


# eUICC for Connected Wearable Technology

Published by  **simalliance** now Trusted Connectivity Alliance



**eUICC for:**

***Connected wearable technology***

---

# INTRODUCTION

The explosive growth of the wearable technology market has been one of the key technological trends of recent years. Worldwide wearable device shipments are predicted to reach 237.5 million in 2021, up from 102.4 million in 2016 (Source: [IDC](#)), while the market for wearable devices is expected to reach over \$150bn annually by 2027 (Source: [IDTechEx](#)).

## Aim of this eBook...

This eBook explores the nature of certain security and logistical challenges posed by connected wearable devices, and suggests how the eUICC can be utilised to successfully address them.

## What is wearable technology?

The term wearable technology encompasses ultra low-power devices that can be worn on the body and which contain computer technology.

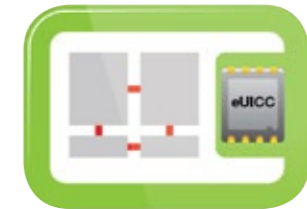
The term is undoubtedly broad, with myriad devices classed as 'wearables', including cameras, headsets and clothing. Watches and wristbands, however, are firmly established as the main form factors today, with a combined market share of close to 96% in 2016. This dominance is set to continue, accounting for 88% of the total market in 2021 (Source: [IDC](#)).

## What is a UICC?

UICC (Universal Integrated Circuit Card) is the hardware used in mobile devices that contains SIM and / or USIM applications enabling access to GSM, UMTS / 3G and LTE networks.

(Source: [GSMA – an industry association representing mobile network operators \(MNOs\)](#)).

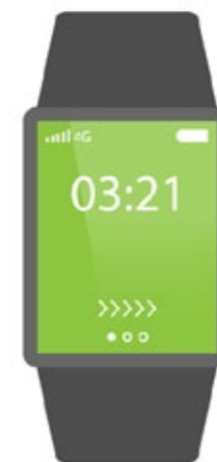
It is the most widely distributed secure application delivery platform in the world.



## What is an eUICC?

eUICC, also known as an embedded UICC or eSIM, refers to a UICC which:

- ▶ Is capable of hosting multiple network connectivity profiles (as defined by GSMA).
- ▶ Supports secure over-the-air (OTA) remote SIM provisioning as well as updates to the operating system (OS), keys, application and connectivity parameters, according to GSMA and GlobalPlatform Specifications.
- ▶ Securely executes sensitive services.
- ▶ Includes soldered (MFF1, MFF2, etc.) and traditional removable (2FF, 3FF, etc.) form factors.



The content of this paper focuses on connected wearables, specifically wearables enabled with cellular connectivity. This type of wearable device can either be autonomously connected to a cellular network via its own modem and a UICC / eUICC, or coupled with a connected primary device such as a smartphone.

In the latter case, a wearable device may still contain its own UICC or eUICC (i.e. it does not rely on a primary device for network identification). Due to limited user interfaces on certain wearables however, it may rely on coupling with a connected device through a local communication bearer, typically Bluetooth Low Energy (BLE) for eUICC personalisation or to facilitate set up.

