasingly generate and store personal data directly on the devices. Consequently, the requirements for proper data management and security as well as for device integrity have increased – more on this in the Security chapter of this white paper.

[1] https://www.forbes.com/sites/frankfitzpatrick/2021/01/01/5-key-hearables-trends-for-2021/
[2] https://www.idc.com/getdoc.jsp?containerId=prUS47534521

2.3 Market growth

Wearables have become an integral part of consumer electronics. According to IDC, the number of devices shipped from across the different producers has increased from 125 million units in 2017[3] to 444 million units in 2020[4] – almost double the volume that the 2017 study predicted for 2021.



The use of smart devices for payments at point of sale have further boosted the global surge in contactless payments and the consumer demand for completely "contact-free" payments driven by COVID-19. Mastercard alone saw an increase of contactless transactions of more than one billion during the first quarter of 2021 compared to the same period of 2020[7] At the same time, the transition to contactless payments have significantly reduced the fraud rates which again have further strengthened the consumers' trust in the technology and hence their willingness to actively use it. A study by Visa and PYMNTS.com showed that "70 percent of consumers consistently feel their devices improve their quality of life. Contributing to that convenience is payment technology"[8].

[3] https://www.idc.com/getdoc.jsp?containerId=prUS42818517
[4] https://www.idc.com/getdoc.jsp?containerId=prUS47534521
[5] https://www2.deloitte.com/be/en/pages/technology-media-and-telecommunications/topics/mobile-consumer-survey-2019/wearables.html
[6] https://www.mordorintelligence.com/industry-reports/wearable-technology-market
[7] https://www.mastercard.com/news/press/2021/april/mastercard-new-payments-index-consumer-appetite-for-digital-payments-takes-off/
[8] https://www.visa.co.uk/content/VISA/usa/englishlanguagemaster/en_US/home/visa-everywhere/innovation/wearable-payment-technology.html

2.4 Challenges with wearables

As wearable devices and the supporting ecosystem are maturing, the core challenges are gradually being mitigated. These challenges are related to the fact that most wearables are small compared to smartphones and the interfaces are much simpler (or non-existent). Currently, the top-3 challenges when it comes to wearables are:

- Limited battery life
- Integration options and contactless performance
- Often complicated service enrolment

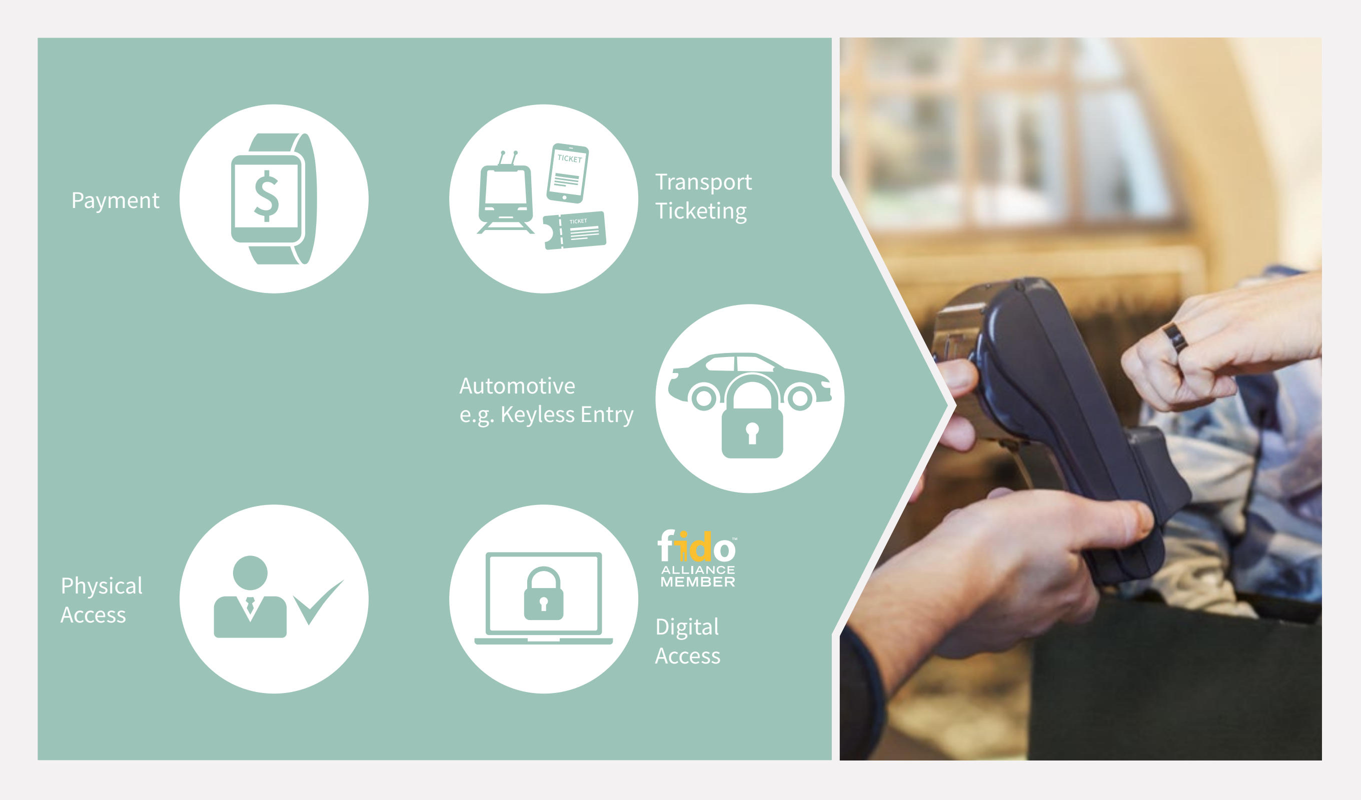
Alongside these practical challenges, many devices also struggle with accuracy and stability and, even more importantly, with data security and device integrity, which becomes increasingly important as the sensitivity of the data generated, or the value of the transactions initiated, increases. We will return to security issues and possible mitigation options later in this paper.

