


eUICC for Connected Cars

Published by  **simalliance** now Trusted Connectivity Alliance



eUICC for: *Connected cars*

INTRODUCTION

The growth in the Internet of Things (IoT) is disrupting even the most traditional market sectors. Transportation is no exception; connected car use cases today are rich and varied.

Mainstream technology and applications can already connect a single vehicle to an external cloud or server to deliver in-car services, such as music and video streaming, traffic alerts and even the European initiative, **eCall**.

Applications can also connect cars with other vehicles or infrastructure. This form of technology is called V2X (Vehicle to Everything) and enables multiple convenience and safety use cases such as autonomous driving and the provision of advance potential hazard warnings, such as road works, emergency vehicle approaching, nearby crashes etc.

With new enabling communication technologies on the horizon, such as 5G, connected car use cases and applications are set to grow exponentially.

Aim of this eBook...

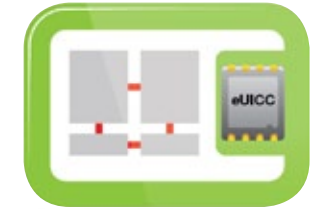
This eBook explores the nature of certain security and logistical challenges posed by connected cars, and suggests how the eUICC can be utilised to successfully address them.

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.

Connected cars: a growing market

While there is a noticeable variance in published data, one source (BI Intelligence) reports that annual connected car shipments will grow from 21 million units in 2016 to 94 million in 2021. The same source expects 381 million connected cars to be on the road by 2020, up from 36 million in 2015. In total, BI Intelligence estimates that the connected car market will generate \$8.1 trillion between 2015-2020.

What is a connected car?

Although definitions vary, this paper defines a connected car as a car which communicates with other devices / objects, and enables connected services, primarily through cellular networks.

While new connected car applications are emerging at an exponential rate, current use cases fall into one of the following categories:

- **Mobility management** – e.g. real-time traffic alerts, fuel consumption data etc.
- **Vehicle management** – e.g. vehicle diagnostics and maintenance, tracking stolen vehicles.
- **Safety** – e.g. vehicle condition alerts, external hazard alerts, eCall.
- **Entertainment** – e.g. high-resolution video and music streaming, WLAN hotspot.
- **Driver assistance** – e.g. autonomous driving, parking assistance.
- **Driver well-being** – e.g. fatigue detection, automatic climate control to ensure optimal driving conditions.

All current use cases point towards an easier, more comfortable and safer future driving experience. If there is one use case, however, that will have the biggest impact on society over a relatively short timescale, it is likely to be autonomous driving. And, when the utopian vision of driverless cars becomes a reality, so will the new security and functionality requirements that will be critical to its delivery.





— Autonomous driving: new functional and security requirements

Offering higher bandwidth, ultra-reliable networks, lower latency and much faster connection speeds, new technologies such as 5G will be influential in bringing autonomous driving – alongside other diverse connected car applications – to the mass market. Sources referenced by [NGMN](#), a mobile telecommunications association of mobile operators, vendors, manufacturers and research institutes, suggest that highly automated driving will hit the road around 2020 and will mature between 2025-2033.

The autonomous driving trend is resulting in new communication requirements for vehicles. In this use case, where human lives are at risk, autonomous vehicles must be consistently aware of, and able to interact with, their surroundings.

This V2X communication spans:

- ▶ V2I (Vehicle-to-Infrastructure) – obtaining data from road signage and signals.
- ▶ V2V (Vehicle-to-Vehicle) – to avoid collisions with other vehicles.
- ▶ V2P (Vehicle-to-Pedestrian) – ensuring safety with pedestrians and cyclists.
- ▶ V2N (Vehicle-to-Network) – real time data about traffic.

Ultra-reliable network connectivity is therefore a critical success factor.

Security, encompassing authentication, data authenticity / integrity, and privacy, is also a vital consideration in this use case. Already, connected vehicles provide attractive targets to attackers, even if reported hacks, such as the Chrysler Jeep hack in 2015 where the hackers were able to force a Jeep off-road and into a ditch, are limited in scope and have been carried out by researchers or academics (Source: [The Guardian](#)).



CONNECTED CARS: WHAT ARE THE CHALLENGES?



