Connected devices and payment wearables in particular

www.infineon.com

Contents

1. Introduction

Infineon has a long and successful history of enabling and securing smart devices across the globe. In this white paper, we will dive into the topic of wearables, explore the different types of wearables and analyze some of the many current and future use cases – reaching beyond simple electronic gadgets to focus in particular on payment-enabled devices. We will also look into the requirements for wearables to gain increased traction in the market and to serve consumers globally.

2. What are wearables?

Wearables are basically mobile products or gadgets worn by the user as opposed to devices that are picked up and carried (like phones, tablets, etc.). By design, wearables thus enable the user to continuously interact – directly or indirectly – with the device.

2.1 Types of wearables

While we continue to see many ideas and innovative approaches in terms of new types of wearables brought to market, we will focus on three key types in this paper:

› Wristbands
› Smart watches
› Fitness/health trackers

All of these categories have seen successful products broadly adopted in the market. Arguably, body-mounted action cameras like GoPro should also be included in the list of widely adopted wearables, but given that the use cases around these types of products have not (yet) expanded beyond filming, we have omitted them from the scope of this paper.

2.2 Functionality

There are still many single-use wearables in the market and with increasingly low market entry barriers, we expect to see an increasing proliferation of relatively simple wearables designed for single use cases. In parallel, we are seeing wearables like smart watches developing into platforms in their own right.

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

It is also important to highlight the fact that the development of functionality in wearables, especially with regard to payment, has meant that smart devices in recent years have moved from consuming data to also generating and storing increasingly personal data directly on the devices. Consequently, the requirements for robust data security and device integrity have increased. We will elaborate on this in the Security chapter of this white paper.

2.3 Market growth

In 2013, ABI Research predicted that "Wearable computing devices, like Apple Watch, will exceed 485 million annual shipments by 2018"[1]. This would appear to be a case of early optimism and somewhat inflated expectations.

While development and adoption have not happened as quickly as expected, the market nonetheless demonstrates continuous growth. Recent estimates from IDC indicate a doubling of the market by 2021[2].

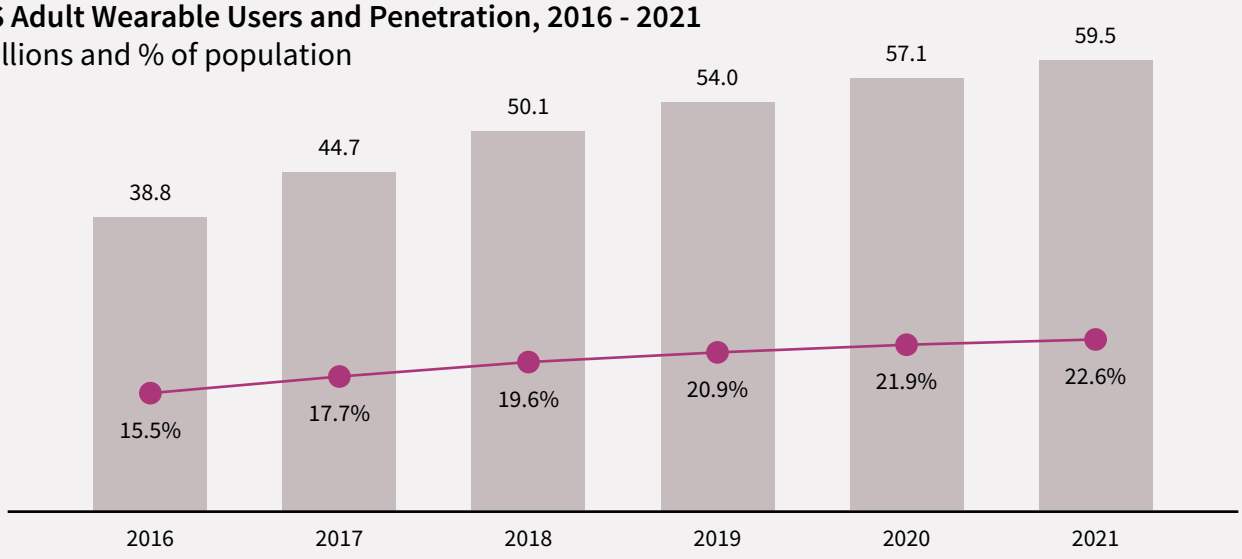
Top Wearable Devices by Product

Product	Shipment Volume 2017	Market Share 2017	Shipment Volume 2021*	Market Share 2021*	CAGR (2017 - 2021)*
Watches	71.4	56.9%	161.0	67.0%	26.5%
Wristbands	47.6	37.9%	52.2	21.7%	1.2%
Clothing	3.3	2.6%	21.6	9.0%	76.1%
Earwear	1.6	1.3%	4.0	1.7%	39.7%
Others	1.6	1.3%	1.4	0.6%	-16.0%
Total	**125.5**	**100.0%**	**240.1**	**100.0%**	**18.2%**

Source: IDC Worldwide Quarterly Wearable Devices Tracker, June 21, 2017

Slower adoption can likely be attributed to the fact that the supporting infrastructure for use cases like payment, including distribution of payment credentials, has taken longer to implement than was expected in 2013. As banks globally connect their card management systems to Token Service Providers (TSP) offering tokenization services specified by the global payment networks and other players, the infrastructure needed for issuing payment instruments to smart devices like phones and wearables has gradually become standardized and widely adopted. This, combined with rapid worldwide growth in contactless payments driven mainly by the mandates of the payment networks, has at least accelerated the adoption of payment-enabled wearables. Wearables like smart watches serve little purpose beyond acting as a "second screen" for the user's smartphone unless they support value-adding use cases such as payment.