3. Wearable use cases requiring a Secure Element (SE)

Telling the time, checking the time or your calendar, counting your paces, measuring your heart rate, etc. Most of the functionality described so far has been what might be called personal use cases, where the interaction only takes place between the user of the wearable and the device itself. There might also be integration from a fitness tracker to a smartphone for a richer user interface, but that still falls into the category of personal use cases.

In this chapter, we will focus on security-related use cases, where the wearable connects to points of interaction with a higher security relevance outside the control of the user, based on additional security countermeasures, which are built into the device itself.

The security-relevant use cases are rarely stand-alone, and some of the best and most successful wearable solutions combine these use cases.



3.1 Payment use cases

Payment has always been a central use case for any smart device manufacturer. The main reason for this is that payments tick a lot of the boxes as payments are:

1. (to a great extent) already digitised
2. something that we all do
3. something that is done frequently
4. ‘personal’

That said, digital payment is also a challenging use case to tackle, as it is already extremely well-served in most countries where card payments are dominant.

Any payment solution ever brought to the market has been dependent on the acceptance infrastructure of the solution. Standardisation around EMV and NFC (“Near Field Communication”) for contactless payments has helped pave the way toward a richer choice of payment solutions. More contactless payment solutions have been made possible thanks to the introduction of tokenisation, which has made the distribution of payment credentials more flexible. As smartphones with biometric sensors have become increasingly common, biometric authentication (using fingerprint or face recognition) for mobile contactless payments is currently a de facto standard, as users perceive biometric authentication as convenient.

Alongside mobile payments (from smartphones), we are now seeing an increasing proliferation of payment solutions in the shape of rings, wristbands, key fobs, clothing or even chips surgically implanted as marketed by the British/Polish company Walletmor[9].

Payment habits can be hard to change, and different markets have seen different pace in the uptake of contactless up until COVID-19, that accelerated the preference for contactless and even fully contact-free (where the payers only touch their own device rather than the POS terminal of the shops).

While payments via smartphones or wearables have seen a major boost during COVID-19, cards are likely to continue to play a central role in digital payments at the point of sale for the years to come. By April 2023, payment networks in most regions will require full contactless migration of POS infrastructure, enabling more and more contactless payments to adopt alternative form factors and increase contactless payment transactions by new devices. This development will further accelerate the virtual issuance of payment cards directly to smart devices and wearables.

Avoiding getting your wallet out is an improvement in terms of convenience, but there are also distinct cases where a wearable device makes for a better and more seamless payment process. These cases include paying for transit tickets while getting on a bus or into a metro where speed is of the essence (see more about this use case below) or going to the beach where a (waterproof) payment ring, wristband, or similar could save you from worrying about theft from your beach bag while you are out swimming. Similar solutions have already proven effective at scale for music festivals and sports events where they improve payment speed and reduce efforts for circulated cash.

[9] https://walletmor.com/

3.2 Transit ticketing

Next to retail payments, ticketing for public transportation is one of the most frequent digital use cases driving transactions at points of interaction. Inspired by payment systems, cards have so far been the predominant form factor for digital transit ticketing systems (originally employing magnetic stripes, cards have evolved to chip technology). However, as speed is of the essence when hundreds of people need to get through the gates in a steady flow, getting a card out of a wallet can cause delays. Embedding the transit ticketing solution into a wearable device can increase convenience significantly for commuters. As more and more transit operators globally embrace the EMV-based ticketing model pioneered by Transport for London, the number of places you can use your payment-enabled wearables for transit ticketing has significantly increased. We also start to see transit operators experiment with even more sophisticated – and completely contact-free – solutions, the so-called BiBo solutions (“Be-In Be-Out”), where the initiation and termination of the ride and the collection of the phare are fully automated based on precise location-aware smart devices like a smartphone or a wearable device in combination with sensors on board of the trains and busses etc. supporting these solutions.

3.3 Physical access

Key cards are widely used across corporate offices, factory buildings, other facilities, sports facilities, gyms etc., across the world. Private homes also increasingly get “smart locks” installed. Traditional key cards can easily be integrated into simple wearables, while connected wearables allow for a more sophisticated distribution of access control, such as one-time keys for logistics companies delivering goods directly to your home as we see with Key by Amazon, which also works for Volvo cars[10] or with the Alexa and Google Home enabled smart locks from Yale[11]. For corporate use, there is still the challenge that many companies combine identity and access cards with a security policy stipulating that the ID cards have to be worn visibly.

[10] https://www.volvocars.com/us/own/additional-choices/in-car-delivery
[11] https://www.yalehome.com/en/solutions/yale-access/

3.4 Identification & authentication

The general need and demand for two-factor authentication continue to increase. This has been driven both by consumer demand for stronger protection as well as by regulatory requirements like the Revised Payment Services Directive – PSD2 – from the European Union, which clearly mandates the use of "Strong Customer Authentication", i.e. at least two-factor authentication. In the context of PSD2, the three categories of factors are:

1. Knowledge – something you know, e.g. a PIN code, passphrase or pattern.
2. Possession – something you have, e.g. a physical device like a card or a phone
3. Inherence – something you are, e.g. your fingerprint or other biometric authentication.

When it comes to supporting authentication, wearables can play a central role as they can support both possession and inherence. A wearable device can also potentially also support entry of a passcode to support the verification of the 'Knowledge' aspect.

Validation of possession will come in the shape of device authentication via an embedded Secure Element integrated into the wearable, while 'Inherence' can be supported in a number of ways through wearables which can track and measure a number of biometric traits that can be used to authenticate the user. This can be face recognition, iris or fingerprint scanning or alternative biometric signatures. Recently the Italian company Deed has announced their screenless Get™ wristband that allows for advanced communication (using bone conduction technology) as well as contactless payments and innovative biometrics[12].

As requirements for stronger authentication increase, usability and convenience are often challenged. The FIDO Alliance[13] is an open industry association that works toward global standards for authentication to mitigate the current problems caused by the widespread use of passwords. In a not so distant password-less future, carrying your ID credentials on a mobile or wearable device that can connect directly to the PC or POS you need to authenticate towards can increase both security and convenience.