— Security challenges of connected vehicles

- **Hacking and hijacking** – As vehicles become increasingly connected, the threat posed by hackers is growing. If attackers command control of a vehicle, there is the potential for them to remotely hijack and subsequently steal or crash the vehicle. The worst-case scenario is that by exploiting a security vulnerability common to a manufacturer or model, hackers could execute a ‘fleet-wide’ attack and simultaneously hijack millions of vehicles (Source: [Electrek](#)). Combatting the risks posed by remote hijacking is particularly pertinent considering the increasing use of vehicles as a threat actor in terrorist attacks.
- **Authentication** – With an increasing number of external objects and interfaces communicating with cars, the need to authenticate the identity of the user, the car’s own network connection and devices connecting with the car has never been so important. In the same way that only authorised individuals should gain access to a vehicle and its controls, the same can be said about external devices. This is a pre-requisite to ensuring that the authorised user – who is authenticated in advance – remains in control of the vehicle at all times.
- **Privacy breaches** – Connected vehicles collect and communicate vast swathes of data, particularly regarding a user’s location and behaviour. To prevent sensitive user data being intercepted and utilised by malicious third parties, connected cars need to offer flexible connectivity while protecting the confidentiality and privacy of data stored on the vehicle and exchanged over the network.
- **Data authenticity and integrity** – The implications of data tampering, manipulation and spoofing (where data is communicated by an unauthorised source) are serious, particularly in the context of automated mobility where the transmission and receipt of inaccurate data could result in collisions and fatalities. Appropriate mutual authentication, data and key protection and encryption is therefore imperative to ensure the provenance, integrity and accuracy of the data that is received 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 connected car is not compromised by malicious actors.

► **Remote software / firmware updates and upgrades** – The pace of advancement within the automotive industry means that both functionality and the threat-landscape are evolving rapidly. Software and firmware in connected cars must be updated regularly, yet it is not feasible for vehicle owners to take their cars to a garage each time an update is required. Besides the convenience factor, some updates, particularly those related to security vulnerabilities, need to be installed

immediately. Updates and upgrades can be managed remotely, OTA, however this process needs end-to-end security – covering data transmission and storage of the cryptographic keys and data within the connected car. If not fully protected, updates could be intercepted and manipulated by unauthorised parties, who could equally use what they learn from the software update data to circumvent security parameters.

► **Conditional access for in-car entertainment** – In-car entertainment systems are now highly advanced, particularly in luxury models. This is leading to a growing consumption of premium content, which requires more sophisticated conditional access policies and systems.



Security considerations: Connectivity and secure services

The security challenges that need to be addressed relative to connected cars are real, diverse and constantly evolving. An advanced, dynamic security solution is key to countering these threats.

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. While it provides secure cellular connectivity, it also offers the security advantages of an embedded Secure Element (eSE). As such, it can be additionally used to enable secure services in the car (fast signature for V2X, toll payments, user authentication in the car, key lock etc). Car manufacturers should consider the use of an eSE – whether dedicated or combined with the eUICC used for cellular connectivity – to isolate and protect the storage and processing of keys and data associated with the delivery of sensitive services within their vehicles.

Another hardware security approach that should also be referenced is the Trusted Platform Module (TPM). Although traditionally found in PCs and laptops, there is an increasing recognition of the value of certain TPM features within the automotive context. For example, the secure boot provided by TPMs can be deployed to ensure the authenticity of integrity of software / firmware to prevent reflashing and jailbreaking of devices, support secure software / firmware updates and upgrades, and deliver secure management of cryptographic keys.

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](#)).

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](#)).



— Logistical challenges of connected vehicles

► **Connectivity** – Network coverage will be critical in many connected car use cases, for the vehicle must always be aware of its environment and able to interact with it at all times. Specific requirements will therefore include the ability to operate without network coverage, through non-3GPP means such as proximity services for device to device communications.