US Adult Wearable Users and Penetration, 2016 - 2021
millions and % of population



Note: At least once per month; individuals aged 18+ who wear accessories or clothing embedded with electronics, software or sensors that have the ability to connect to the Internet (via built-in connectivity or tethering), which in turn collects and exchanges data with a manufacturer, an operator or other connected devices

Source: eMarketer, Dec 2017

[1] https://www.abiresearch.com/press/wearable-computing-devices-like-apples-iwatch-will/
[2] https://www.idc.com/getdoc.jsp?containerId=prUS42818517

2.4 Challenges facing wearables

As development of most wearable types is still at an early stage compared with the extremely fast-paced evolution of smartphones over the past decade, they still face several challenges. These hurdles are related to the fact that most wearables are small compared with smartphones. Currently, the biggest challenges facing many wearables are:

› Limited battery life
› High prices for consumers
› Limited use cases (compared with smartphones)

These challenges are similar to those seen with the first generations of digital watches, , and can therefore be gradually overcome if industry quickly drives the necessary innovation and developments.

Alongside these practical challenges, many devices also struggle with data security and device integrity – aspects which become 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].

[3] Please also see Infineon's white paper: Contactless Payment Accessories, April 2018

3. Security-critical wearable use cases

Typical wearable applications include telling the time, checking your calendar, counting your paces, measuring your heart rate, and the like. 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. A fitness tracker may also be integrated with 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 that are beyond the control of the user. These use cases call for additional security counter-measures, which are built into the device itself.

The security-relevant use cases are rarely standalone, and some of the best and most successful wearable solutions combine one or more of these use cases.

3.1 Payment use cases

Payment has always been a central use case for smart device manufacturers. The main reason for this is that payments tick a lot of the boxes that users are looking for in a wearable. Payment is:

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

That said, payment is also a challenging use case to tackle, as it is already extremely well-served in most countries where card payments are dominant. This, combined with the fact that payments are also driven more by habit than by connectivity options, makes any change in consumer behavior difficult.

Any payment solution ever brought to the market has been dependent on the acceptance infrastructure of the solution in question. Standardization around EMV and NFC for contactless payments has helped pave the way toward a richer choice of payment solutions. Contactless payment solutions have been further accelerated by the introduction of tokenization, which, again, has made distribution of payment credentials more flexible. As the proliferation of mobile phones with biometric sensing increases, biometric authentication of mobile contactless payments is expected to become a de-facto standard, and further enhance the popularity of a technology offering obvious convenience benefits for users.

Alongside mobile payments (using smartphones), we are now seeing an increasing proliferation of payment solutions in the shape of rings, wristbands, key fobs and chips directly integrated into smart clothing.

While payments via smartphones or wearables are experiencing steady growth rates, cards are likely to remain the dominant method for digital payments at the point of sale for the next five years. By April 2023, payment networks in most regions will require POS infrastructures to migrate in full to contactless payments to encourage the adoption of alternative form factors and increase contactless payment transactions using new devices. At this point, debit and credit cards will still be needed as a basis for a digital token stored in wearables or other devices. Rather than being carried on the person, they will increasingly be left at home.

Getting your wallet out can be troublesome, and there are distinct cases where a wearable device would make for a better and more seamless payment process. These cases include paying for transit tickets, getting on a bus or into a subway system 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 would mean that you no longer have to worry about your money or cards being stolen. Similar solutions have already proven effective at scale for music festivals and sports events, where they improve payment speed and reduce cash in circulation.

While most payment-enabled wearables focus on the ability to make payments, there is also a use case for designing wearables capable of receiving payments as demonstrated by the Dutch company N=5. With a group of partners, they designed the "Helping Heart", a jacket for homeless people, enabling the carrier to receive payments as people tap their contactless cards (or payment-enabled wearables) on the 'heart' on the jacket to donate money. The received funds can then be redeemed for short-term needs like food or shelter or more long-term goals like vocational training courses[4].

[4] https://nis5.pr.co/155981-a-unique-collaboration-between-advertising-social-enterprise-fintech-and-production-for-greater-good

3.2 Transit ticketing

Looking beyond payments, ticketing for public transportation is one of the most frequent digital use cases for 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 – whether in a travel card like Octopus used in Hong Kong or EMV-payment based ones used in London's transportation system – into a wearable device can increase convenience significantly for commuters.

Similarly, imagine a gate in Greater São Paulo for electronic toll collection where wearables make life so much easier for motorcyclists who can pay with the watch at the contactless gate instead of stopping and taking out a card to pay. In this case, the payment is made via a closed loop CIPURSE™ – based payment system, but it could also be effected via an EMVCo transaction.

We have seen recent examples of how this development could be taken one step further. Sweden's SJ rail company has offered a group of users the option to have a transit chip injected under the skin of their hand to ensure they never forget their travel passes[5].

3.3 Physical access

Key cards are widely used across corporate offices, factory buildings, gyms and other sports or service facilities across the world. Even private homes get digital "smart locks" installed. Traditional key cards can easily be integrated into simple wearables, while connected wearables allow for more granular access control, such as one-time keys for logistics companies delivering goods directly to your home (or car as introduced by Volvo in Sweden and Switzerland[6]). In the corporate context, 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.