3.5 Automotive use cases (e.g. keyless entry)

Remote keyless systems have for long been the de-facto standard for unlocking cars, but has so far been dominated by stand-alone "smart keys" or key fobs. With the advancements in technology to support distributed key credentials on other smart devices, we are now seeing manufacturers exploring more innovative and convenient solutions. To make these digital key solutions truly ubiquitous, the global industry forum - The Car Connectivity Consortium® (CCC)[14] is working to develop standards for digital keys and data exchange that allow for interoperability, security and data privacy.

One example of a digital key implementation is from CCC-member Hyundai, which has introduced Hyundai Blue Link[15], a car app that accesses features through a smartwatch and provides connected care, like automatic collision notification, SOS emergency assistance, and email alerts on driving performance, while also allowing for remote access and vehicle tracking.

At the same time, we also see many automotive manufacturers expanding their service portfolio within financial services. Financing has been an integral part of the business model for many years, but we also see more and more manufacturers utilising the financial licenses they have acquired to also expand their financial services beyond financing and into payments to further increase customer engagement while at the same time opening for new revenue streams.

[12] https://www.infineon.com/cms/en/about-infineon/press/market-news/2021/INFCSS202106-083.html
[13] https://fidoalliance.org/
[14] https://carconnectivity.org/
[15] https://www.hyundai.com/eu/about-hyundai/our-cars/bluelink-connectivity.html

3.6 Enterprise use cases

Most of the previous use cases have focused on the individual and personal use of wearables. Enterprise, corporate or industrial use of wearable technology is also under development across a great number of suppliers. An important use case for enterprises, companies and university campuses are wearables that work to replace badges to regulate physical and digital access to certain areas, often in combination with digital access to workstations or with payment use cases in canteens and campus shops.

The continuous location monitoring enabled by wearables can be used at large workplaces like hospitals, airports, factories etc to reduce the time staff spend on finding each other during the day and, even more importantly, reduce the response time in emergency situations which can occur at all three types of places mentioned above and where timing is crucial. We also see wearables applied with great success to "pickers" at warehouses who can use smart glasses to guide them more efficiently when packing orders.

Enterprise wearables are also used for health purposes. There are solutions in the market that protect wearers against injuries from strain. As seen during COVID-19, location-aware wearables have helped to keep proper social distancing at workplaces.

While there are obvious benefits of these enterprise use cases, tracking and monitoring employees do raise an important debate about how the solutions and data are being used.

3.7 Health tracking

Wearables have many great use cases within fitness tracking and health monitoring. While fitness trackers are the wearable that first comes to mind for most people, the ability to combine continuous tracking and measurement allows for much richer data generation and subsequent analysis than previously available. This development has also been further catalysed by COVID-19 as we have seen a boom in the use of telemedicine and remote monitoring of vital signs due to restrictions on physical access to doctors and hospitals.

Thanks to the advancement in sensor technology, we have seen fitness trackers capable of monitoring and measuring across an increasing number of data points, including (but not limited to):

- Location & movement
  - Steps
  - Location via GPS, BLE or UWB
  - Elevation
  - Speed/acceleration
- Health
  - Stress levels via Galvanic Skin Response (GSR)
  - Heart rate / pulse
  - Temperature
  - Sleep patterns
  - Blood pressure
  - Blood sugar levels
- Other
  - Gestures
  - Light (in some cases also UV for health purposes)

But health is much more than fitness and activity tracking. Wearable devices can also serve users in many other ways. Since the first digital hearing aid was introduced in 1987 by Nicolet Corp., development has been exceptional, and today we see digital hearing aids incorporated in everything from glasses to necklaces.

While the heart rate monitor in fitness trackers might be accurate enough for most people, people with heart conditions have so far been reliant on medical-grade equipment for full ECG monitoring. Today, companies like Qardio[16] have developed wearable solutions that serve this segment.

Wearables can also serve as potential life-savers or improve the quality of life for people living with a chronic disease as seen with the Empatica's Embrace[17] wristband that tracks and alerts epilepsy patients (and their carers) to potential convulsive seizures. This and other examples clearly show that wearables are much more than just "gadgets".

[16] https://www.getqardio.com/qardiocore-wearable-ecg-ekg-monitor-iphone/

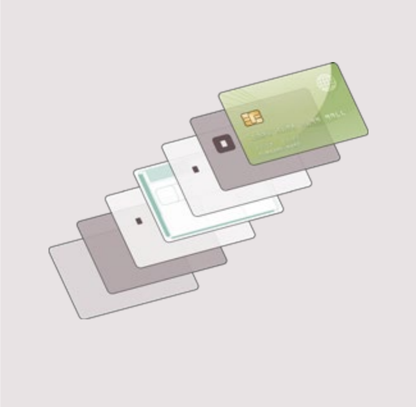
[17] https://www.empatica.com/

4. The evolution of wearables

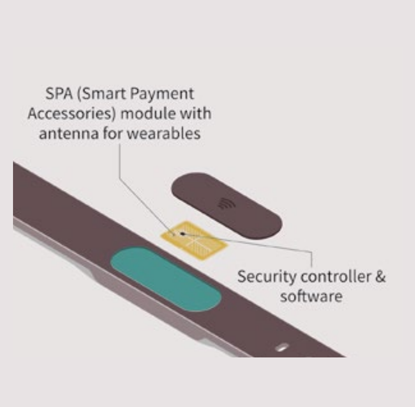
As most wearables are smaller than smartphones, the deployment of Secure Elements and other integrated circuits (IC) has required continuous improvement and innovation from manufacturers. This, in turn, has led to the development not only of increasingly small chipsets but also of different types of hardware allowing for different uses as well as different security measures.

The evolution of Secure Elements for wearables can be divided into three developmental stages.

1. First came the EMVCo-approved security controller, which is integrated into a dual interface payment card. This version is based on a non-connected contactless interface (ISO14443) and has a large antenna implemented to operate.
2. Next came the design of advanced small-format contactless security controllers and non-connected payment accessories powered by small antennas – i.e. without batteries.
3. Concluding the preliminary evolution are connected wearables with components consisting of a connected contactless IC system mostly based on a boosted NFC SE, which is connected to a host processor for internet connectivity. Due to the very small architecture of these connected wearables, a micro-antenna will be integrated, and the NFC system will be connected to a small battery for optimum contactless performance.