## **Wearable connectivity choices**

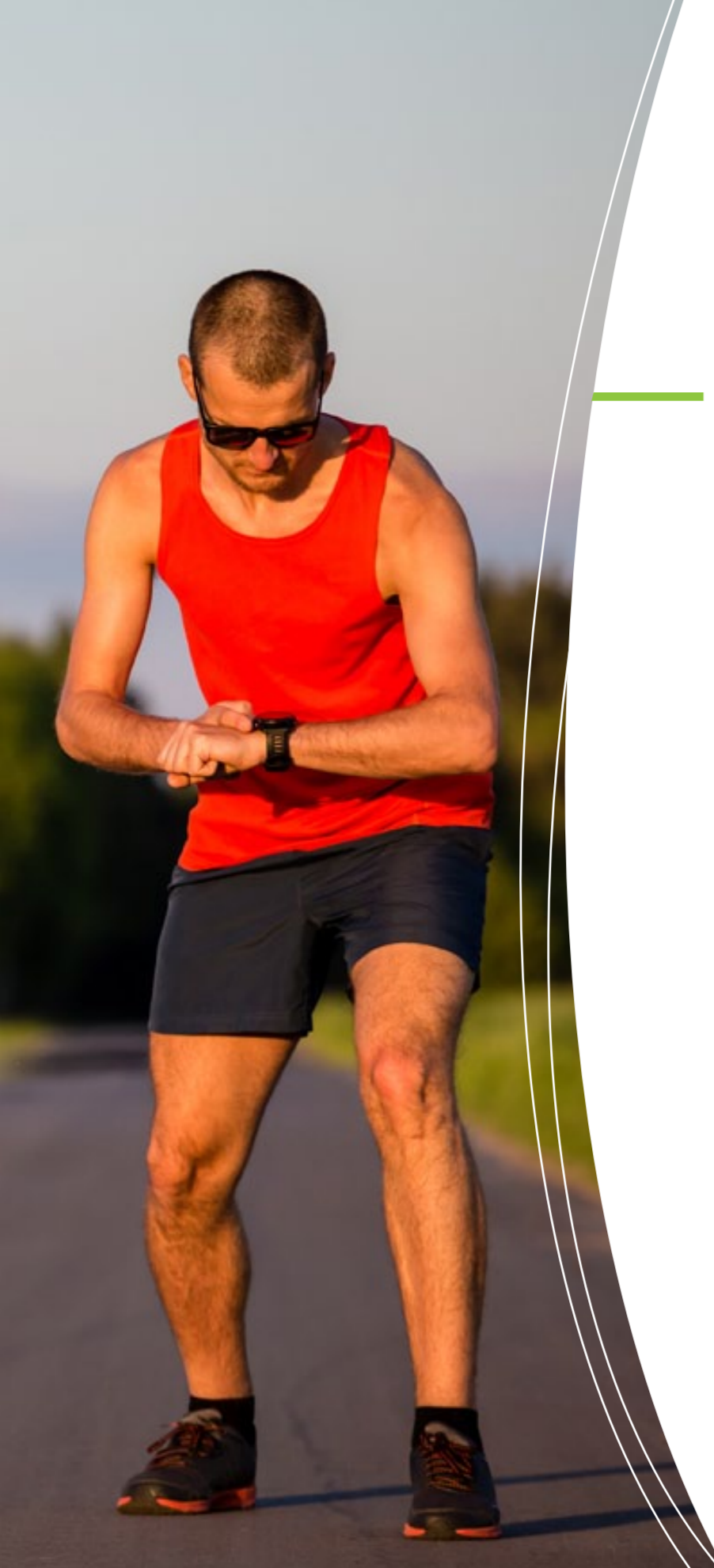
Wearable devices have evolved over decades from basic early iterations,

such as hearing aids and calculator watches, to all manner of wearable objects connected to each other and more generally, the cloud.

There are multiple ways in which wearable devices can connect with other devices and servers. Decisions are based on the frequency and duration of connectivity requests, in addition to bandwidth, power consumption and range considerations.

Traditionally, most wearable devices offer short-range connectivity options, such as BLE, primarily to benefit from low power consumption and a fast connection. This results in their reliance on a tethered companion device, typically a smartphone, to process data and manage communications. Although tethering delivers some advantages, especially when considering the limited user interface of many wearable devices, it does also serve to inherently limit the potential functionality.





## The benefits of cellular connectivity

Increasingly, device manufacturers are realising the benefits of incorporating cellular connectivity within wearable devices, such as broad reach across inhabited areas, low infrastructure costs, reduced deployment costs and quick implementation times. One of the key advantages is that wearable devices can communicate directly with the cellular network, in the same way as a smart phone does. This means that tethering is no longer required for data processing and unlimited connectivity, while wearable functionality can be enhanced to offer standalone voice, text, browsing and payments services, for example. It should be noted, however, that autonomous wearables must still tether to a primary device during the initial personalisation process.