[5] http://www.independent.co.uk/travel/news-and-advice/sj-rail-train-tickets-hand-implant-microchip-biometric-sweden-a7793641.html
[6] https://incardelivery.volvocars.com/

3.4 Identification & authentication

The general need and demand for two-factor authentication continues 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 possible 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 form of identification

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 serve as a PIN pad for 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 (SE) 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.

An interesting recent example of the latter was announced by the University of Michigan in late 2017 when a group of researchers came up with a way to utilize wearables to provide strong authentication for voice-based interactions such as services offered through Amazon Echo, Google Home or some of the increasing number of virtual assistants. The researchers found that voice recognition in itself was not sufficiently secure. To bring two-factor authentication to voice-based interactions, they developed a security token that could be integrated into a necklace, glasses or earbud combining voice patterns with the registration of speech-induced vibrations through the wearer's body[7], thereby creating a unique signature for strong authentication. This could also be integrated into a wearable.

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

Today, remote keyless systems have already become the de-facto standard for unlocking automobiles. However, it is still unusual to have a remote keyless system built into a wearable device that will unlock the car and continue, for example, to start the engine or arrange the seat to the exact preferences of the driver. These days, automakers are doing everything they can to integrate wearable solutions into their cars to cater to tech-savvy consumers. One example of this is South Korean automobile manufacturer Hyundai, which has introduced Hyundai Blue Link, 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.

[7] University of Michigan. "Wearables to boost security of voice-based log-in." ScienceDaily, 17 October 2017. www.sciencedaily.com/releases/2017/10/171017124400.htm

3.6 Enterprise use cases

Most of the previous use cases have focused on the individual and personal use of wearables. Many device manufacturers are also investing in the development of wearable technology for enterprise, corporate or industrial use. An important use case for enterprises, companies and university campuses is wearables that work to replace badges that control 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. Another example of enterprise or even industrial use is the Canadian firm Priologic, which has developed Hardhat Connect[8]. This platform connects a number of wearables from headgear to smart glasses to support collaboration across remote industry sites such as oil rigs, mines and forests. 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. Although still under debate, we have seen wearable location sensors used in hospitals to reduce the time staff spend finding each other during the day. A final high-profile example of successful industrial use of wearables is the collaboration between NASA and Microsoft that has brought Microsoft's Augmented Reality (AR) glasses – HoloLens – to the International Space Station, ISS[9]. The HoloLens allows ground staff to transmit 3D images to the ISS crew to support repairs and other tasks.

3.7 Security-relevant use cases with health tracking functionalities

Wearables have many great use cases within health tracking and monitoring. While fitness trackers are the type of wearable most people first think of, the ability to combine continuous tracking and measurement allows for much richer data generation and subsequent analysis than previously available.

Thanks to advancements 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):

- Steps
- GPS/location
- Elevation
- Speed/acceleration
- Light (in some cases also UV)
- Stress levels via Galvanic Skin Response (GSR)
- Heart rate/pulse
- Temperature
- Sleep patterns

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[10] have developed wearable solutions that serve this segment.

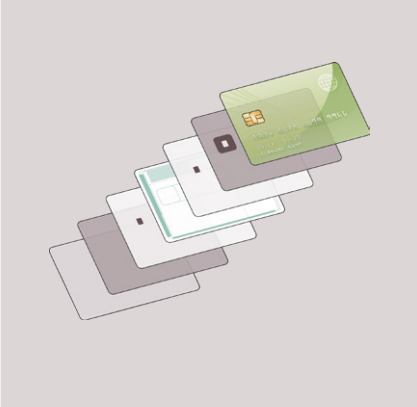
Wearables can also serve as potential life-savers or improve the quality of life for people living with a chronic disease as seen with the Empatica's Embrace[11] wristband that tracks and alerts epilepsy patients (and their carers) to potential convulsive seizures. Another example is the sleep apnea tracker Motio HW by Neogia[12]. These and other examples clearly show that wearables are much more than just "gadgets".

[8] https://hardhatconnect.com/
[9] https://blogs.windows.com/devices/2016/02/20/microsoft-hololens-in-space-making-science-fiction-mixed-reality/
[10] https://www.getqardio.com/qardiocore-wearable-ecg-ekg-monitor-iphone/
[11] https://www.empatica.com/
[12] https://neogia.xyz/

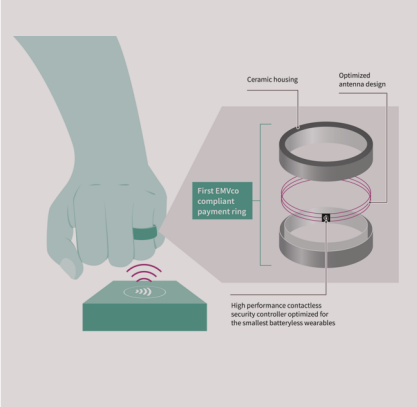
4. The evolution of wearables

As most wearables are smaller than smartphones, the deployment of Secure Elements (SE) 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. 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 (ISO 14443) and has a large antenna implemented in the card. Next came the design of advanced small-format contactless security controllers and non-connected payment accessories powered by small antennae – i.e. without batteries. Concluding the preliminary phase of 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 is generally integrated, and the NFC system is usually connected to a small battery for optimum contactless performance.