Dual-interface security controller (passive, contactless acc. to ISO 14443)


SPA (Smart Payment Accessories) module with antenna for wearables
Security controller & software

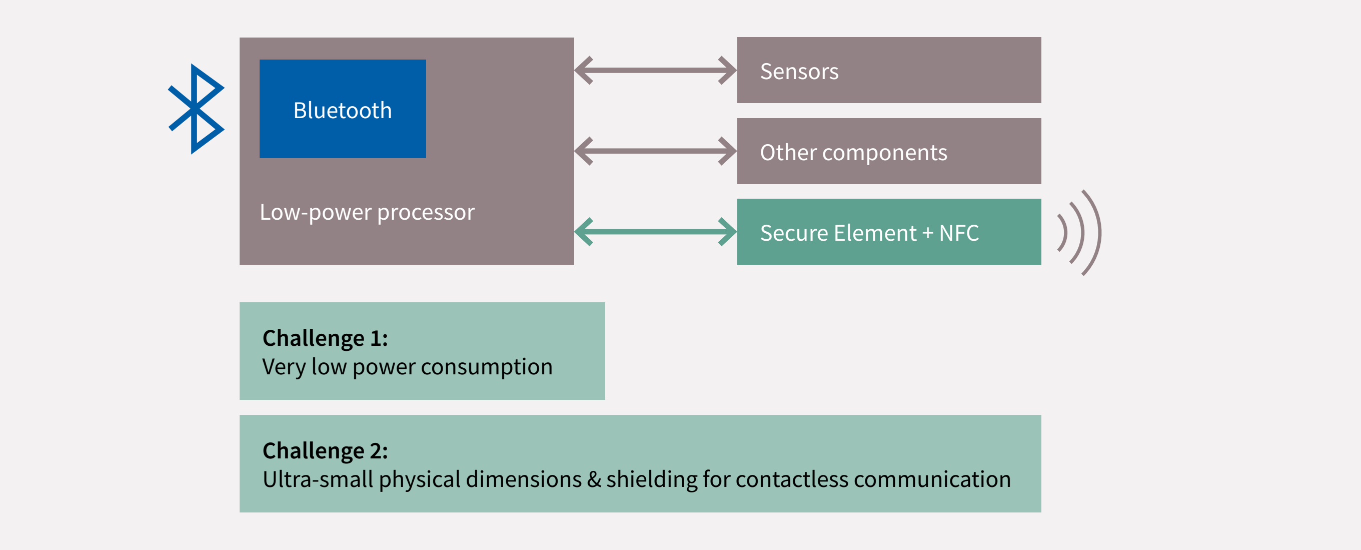
Advanced contactless security controller (small antenna acc. to ISO 14443)

Security controller & software
NFC Booster

Active contactless with battery driven micro-antenna and Internet connectivity

4.1 Security, low power consumption & high-performance NFC transactions

To enable high-performance NFC solutions for SE systems, an IC supplier has to overcome some critical technical challenges. Wearable systems are usually constructed in minimal physical dimensions, while end-users expect a long battery life.



Consider the energy density of battery technology today – restriction of power capacity to reduce the component power consumption is the only choice. The standby power consumption of the security NFC system must be as low as possible. On the other hand, the support of all NFC applications in terms of security and tamper resistance is mandatory in order to obtain all necessary security approvals. At the same time, the functional operations have to fulfil specific requirements in terms of contactless performance and power consumption with either a battery-less or very low power active NFC model. Infineon specifically selected the architecture of IC sets either as field-powered (passive) NFC modes or compatible solutions in active NFC transmission mode with the lowest power consumption. One example is ultra-small SECORA Connect S for field-powered NFC (2x2mm). Besides that, the SECORA Connect X boosted Multi-Chip-Package (4x4mm or upcoming 3x3mm), allowing customisation of the external antenna towards device requirements (e.g. metal environment) for best power consumption and contactless performance. These solutions consume significantly less of the power required for any conventional modem solution as low power consumption is a key requisite for payment wearables.

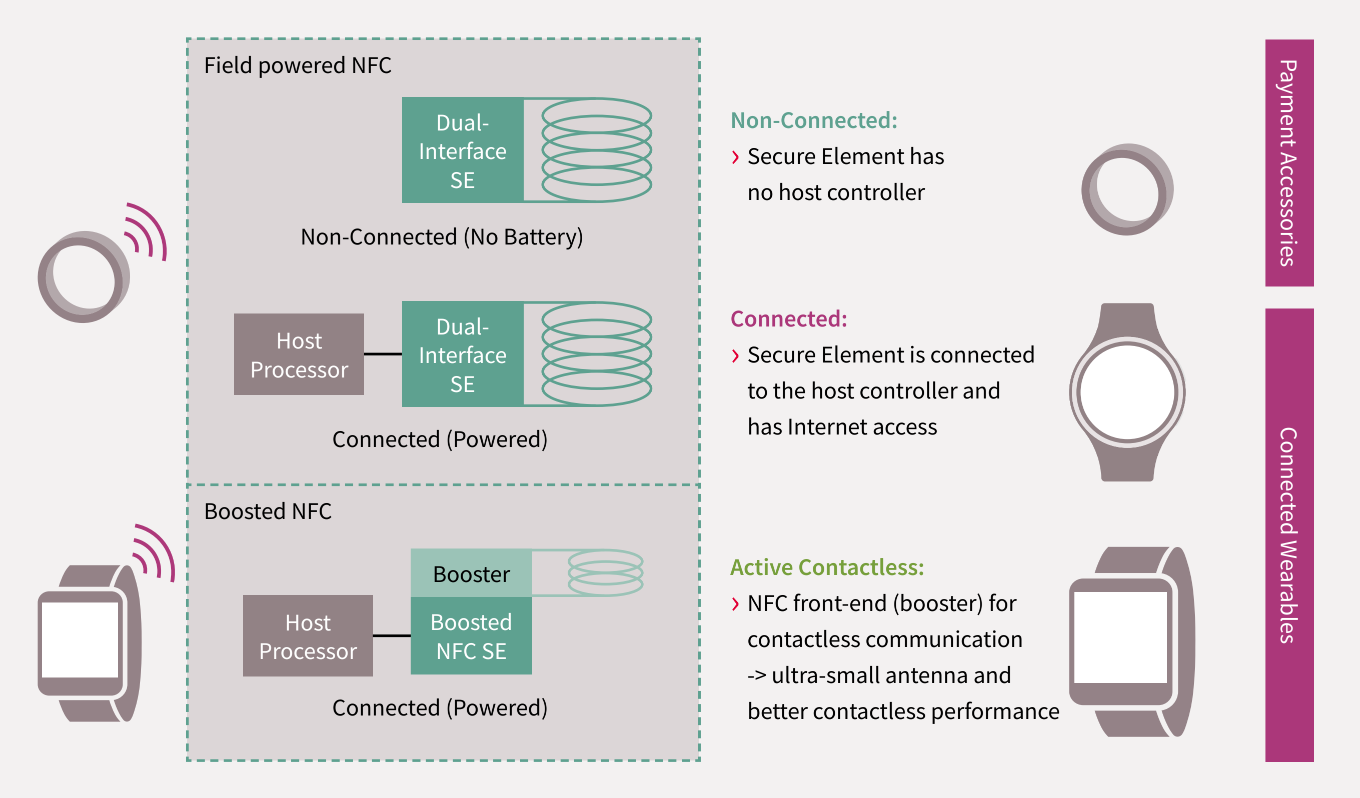
› Ultra-small
› Very low power
› Fast system integration