The emergence of un-tethered wearable devices with cellular connectivity offers enormous potential for the development of an unforeseen volume of applications across multiple market sectors. By incorporating cellular connectivity, wearable manufacturers have the opportunity to enhance the value proposition of their devices, encouraging retainment and driving broader adoption.

In parallel, the security of cellular networks has been proven over decades. A particular feature of their success has been device and network authentication, which ensures that only authorised devices are connected. This offers lower costs and risk of security breaches in wearable device networks.

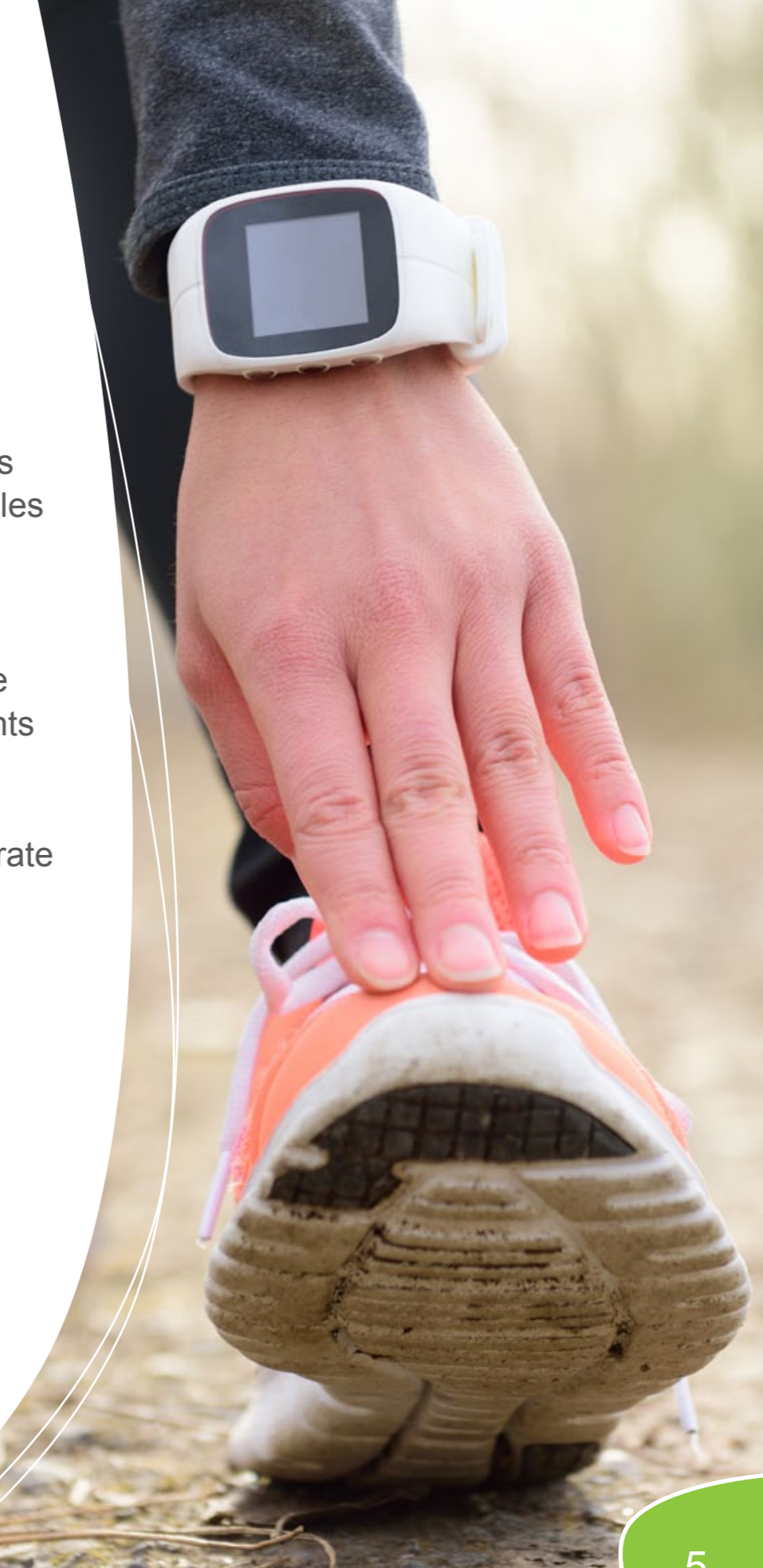
## Key use cases: fitness and healthcare