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

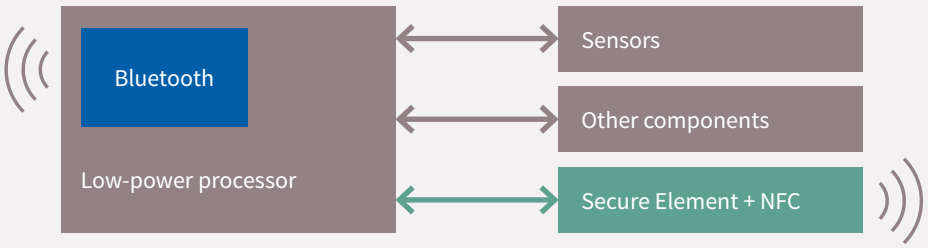


Advanced contactless security controller (small antenna acc. to ISO 14443)

Active contactless with battery driven micro-antenna and Internet connectivity

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

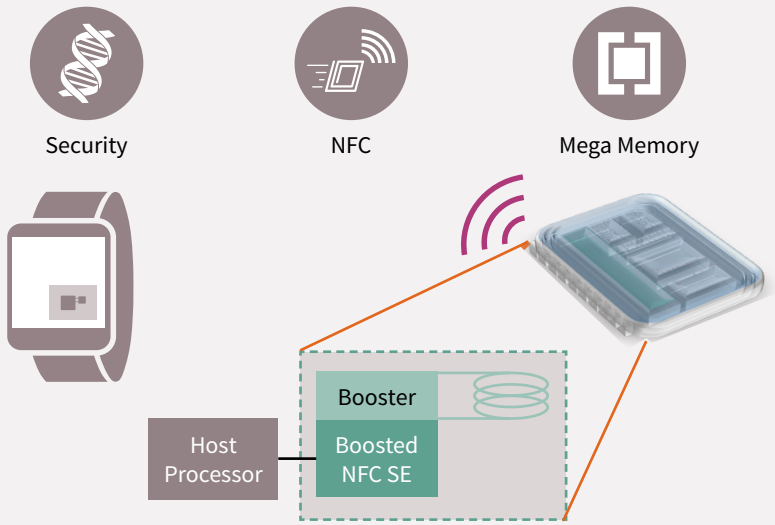
In order to enable high-performance Near Field Communication (NFC) solutions for SE systems, an IC supplier has to overcome some critical technical challenges. Wearable systems are usually designed on very small physical footprints and end users expect a long battery life.



Challenge 1:
Very low power consumption

Challenge 2:
Ultra-small physical dimensions & shielding for contactless communication

Consider the energy density of battery technology today. The only way to reduce the amount of power consumed by the component is to limit the power capacity. The standby power consumption of security NFC systems must be as low as possible. At the same time, all NFC applications must meet the relevant security and tamper-resistance standards to obtain all necessary security approvals. And the device must deliver the functional and power consumption performance mandated for contactless transactions using either a battery-less or very-low-power active NFC model. To meet market demand, Infineon specifically designed the architecture of IC sets either with large security memories and passive NFC modes, or compatible solutions in active NFC transmission mode with the lowest power consumption. One example is the SECORA™ Connect product delivered in ultra-small package dimensions (5x5 mm) and with all system components, including the antenna, integrated. These solutions consume only 1/3 of the power required for conventional modem solutions, while offering easy and quick system integration without the implementation of an additional software stack. Infineon thus delivers low-power, miniaturized components ideal for payment wearables.