4.2 Different SE solutions for wearables

Non-connected wearables are usually pre-programmed to specific functionalities and use cases. These allow for relatively efficient mass distribution – e.g. for use at events or other confined environments. At events like music festivals, the mass-distributed non-connected wearables – often in the shape of wristbands – can serve both access and payment use cases. They eliminate the need to carry cash and reduce queuing for both access and purchasing of food and beverages, which again improves the overall experience for the users.

These non-connected wearables – also called accessories – can also be designed for open-loop use – e.g. for payments outside the event venue (such as the possibility to pay at merchants showing the acceptance marks of the respective payment scheme such as Visa or Mastercard) – which further supports the branding value, e.g. a particular stadium or festival.

The combination of dedicated hardware, controlled issuance and standardised or dedicated communication interfaces (e.g. to contactless readers) allow for a highly secure setup. As these non-connected devices do not come with a full smart device's rich interface or features, additional security can be applied at the point of sale, e.g. where a higher transaction amount would require pin entry at the POS.


Field powered NFC
Dual-Interface SE
Non-Connected (No Battery)
Host Processor
Dual-Interface SE
Connected (Powered)
Boosted NFC
Booster
Host Processor
Boosted NFC SE
Connected (Powered)
Non-Connected:
› Secure Element has no host controller
Connected:
› Secure Element is connected to the host controller and has Internet access
Active Contactless:
› NFC front-end (booster) for contactless communication -> ultra-small antenna and better contactless performance
Payment Accessories
Connected Wearables

4.3 Connected wearables

Connected wearables, such as smartwatches, are more complex and allow for broader use cases and thus for the ability to play a bigger role in daily life, as these devices can be re-programmed in the field and equipped with different applications. This multi-application approach also allows for continuous development and deployment of apps or app-like services to the devices.

These more flexible platforms, introduced with connected wearables like smartphones, do, however, introduce some security concerns as neither the hardware manufacturer nor the issuers of, for example, payment solutions to the product will have full control of what else the users decide to install on their devices. This means that the requirement of the underlying security hardware will increase accordingly, and tamper-resistant secure elements will be even more relevant for security in these solutions. Software-based security can and should also be applied to solutions on connected wearables, but since continuous software updates can prove even more challenging than for smartphones, top-notch hardware security is paramount, especially for payment wearables.

The connectivity of these so-called 'active devices' does also enable different features like remote provisioning of security credentials and remote management of the secure element inside the device. Furthermore, consumer device 'cardholder' verification is enabled more convenient payments at high security (no need to enter the PIN on the POS terminal).

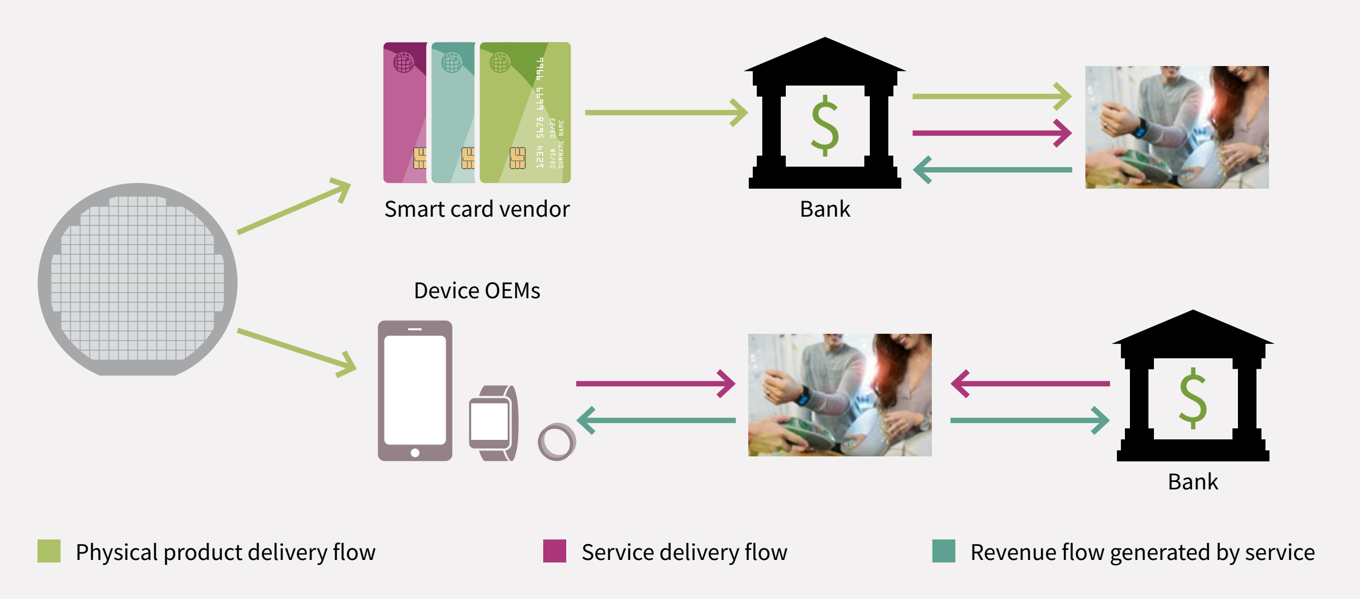
4.4 Service enrollment and security

If we look at the distribution of electronic payment credentials in the traditional card issuance flow, security hardware is the service carrier of Identification, Authentication, and Transactions. This applies to ID cards, access cards, and payment cards and is typically managed by smart card vendors. These, in addition, manage the physical production of the card – including the personalisation (i.e. the embedding of the card number into the chip) – on behalf of the issuing bank.