According to [IDC](#), health and fitness remains a major focus within the smart wearables market. Its report suggests that hybrid watches and other fashion accessories with fitness tracking capabilities are starting to gain traction, creating opportunities to sell multiple wearables to a single consumer under the guise of 'fashion'.

Another important application for wearables is the utilisation of data gained through personal health devices within

the healthcare sector. With care costs escalating rapidly worldwide, wearables offer healthcare organisations the opportunity to encourage users of personal health devices to lead a more active lifestyle, through tangible incentives such as insurance discounts (Source: [STAT News](#)). Similarly, insurance companies are using wearable data to develop more accurate risk profiles and calculate individual premiums accordingly.

*Health and fitness remains a major focus within the smart wearables market.*



# WEARABLES: WHAT ARE THE CHALLENGES?

As is well documented, the development and deployment of IoT and M2M solutions present various industry stakeholders with security and logistical challenges.

Wearable devices are no different.



## — Security challenges in wearable device deployments

► **Privacy breaches** – Wearable devices collate, store and transmit an unprecedented and unparalleled combination of highly sensitive user data, including but not limited to: health-related statistics and indicators; activity tracking and location information; payment credentials; purchasing records; messaging histories; and social media activity.

When combined, this data can be utilised to build a detailed picture of an individual's identity, health, behaviour, preferences and activity. Considering that the healthcare industry is uniquely vulnerable to privacy breaches – partly because healthcare records can contain the most valuable information available, including social security numbers, home addresses and patient health histories – the security of personal health devices should not be overlooked (Source: [ComputerWorld](#)).

In addition, the inherent sensitivity of the data, coupled with the rapid global

increase in ransomware attacks, exposes individuals to potential extortion and blackmail attempts if their data is compromised or breached (Source: [IBM](#)).

To prevent user data falling into the hands of malicious third parties, a solution is needed which offers flexible connectivity while protecting the confidentiality and privacy of data stored on the device and exchanged over the network.

► **Data tampering** – The increasing deployment of wearable data within the healthcare sector means that the consequences of data tampering and manipulation are profound. For example, it could lead to a patient being misdiagnosed, an individual being refused an insurance claim, or an employee incorrectly being deemed eligible to work. Appropriate protection and key encryption is therefore imperative to ensuring the integrity and accuracy of the data that is stored and transmitted.



- 
- ▶ **Software / firmware authenticity and integrity** – For the same reasons, it is imperative that the authenticity and integrity of the software / firmware within a wearable device is not compromised by malicious actors.
  - ▶ **Lost and stolen devices** – As devices become more advanced and powerful,

they are an increasingly high-value target for thieves. In parallel, the use of wearables in active and dynamic environments raises the risk of devices being dislodged and subsequently lost. This poses the risk that highly sensitive data stored on the wearable device can fall into unauthorised hands.

## Advanced security is key to countering these threats.

While there are differing options available, the eUICC is built on the most widely distributed and secure application delivery platform in the world (UICC), which is certifiable and specified by the GSMA.



## — Logistical challenges in wearable device deployments

► **Standalone connectivity** – As already mentioned, a growing number of wearable devices are becoming connected to cellular networks to deliver advanced functionality and communication capabilities. A solution is required which can provide this connectivity quickly.

Flexibility is also required to ensure a simple and efficient manufacturing and distribution process for devices. When producing a wearable with cellular connectivity, a device manufacturer will benefit significantly from the ability to develop and ship one device design compatible with various global MNOs.