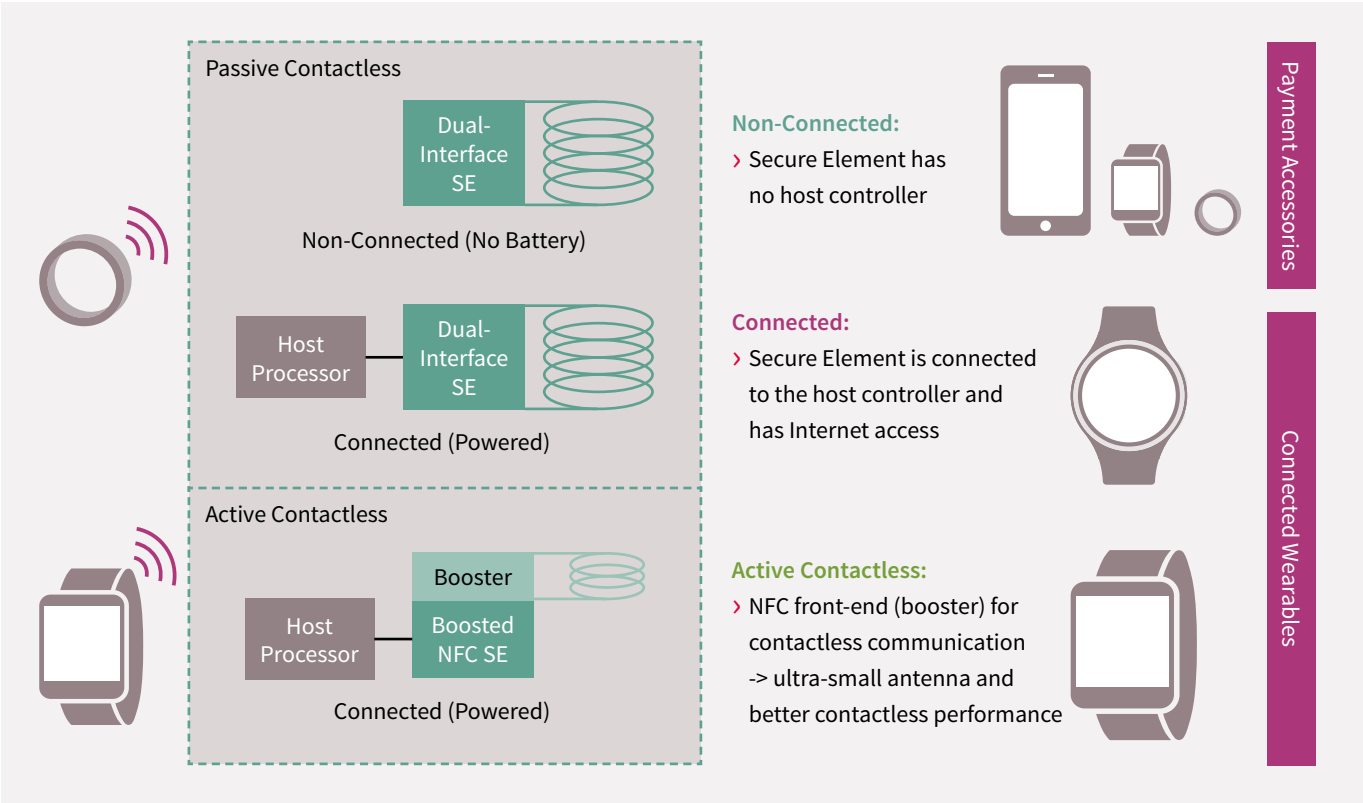
- Ultra-small: 5x5 mm SiP with integrated NFC antenna
- Simple interface with APDU according to ISO 7816 or I2C
- Card functions and tag
- Very low power consumption, 1/3 that of conventional NFC modem solutions
- Quick system integration without requiring NFC software stack

4.2 Different SE solutions for wearables

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

These non-connected wearables 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 network such as Visa or MasterCard) – which further supports the branding value, e.g. a certain stadium or festival.

The combination of dedicated hardware, controlled issuance and standardized or dedicated communication interfaces (e.g. to contactless readers) allows for a highly secure setup.



4.3 Connected wearables

Connected wearables, such as smart watches, 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 provisioned with different applications. This multi-application approach also allows for continuous development and deployment of apps or app-like services to the devices.

The move towards more flexible platforms to support connected wearables does, however, introduce some security concerns (similar to those associated with smartphones) as neither the hardware manufacturer nor the issuers of payment or similar services have full control over the other functions that the user may decide to install on their device. This means that the underlying hardware will have to meet even more robust security requirements. Tamper-resistant Secure Elements are even more important for security-critical use cases such as these. Software-based security can and should also be applied to payment applications on connected wearables, but since continuous software updates can prove even more challenging than in the case of smartphones, top-notch hardware security is paramount, especially for payment wearables.