The bank manages the interaction as well as the entire commercial relationship with the consumer. This flow is indeed a sophisticated process but also a clearly defined 'linear' value chain that has been optimised and fine-tuned over decades. This process can be easily replicated for simpler and often single-purpose wearables and is often used for payment accessories.

For more sophisticated smart devices, the flow is radically different. The chip manufacturers still deliver security hardware to the "device makers" similar to the card vendors, but in most cases, the device makers sell their products directly to the consumer. The consumer is no longer just "cardholders" – i.e. the user but not owner of a bank-issued product – but rather "device owners" who are in much greater control over the services that they want to enable on their smart device.

This development calls for a new type of commercial dynamics which again results in a more fragmented (non-linear) value chain.


Smart card vendor
Bank
Device OEMs
Bank
Physical product delivery flow
Service delivery flow
Revenue flow generated by service

As banks are still responsible for the payment instruments they issue, they must protect (as they have done when issuing cards) the consumer's identity through the KYC (Know Your Customer) process. With connected wearables and other smart devices, they also need to focus on device identity.

In payment card issuance, management of the secure element – i.e. the chip on the payment cards – has been managed centrally in the personalisation bureau of the smart card vendors. The same process also applies typically to non-connected wearables, which makes it easy to replicate. In the future, we will also see non-connected wearables to be provisioned contactless via NFC smartphones enabling better consumer experience, new business and distribution models and will enable this market to scale.

To support secured management of connected wearables, the provisioning of the credentials (e.g. ID or payment tokens) often happens via the consumer's smartphone, which again is connected to the consumer's wearable devices via BLE. To securely manage such a process, a number of security measures could and should be implemented.

4.4.1 Decentralised SE Management (DSEM)

In order to establish a secure service in a Secure Element of an end-device (e.g. mobile, wearable, IoT device), a service provider must typically use the SE Issuer Trusted Service Management (SEI-TSM) system to deploy the application on a specific SE. This requires a direct commercial contract between the Service Provider and the SE Issuer as well as direct technical integration of the Service Provider systems into the SE Issuer systems. In these cases, DSEM will simplify or enable wearable deployment. Moreover, token service provider platforms like Mastercard's MDES and Visa's VTS will be integrated into the DSEM flow by mapping tokens with the initial PAN of the user and forwarding tokens to the issuers for authorisation. Considering the fact that Secure Elements in the field have been issued by many different Issuers, a Service Provider has to establish commercial contracts with several entities and integrate to their systems at the same time in order to perform a wide deployment of the service in the field. Because of this, many Service Providers have not yet been able to reach a decent coverage of service deployment. However, initiatives are afoot to standardise the access and API interfaces towards secure elements like Google's Android Ready SE Alliance[18].

4.5 Security measures for connected devices

Wearables, as well as other connected smart devices, all face a number of security threats. Below, we list some of the overarching countermeasures that can and should be applied by suppliers and service providers.

4.5.1. Strong device identity

The identity of the devices is not only a question of security but is also a prerequisite for delivering personalised secured payment services.

4.5.2. User authentication

Once the identity of the device has been established, it is equally important that the service providers check that the intent and consent of the user is properly authenticated both during the initial setup of personal credentials and during the subsequent initiation of transactions.

4.5.3. Strong device authentication

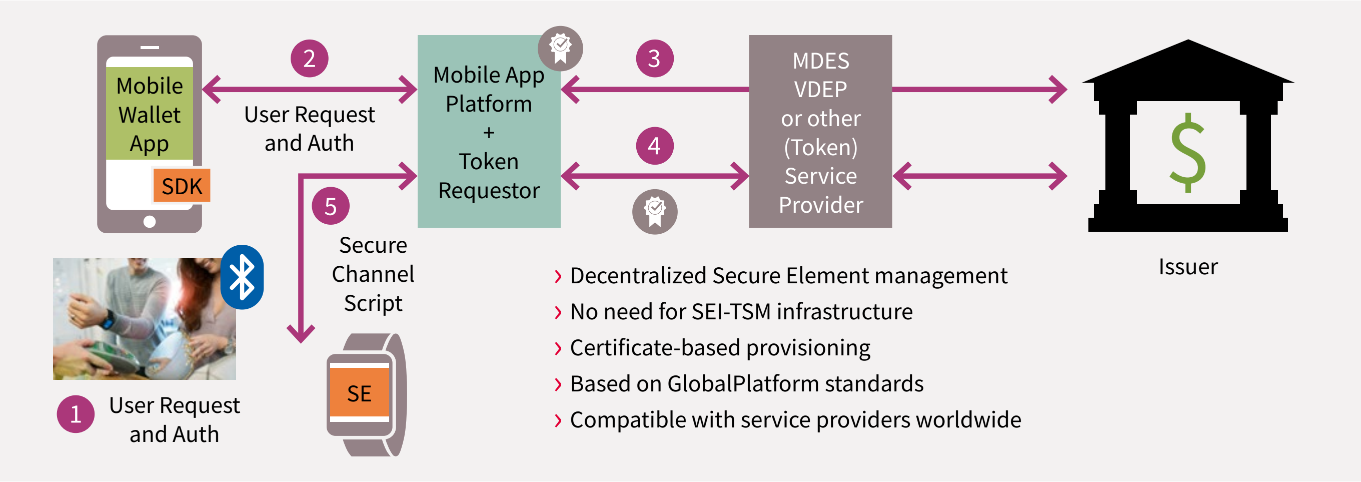
When connected devices request the initiation of a payment or the exchange of sensitive information, it is vital that the service provider fulfilling this request obtains certainty that the device is indeed the device of an identified user. Hardware-based security allows checking that a device is authentic.