► **Management of one cellular subscription across multiple devices** –

A single consumer may now possess multiple connected devices, e.g. a smartphone, a tablet, a laptop and various wearable devices. Some MNOs are already offering consumers the ability to use one subscription – and one telephone number – across many devices. As global device volumes increase, this ability to share one subscription across multiple devices will become ever more important to ensure end-user convenience. In line

with this, consumers need to be given the ability to manage their device subscriptions flexibly, both in terms of choosing MNOs and making subscription adjustments quickly and simply, as and when required.

► **Miniaturisation** – As the wearables market expands beyond health and fitness, improved aesthetics are central to encouraging adoption from broader audiences. This necessitates smaller components. According to [RCR Wireless](#), wearable devices are miniaturised for comfort, portability and to capture an aesthetic more common in high fashion than high tech.

► **Ruggedisation** – The nature of wearable devices means they must be designed to be sufficiently robust to withstand adverse and challenging environmental conditions, such as humidity, sweat, vibration and shock.

► **Battery life** – In the competitive wearables market, adequate battery life is a point of difference. Indeed, 47% of US consumers rank battery life as a highly important feature (Source: [Wareable](#)). Optimised power consumption is therefore a key consideration.



## What is a Secure Element?

A Secure Element (SE) is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities.  
(Source: [GlobalPlatform](#)).

As the **eUICC** retains all the security benefits of the UICC and the various discrete Secure Element (SE) form factors such as embedded Secure Elements (eSE), together with those of Trusted Platform Modules (TPM), **it is the most secure option for protecting highly sensitive use cases**. It also has significant logistical advantages. **Key benefits are associated with both the autonomy of cellular connectivity on optimised LTE and NB-IoT networks, together with remote management**, such as the ability to lock or wipe the device and enable subscriptions to be used across multiple devices.

*Key benefits are associated with both the autonomy of cellular connectivity on optimised LTE and NB-IoT networks, together with remote management.*

## What is a Trusted Platform Module?

A Trusted Platform Module (TPM) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform.

These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy (Source: [Trusted Computing Group](#)).

# HOW CAN THE eUICC OVERCOME THESE CHALLENGES?

The eUICC is well placed to overcome many security and logistical challenges associated with wearable deployments:



## Enhancing security

There are myriad reasons why the concept and design of the eUICC make it the most secure option and the best way to deliver advanced security to wearable devices:

### De facto security platform

The UICC has been proven through billions of deployments spanning decades as the best way to build security into mobile and connected devices.

An eUICC is still a physical hardware SIM product which, like UICCs and SEs, supports the execution of sensitive applications such as payment, access control and biometrics. This is combined with the ability to support OTA remote SIM provisioning and management. It is a discrete, tamper resistant hardware module with its own processing power and data storage, and is therefore isolated from those resources of the device, protecting data and keys stored and executed within it against hacking, tampering and unauthorised access. This means it retains all of the security benefits of traditional removable SIMs and SEs. It is also certifiable and specified by GSMA. When correctly developed, implemented and distributed, eUICC solutions are uniquely positioned to deliver the advanced security required by wearable devices.

### Remote security updates / upgrades

In parallel, the eUICC has the potential to provide security not only now, but in the future. Remote software / firmware upgrades and OS patches could be utilised to address emerging security challenges and threats. This flexibility and reactivity will be essential to ensure the long-term security of wearable devices.

*When correctly developed, implemented and distributed, eUICC solutions are uniquely positioned to deliver the advanced security required by wearable devices.*



*The eUICC is based on a highly efficient, advanced and security-certifiable process landscape.*

### **Data encryption**

Sensitive data stored within an eUICC on a wearable device can be encrypted, to prevent it being accessed by unauthorised parties, even if the device falls into the wrong hands in instances where it is either lost or stolen.