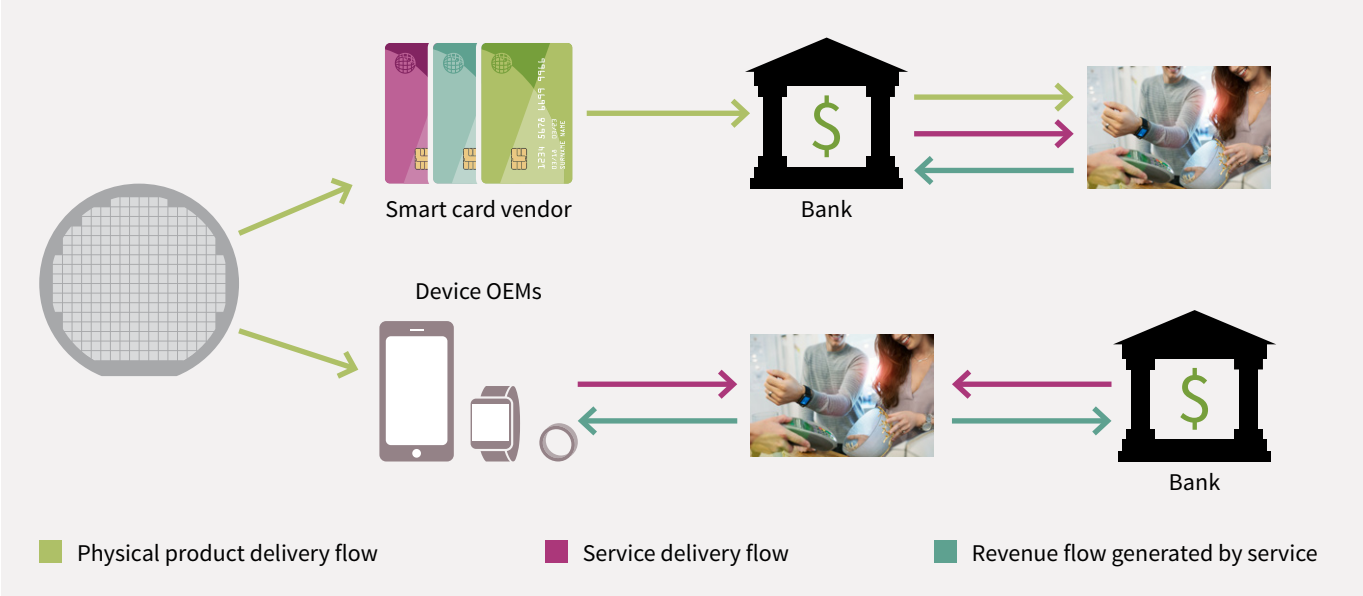
4.4 Service distribution and security

If we look at the distribution of electronic payment credentials in the traditional card issuance flow, secured hardware is the key enabler of identification, authentication, and transactions. This applies to ID cards, access cards and payment cards, and is typically built in by the chip manufacturers delivering the chip to the smart card vendors. These manage the physical production of the card – including the personalization (i.e. the embedding of the PAN – 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 optimized and fine-tuned over decades. This process can be easily replicated for simpler and often single-purpose wearables like the very successful payment wearables issued by Barclays called bPay[13].

For more sophisticated smart devices, the flow is radically different. The chip manufacturers still deliver secure hardware to the "device makers" similar to the card vendors, but in most cases the device makers sell their products directly to the consumer. This means that the consumer is no longer just a "cardholder" – i.e. the user but not owner of a bank-issued product – but actually a "device owner" who is in much greater control over the services that he or she wants to enable on his or her smart device.

This calls in most cases for a new type of business dynamic as well as a more fragmented (non-linear) value chain.



As banks are still responsible for the payment instruments they issue, they have to 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 (SE) – i.e. the chip on the payment cards – has been managed centrally by what is known as the personalization bureaux of the smart card vendors. The same process also applies to non-connected wearables, which makes it easy to replicate.

To support secured management of connected wearables, a number of security measures could and should be implemented.

[13] https://www.bpay.co.uk/

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.

1. Strong device identity
Device identity is not only a question of security, but is also a prerequisite for delivering personalized secure payment services.

2. User authentication
Once the identity of the device has been established, it is equally important that the service providers can 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.

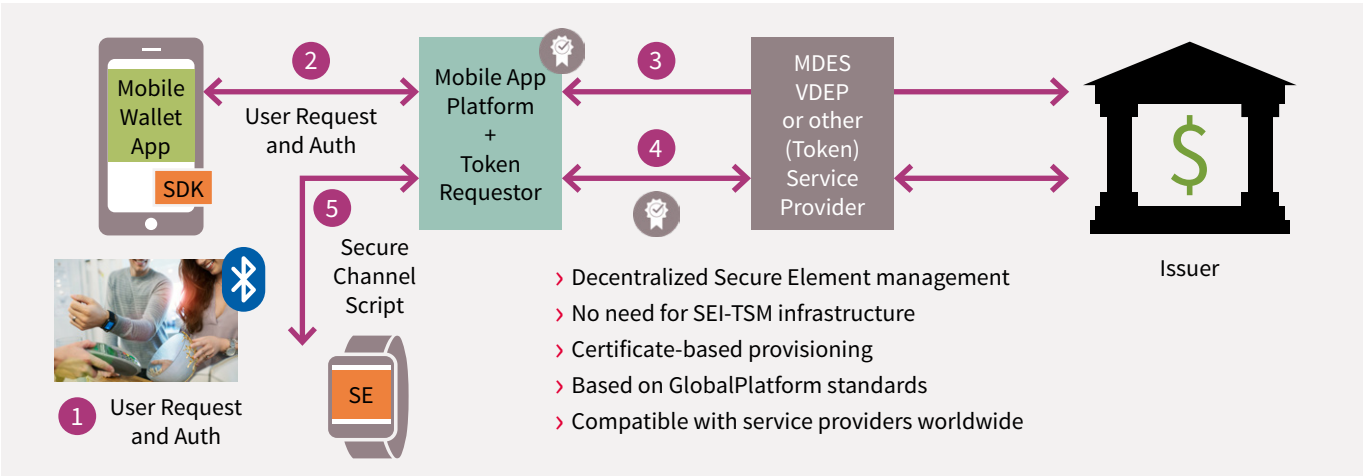
3. Strong device authentication
When connected devices request the initiation of a payment or the exchange of sensitive information, it is vital that the service provider fulfilling this request obtains certainty that the device is indeed the device of an identified user. Hardware-based security can be used to establish that a device has not been cloned.

4. Device integrity
As well as establishing the identity and authenticity of a device, security can be further enhanced by checking device integrity. In other words, dedicated hardware can detect and report attempts at tampering that could potentially compromise the device.

5. Remote attestation
Similar to the device integrity verification, remote attestation focuses on ensuring that the device plus software is running in a specified configuration or state. This can, for example, involve the establishment of secure enclaves.

6. Decentralized SE Management (DSEM)
In order to establish a secure service in a Secure Element of an endpoint device (e.g. mobile, wearable, IoT device), a service provider must typically use the Secure Element Issuer Trusted Service Management (SEI-TSM) system to deploy the application to a specific Secure Element in the field. This requires a direct business contract between the lower case and the Secure Element Issuer as well as direct technical integration of the service provider systems into the Secure Element 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 in the DSEM flow by mapping tokens with the initial PAN of the user and forwarding tokens to the issuers for authorization.