4.5.4. Device Integrity

As well as establishing the identity and authenticity of a device, security can be further enhanced by applying device integrity, where dedicated hardware can detect and report attempts of tampering that could potentially compromise the device.

4.5.5. Remote Attestation

Similar to the device integrity verification, remote attestation allows for certainty that the device including the software is running in a specified configuration or state. This can, for example, be the establishment of "Secure Enclaves".



- Decentralized Secure Element management
- No need for SEI-TSM infrastructure
- Certificate-based provisioning
- Based on GlobalPlatform standards
- Compatible with service providers worldwide

[18] https://security.googleblog.com/2021/03/announcing-android-ready-se-alliance.html

5. The (near) future of payments in wearable devices and connected devices

Multi-function connected wearable devices have now had their mainstream breakthrough in terms of the number of units shipped. However, the more complex integrations and interactions are yet to unfold fully. This development will be fuelled by the advancements of IoT – which according to some analysts, will reach around 31 billion interconnected devices by 2025[19]. The more things being integrated, the bigger the need for standardisation to enable the integration. At the same time, the security requirements will grow, and Infineon expects that the most connected devices will continue to use hardware-based hardware security.

5.1 The need for hardware-based security

All transaction-based services will rely on consumer trust, and as such, the payment industry will have to actively address the security challenges and concerns. This became evident in January 2018, when news broke that the GPS tracking company Strava had created a Global Heat Map, using satellite information to map the movement of subscribers to the company's fitness service over a two-year period. By doing so, the company had inadvertently revealed the location of sensitive American military locations[20]. Examples like this help to bring close attention to the way wearable devices are causing users to produce a trail of digital footprints that echo real-life activities. Security concerns are further reinforced by the fact that most wearable devices are more prone to security issues than connected devices like mobile phones because online access allows for easier and more frequent distribution of security updates.

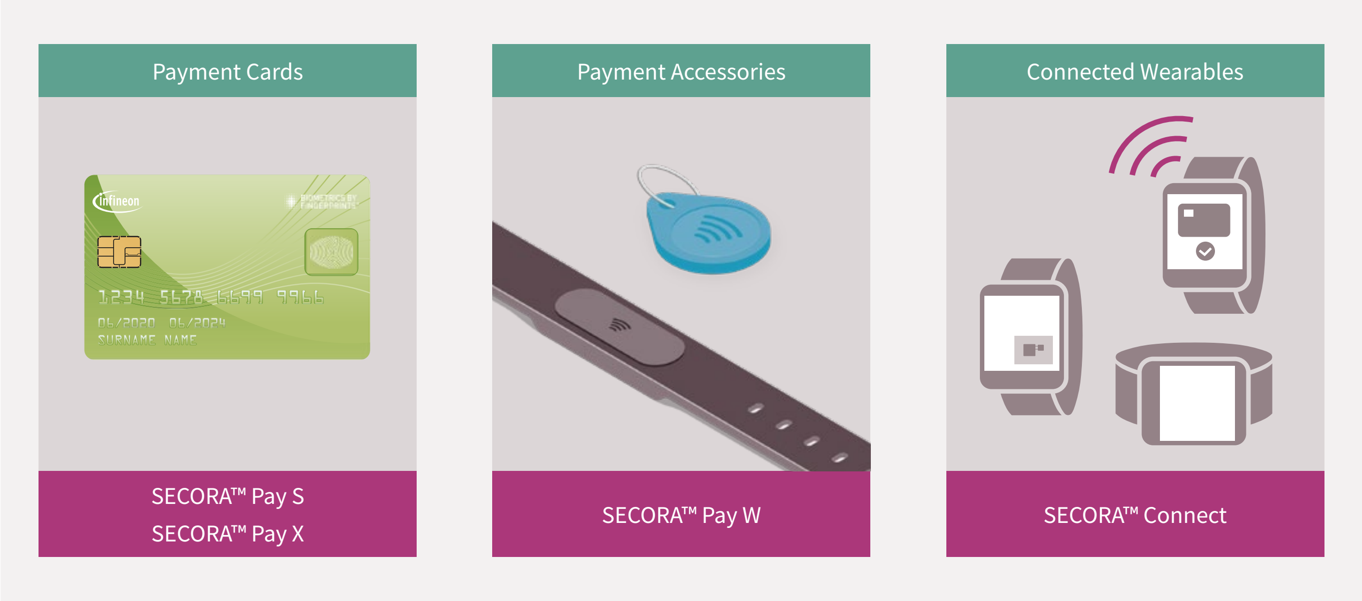
Less grave but much more widespread is the fraud related to online payments. As e-commerce continues to grow in volume across the globe - a trend that has been further catalysed by COVID-19 - so do the fraud attempts targeting both merchants and consumers. Mitigating risk by raising security levels will be ongoing development, and to this purpose, hardware-based security measures will continue to play an important role.

[19] https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

[20] https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html

5.2 SECORA™ Pay and SECORA™ Connect: Everything is potentially a payment device

One way to address the security issues is to employ hardware-based security via a lightweight SE as provided by Infineon’s Java Card based payment solution portfolio SECORATM Pay. This innovative suite of payment solutions (serialised S, X, and W) provides state-of-the-art contact and dual-interface EMV security controllers with the latest EMV applets, allowing all cards, accessories, form factors, and non-connected wearable devices to transform themselves into payment instruments whilst providing the flexibility needed to meet regional market requirements. SECORA™ Pay W solution portfolio includes not only the EMV chip card OS and payment applets but also offers innovative packaging options to address the market need to realise non-connected, field-powered wearable devices, or so-called “Payment Accessories”.