### **Secure process landscape**

Advanced security comes not only from the eUICC, but also the correct execution of the various related data management processes. For example, the exchange and transmission of sensitive data – such as that used

for billing, network authentication or the protection of encryption keys – requires a huge degree of trust between the stakeholders involved. The eUICC, together with the cellular connectivity it brings, is based on a highly efficient, advanced and security-certifiable process-landscape, borne through decades of successful partnerships between MNOs and SE vendors.

### **Soldered form factor**

Finally, the eUICC delivers physical security benefits. As it can be soldered and is tamper-resistant, it cannot be stolen and subsequently used fraudulently.





## Reducing complexity / increasing flexibility

### Secure cellular connectivity

As manufacturers increasingly seek to utilise cellular technology to deliver advanced functionality, the eUICC, based on the proven, established and secure UICC platform, is certified and specified by the GSMA.

Cellular networks offer higher bandwidth thanks to the UICC / eUICC authentication. This higher bandwidth enables device manufacturers to make safe and secure remote firmware upgrades to wearable devices, for example, in order to update features and provide new services.

### Remote profile provisioning and management

eUICCs offer OTA remote provisioning capabilities, which enables the loading and management of subscriptions for deployed wearable devices and the management of subscriptions across multiple devices.

### Miniaturisation

As the eUICC can be several times smaller than removable SIMs, wearable devices can be designed to be lighter and more streamlined, yet still benefit from the same functionality, security and connectivity features as provided by a UICC.

### Low power

As wearable manufacturers look to improve battery life as part of an enhanced value proposition, some forms of eUICC may be optimised for low power consumption.

### Ruggedisation

Since it is embedded, and capable of being managed remotely, an eUICC is a prerequisite for devices to be effectively waterproofed (sealed) and ruggedised for use.

# CHALLENGES OF WEARABLE DEPLOYMENTS

<i>eUICC features / functionality</i>	<i>Security Challenges</i>				<i>Logistical Challenges</i>				
	<i>Privacy breaches</i>	<i>Data tampering</i>	<i>Software / firmware integrity</i>	<i>Lost &amp; stolen devices</i>	<i>Standalone connectivity</i>	<i>Subscription mgmt</i>	<i>Device miniaturisation</i>	<i>Hostile environment</i>	<i>Battery life</i>
Remote provisioning & mgmt	X	X	X	X		X			
Tamper resistant	X	X	X	X					
Isolated	X	X	X	X					
Encryption	X	X	X	X					
GSMA certified	X	X	X		X	X			
Multiple connectivity profiles					X	X			
Soldered		X		X			X	X	
Miniaturised							X	X	
Ruggedised								X	
Low power									X





# THE ROLE OF THE SE INDUSTRY

The importance of security and simplicity within wearable deployments, and the increasing reliance on cellular networks to enhance device functionality and connectivity, means that the following assets of the SE industry are now more relevant than ever within this ecosystem:

- ▶ An established IT infrastructure capable of remotely managing the lifecycle of global UICC / eUICC deployments;
- ▶ Advanced understanding of cellular connectivity / MNO requirements;
- ▶ Developed 'trust' relationships with MNOs;
- ▶ A long-established and secure process landscape – are key to the continued expansion of this ecosystem.

SE vendors have the most extensive and proven experience in providing secure OS for UICC / eUICC, secure subscription and data management services, remote provisioning capabilities and a comprehensive understanding of MNO requirements, built over many decades and founded on a trusted relationship. These core competencies can be transferred and tailored to various IoT and M2M use cases, such as wearables, leaving the SE industry best placed to deliver the strongest available device security and reduced complexity for both consumers and manufacturers.



# CONCLUSION

The eUICC is already delivering advanced security and significantly reduced complexity to the wearables market. Most notably, it has been successfully deployed in flagship products from manufacturers such as Huawei and Samsung to millions of consumers across the world.

SE vendors are a key enabling stakeholder for the wearables sector as it continues on a path to rapid growth and expansion. The traditional core competencies of the SE industry translate seamlessly to support and facilitate the ongoing deployment of secure, advanced wearable devices.

*SE vendors are a key enabling stakeholder for the wearables sector as it continues on a path to rapid growth and expansion.*