Considering the large number of different Secure Element Issuers, a service provider has to establish business contracts with several Secure Element Issuers and integrate its system with their systems in order to offer broadbase in-field service provisioning capabilities. Because of this, many service providers have limited service reach. This particularly applies in heterogeneous environments where a variety of different Secure Elements are available but may be provided by different Secure Element Issuers independently. Another key advantage of the DSEM platform its full compliance with GlobalPlatform GP standards Amendment A enabling fast and tight integration in the mobile app store without any proprietary and complex adaptations.



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

Connected, multi-application wearables are on the brink of a mainstream breakthrough. Fueled by the advancements of the IoT – which according to one report by Gartner will reach around 20 billion interconnected devices by 2020[14] – and the underlying tendency of technology to both increase in speed and decrease in size, payments are predicted to be one of the main transformational applications that will drive the mass uptake of wearable technology alongside services related to fitness, access, transit and healthcare. The sentiment is supported by a recent study conducted by Mastercard in collaboration with GCT Research, which shows that 175 million Europeans – approximately one quarter of the entire European population – are ready to use wearables like smart watches, bracelets and keyrings for contactless payments[15]. At any rate, it is still a nascent industry with a number of challenges to overcome. In addition to issues of standardization, manageability and aggregation of services, the main focus of industry leaders is on creating reliable and secure wearable devices that consumers can trust. With this development in mind, Infineon estimates that by 2020, at least 40% of all wearable devices will feature security functions.

5.1 The need for hardware-based security

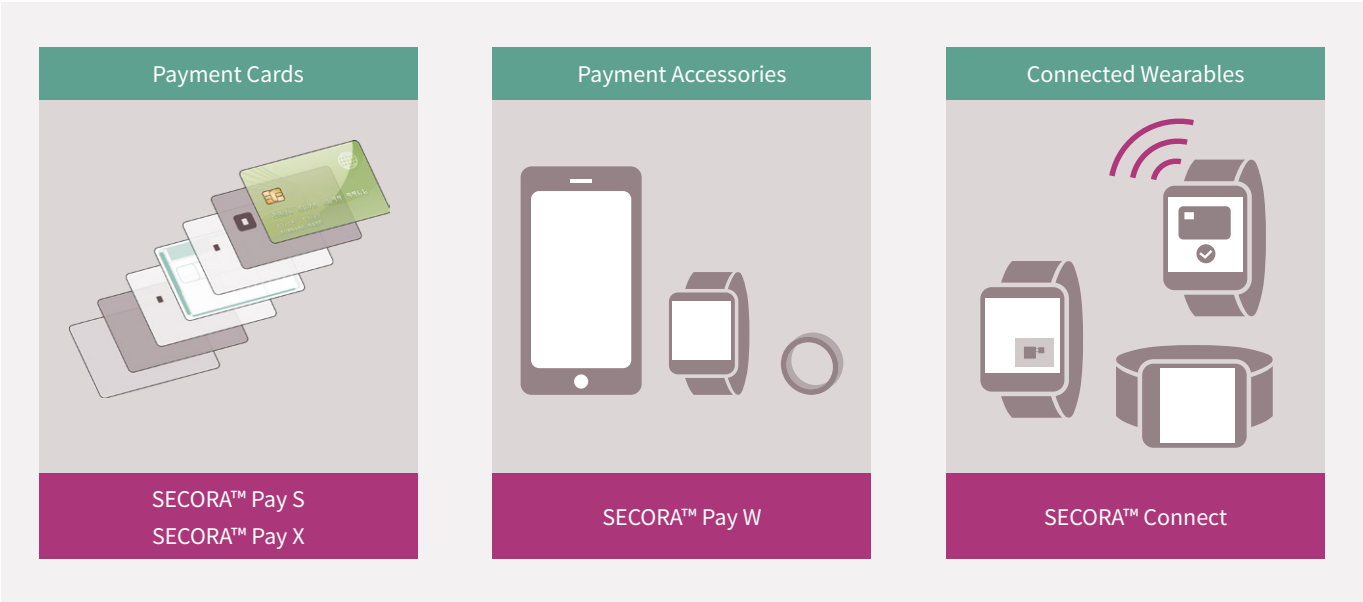
As NFC-based technology continues to gain traction and widespread acceptance, the way is gradually being paved for new kinds of convenient solutions and innovative use cases for wearable devices. But these use cases also present the industry with a number of safety and security challenges and concerns. This became evident in late January 2018, when news broke that the GPS tracking company Strava had created a Global Heat Map, using satellite information to map the movements 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[16]. 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 provisioning of security updates. That said, one of the greatest security challenges facing connected wearable devices relying on cloud-based payments like HCE – e.g. in cases such as transit – is the occurrence of temporary outages which affect device connectivity. Once a device is unable to connect and communicate with the cloud, it becomes impossible to complete any form of secured verification and authentication to enable a transaction.

[14] https://www.gartner.com/newsroom/id/3598917
[15] https://newsroom.mastercard.com/press-releases/over-175-million-europeans-ready-to-pay-with-wearable-devices/
[16] 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?noredirect=on&utm_term=.34afb553848a

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

With the rapidly growing global IoT market, it is not hard to imagine the profound impact this new evolution will have on a number of industries – not least the payment industry where consumers have come to expect seamless payment experiences on every available payment platform: cards, accessories and wearable devices.