Payment Cards

Payment Accessories

Connected Wearables

SECORA™ Pay S
SECORA™ Pay X

SECORA™ Pay W

SECORA™ Connect

In addition to the employment of hardware-based security, challenging circumstances like those mentioned above emphasise the need for security measures such as increased regulation, tokenisation, encryption of data, remote erase features and highly robust multi-factor security mechanisms related to identification, authentication and authorisation – all to protect the safety of the underlying user credentials. These circumstances also encourage companies and organisations to take a data-centric approach to security, looking at the way this information has been transmitted to a company or organisation from a device and how it is subsequently managed and controlled.

Pre-approved EMV solutions from integrated circuit manufacturers have been required in order to shorten certification and qualification processes and enable device manufacturers to develop power-efficient wearable solutions with the highest possible contactless performance.

Infineon teams up with relevant market players to address the service enrolment challenges, to foster the availability of respective complementary tokenisation services for wearable OEMs.

5.3 Uncovering the right use cases

The prioritisation of the different security aspects related to wearable devices depends in many ways on what the user experience the wearables manufacturers want to deliver to their customers. This can influence the decision on whether they want to deploy standalone or companion devices. Consequently, Infineon focuses on helping manufacturers create the right platform to leverage their interface and uncover the use cases that complement each product. However, as more and more services are provisioned to operate through wearable devices, the lines between the different services begin to blur. With a single application, it is much easier to pinpoint the different aspects of the application that requires a distinct security level, but by mixing a number of application services, you create a security system with issues that are increasingly complex to handle. In response to growing consumer concerns and expectations, manufacturers are required to ensure proper device security, or they will face backlashes from consumers and authorities – regardless of how innovative a product they bring to market.

5.4 Standardising across the industry

As more and more wearable-related applications and services emerge, it is becoming increasingly clear how standardisation (and regulation) will be key to protecting the functionality, interoperability and security in connected wearable devices. Only by adhering to global standards will the entire industry invested in wearable devices be able to cooperate as seamlessly and beneficially as envisaged by all interested parties. To further advance the development and integration of contactless payments in wearables, Mastercard, Visa, Discover, and American Express are jointly pushing for a more consistent and regulated market. The global payment schemes are all linked with security protocols, and they are working on connecting more and more issuers, processors, acquirers, OEMs and application developers through unified tokenisation platforms.
At the same time, they are partnering with companies across multiple categories to enable simple and secured transactions to fit a consumer lifestyle of payments “on the go”. These interoperable standards and partnerships will surely help to accelerate the process of creating an appropriate payment infrastructure to support contactless payments, but not without presenting a few hurdles along the way. In addition to the ability to differentiate between open and closed-loop payment systems, an appropriate payment infrastructure will need to include ubiquitous EMV POS terminals capable of supporting a variety of payment solutions.

It should also be noted that the strong customer authentication (SCA) requirements, which have been applied to a wide range of payment methods with the introduction of PSD2 in the EU, increases dependency on stronger and better authentication for most types of transactions as mandated by the EBA. Wearable devices with biometric sensors in combination with hardware-based security will be a meaningful tool to support strong customer authentication requirements in a convenient way.

5.5 Looking further ahead

With the accelerated consumer adoption and use of payment wearables and IoT devices, the demand for more seamlessly integrated and personalised devices with embedded multi-usage services will continue to increase in the coming years. The key to successful deployment will be to make it as simple as possible for consumers to add additional services to devices. Even if some high-end wearables feature standalone cellular network access, we expect large-display smart personal devices like smartphones to continue to function as the preferred intermediator when managing wearable devices. We also expect non-connected wearables like bracelets and smart rings to gain increased traction as contactless solutions replace cash payments, as well as serving access and identification use cases.

While securing digital payments, wearables – and connected wearables in particular – represent a unique opportunity for banks and financial service providers to interact and engage with consumers in new ways. Wearables will become a top digital payment choice for many by offering a quick and convenient way of paying for products and services[21]. In the longer term, we can expect to some extent that wearable devices will take over from smartphones as facilitators of peer-to-peer payments and catalysts of the sharing economy. However, as with every other digital service that generates and aggregates data from the daily life of individuals, it is paramount to have robust security measures in place to avoid compromising privacy along the way. Finally, the trend towards completely invisible payments like the experience offered at Amazon's Go stores[22] also proves a great use case for wearables as they can relatively easily support location-based payments using UWB and BLE technology rather than NFC.

Digital currencies, stablecoins and other crypto-assets are also seeing massive growth in recent years and more and more established financial institutions as well as central banks across the world start to embrace and explore the new opportunities. Central Bank Digital Currencies (CBDCs) are on the agenda across the globe, and many central banks working with this are actively making requirements towards enabling secure person to person (in some cases even off-line) transactions of this new type of 'digital cash'.

Infineon believes that connected devices will play an increasingly important role in the future of all digital transactions and will be a prerequisite for the successful mass adoption of crypto-assets like CBDCs. The total current and future value of the assets managed in combination with the value of the data generated via wearables and other connected devices is significant. The monetary value, as well as the ethics, should call for serious security considerations by both device manufacturers and service providers. Consumers will expect security, count on privacy and demand convenience from all involved providers.

Wearables are already part of our lives today and will surely – with the right solutions and services in place – become an even bigger part of tomorrow.

[21] https://www.visa.co.uk/content/VISA/usa/englishlanguagemaster/en_US/home/visa-everywhere/innovation/connected-consumer-survey.html
[22] https://www.amazon.com/b?ie=UTF8&node=16008589011

Where to buy

Infineon distribution partners and sales offices:
www.infineon.com/WhereToBuy

Service hotline

Infineon offers its toll-free 0800/4001 service hotline as one central number, available 24/7 in English, Mandarin and German.

› Germany	0800 951 951 951 (German/English)
› China, mainland	4001 200 951 (Mandarin/English)
› India	000 800 4402 951 (English)
› USA	1-866 951 9519 (English/German)
› Other countries	00* 800 951 951 951 (English/German)
› Direct access	+49 89 234-0 (interconnection fee, German/English)

* Please note: Some countries may require you to dial a code other than "00" to access this international number.
Please visit www.infineon.com/service for your country!

Mobile product catalog

Mobile app for iOS and Android.

www.infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany

Document number: B180-I0823-V2-7600-EU-EC-P
Date: 08/2021

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.