One way to meet consumer demands is to employ hardware-based security via a lightweight Secure Element (SE) as provided by Infineon's Java Card-based payment solution portfolio SECORA™ Pay. This innovative suite of payment solutions (S, X and W series) bundles 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 be transformed into payment instruments. At the same time, this suite provides the flexibility needed to meet regional market requirements. SECORA™ Pay S is a ready-to-use solution for standard payment cards which follows the specifications of global schemes. SECORA™ Pay X supports multi-application and domestic payment schemes, while also supporting the CIPURSE™ open standard, enabling the realization of interoperable and sustainable business models for transport ticketing and beyond. The SECORA™ Pay W solution portfolio includes not only the EMV chip card OS and payment applets, but also offers innovative packaging options to meet market demand for non-connected, passive wearable or payment accessories.



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

With network mandates stipulating the shift towards contactless card issuance after October 2018 and April 2019, the industry is expected to provide innovative and future-proof solutions not only for the immense payment card market of 4 billion process control systems, but also for the rapidly growing wearable payments, where the requirements for security, durability and usability are rising.

Pre-approved EMV solutions from integrated circuit manufacturers are required in order to shorten certification and qualification processes and enable ODMs to develop power-efficient wearable solutions with the highest possible contactless performance. The payment dual-interface and wearable solutions presented in this paper deliver outstanding performance and approval lifetimes, while complying with the topmost industry quality and NFC performance standards.

Today, it is common for customers to carry two or three contact or dual-interface payment cards. However, a paradigm shift of the payment ecosystem is just around the corner. If industry players meet both the technical and technological requirements of the digital payments era, it is expected that all sorts of consumer devices will develop into IoT-enabled payment devices. This means that, within three to four years, customers will own a variety of connected payment devices linked to dozens of apps and web services. This paper demonstrates how industry players and partners already have the technology needed to supply the market with independent non-connected or connected Secure Elements that operate on minimal power consumption in ultra-small physical dimensions to fit into every modern consumer device.

5.3 Identifying the right use cases

ODMs will tailor wearable security functionality to the user experience their consumers are expecting and the wearable format (i.e. standalone or companion devices). Consequently, Infineon focuses on helping ODMs create the right platform to leverage their interface and develop the use cases that complement each product. However, as more and more services are provisioned to wearable devices, the lines between distinct services are beginning to blur. With a single application, it is much easier to pinpoint the different aspects of an application that requires a specific security level, but, by mixing a number of application services, you create a security system with demands that are increasingly complex to handle. Responding to growing consumer concerns and the development of industry standards, ODMs will be required outperform each other in relation to security, and consumers will abandon manufacturers who fail to repel attacks.

5.4 Standardizing across the industry

As more and more wearable-related applications and services emerge, it is becoming increasingly clear how standardization (and regulation) will be key to protecting the functionality, interoperability and security of connected wearable devices. Only by adhering to global standards will the entire industry invested in wearable devices be able to cooperate seamlessly to the benefit of all stakeholders. To further advance the development and integration of contactless payments using wearables, Mastercard, Visa, Discover and American Express are jointly pushing for a more consistent and regulated market. The global card schemes are all linked with security protocols and are working on connecting more and more issuers, processors, acquirers, OEMs and application developers through unified tokenization platforms and a newly announced single-button strategy[17] to harmonize a fragmented ecosystem. 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 contactless payment technologies[18].

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, increase the need for stronger and better authentication for most types of transactions as mandated by September 2019 by the EBA. For wearable devices seen as new form factors of contactless payment cards, the focus will be on increasing card-based payment and reducing cash handling. However, in the case of wearable devices enabled with biometric sensing functionalities, the combination of hardware-based security, health monitoring and biometric authentication will be a meaningful tool to support the strong customer authentication capabilities driven by PSD2 in Europe.

[17] The project is led by Mastercard and Visa, who are planning to convert their payment solutions, Masterpass payment and Visa Checkout, into one single checkout button.
[18] QR codes, HCE and SE NFC, and Wi-Fi.

5.5 Looking further ahead

With consumers increasingly adopting payment wearable and IoT devices into their daily lives, the demand for more seamlessly integrated and personalized, close-to-your-body devices with embedded multi-usage services is likely to increase over the next couple of years. The key to successful deployment, attuned to specific consumer needs at a particular time, will lie in making it as simple as possible to add additional services to a device and in managing multiple applications simultaneously. Regardless of the fact that some high-end wearables will feature standalone cellular network access, we expect large-display smart personal devices like smartphones and tablets to continue to function as the preferred platform when managing wearable devices. We also expect non-connected wearables like bracelets and smart rings to gain increased traction as they further replace cash for low-value 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 payment networks alike to help reduce cash usage and build a closer bond with consumers by embracing the new world of “situational finance”. Wearables will become a top digital payment choice for many by virtue of the fact that they offer a quick and convenient way of paying for products and services. 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 aspect of modern existence that deals with the quantification of consumers’ daily life in terms of data, it is paramount to have robust security measures in place to avoid compromising consumer privacy along the way.

Infineon believes that connected devices will initiate $1 trillion worth of transactions by 2020. Combining this monetary value with the value of the data generated, stored and transferred via wearables and other connected devices, the total value of wearable-enabled transactions is significant. The value, as well as the ethics, calls on both device manufacturers and service providers to give careful consideration to the security ramifications. Consumers will expect security, privacy and convenience from all stakeholders in the value chain.

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.

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

Date: 01 / 2019