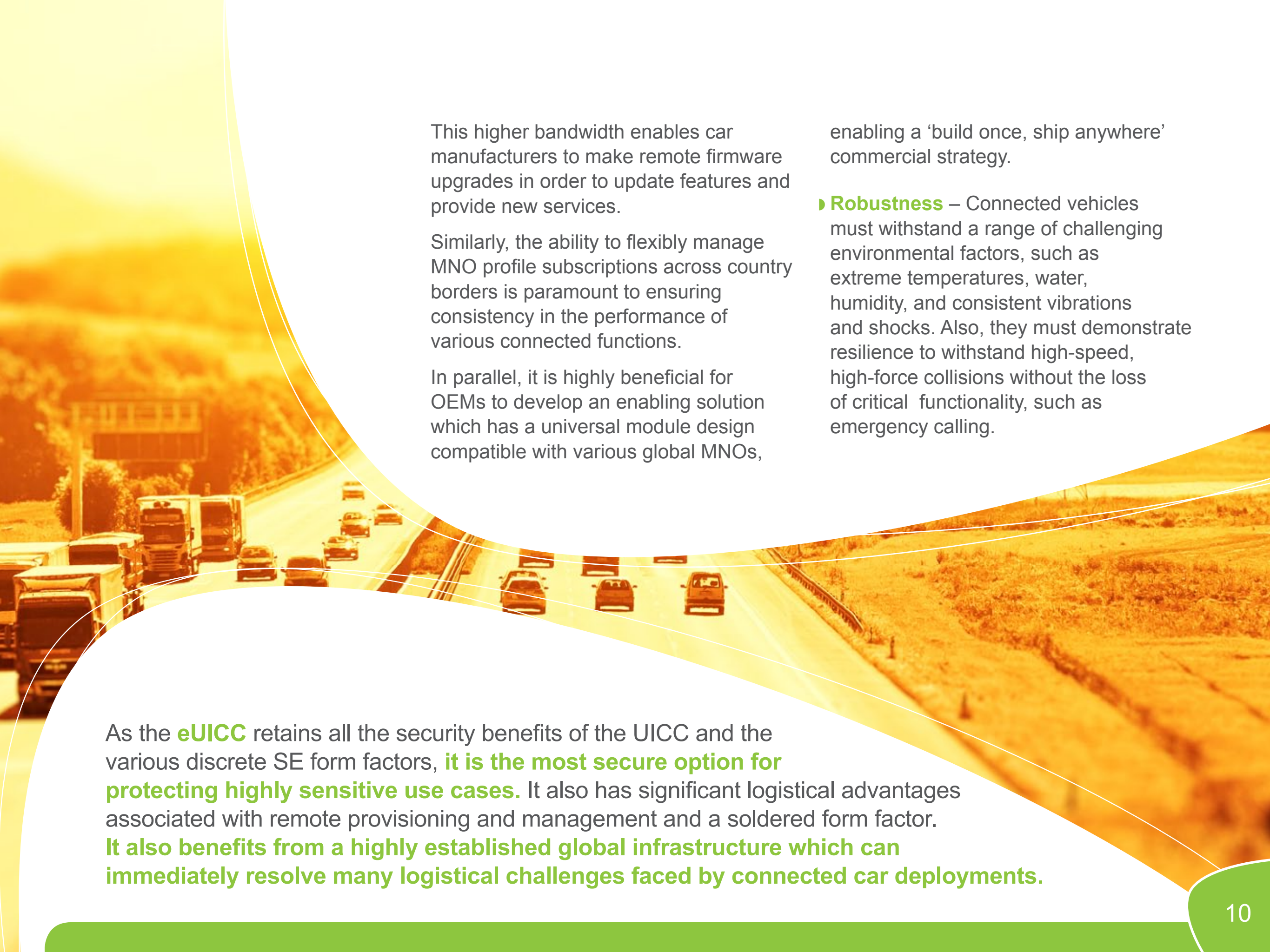
It has been widely acknowledged that the advent of 5G will be a key market enabler – and potentially a unifying connectivity technology – for certain connected car use cases because of the performance advantages that it will provide over existing connectivity. These include faster throughput and the ability to process the significantly higher levels of data traffic that a burgeoning global connected car ecosystem will generate.

► **Regulation** – With the rise in sensitive use cases and the growing volume of data generated and transmitted by connected cars, car manufacturers will increasingly need to navigate a complex and evolving regulatory landscape. A successful connected car ecosystem will require security solutions which can

provide the necessary certifications and assurances to ensure compliance with regulation covering aspects such as data protection, safety and payments. In parallel, solutions must ensure continued alignment and compliance with existing quality control standards such as ISO/TS 16949, which applies to the design, development, production, installation and servicing of automotive-related products (Source: [ISO](#)).

► **Post-issuance personalisation and remote management** – The average age of a car on the road is currently 11.6 years, during which it will have an average of four owners (Sources: [Automotive News / RAC](#)). This suggests that besides the initial personalisation of a vehicle, which must be carried out post-production, various MNO profile changes, software, firmware and application updates and upgrades will be necessary during the lifespan of a connected vehicle.

To maximise efficiencies for both OEMs and consumers, there is a requirement for these to be managed remotely. Cellular networks offer higher bandwidth thanks to the UICC / eUICC authentication.



This higher bandwidth enables car manufacturers to make remote firmware upgrades in order to update features and provide new services.

Similarly, the ability to flexibly manage MNO profile subscriptions across country borders is paramount to ensuring consistency in the performance of various connected functions.

In parallel, it is highly beneficial for OEMs to develop an enabling solution which has a universal module design compatible with various global MNOs,

enabling a 'build once, ship anywhere' commercial strategy.

- **Robustness** – Connected vehicles must withstand a range of challenging environmental factors, such as extreme temperatures, water, humidity, and consistent vibrations and shocks. Also, they must demonstrate resilience to withstand high-speed, high-force collisions without the loss of critical functionality, such as emergency calling.

As the **eUICC** retains all the security benefits of the UICC and the various discrete SE form factors, **it is the most secure option for protecting highly sensitive use cases**. It also has significant logistical advantages associated with remote provisioning and management and a soldered form factor. **It also benefits from a highly established global infrastructure which can immediately resolve many logistical challenges faced by connected car deployments.**



HOW CAN THE eUICC OVERCOME THESE CHALLENGES?

The eUICC is well placed to overcome many common security and logistical challenges associated with connected car 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 the advanced security required by connected vehicles:

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 and objects.

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 separate, 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. 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 connected vehicles, to address hacking, privacy, authenticity, integrity and anti-piracy among other security requirements.

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 reduces the risk of security breaches in connected vehicle networks.

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



The eUICC has the potential to provide security not only now, but in the future.

Remote security updates / upgrades

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. In addition, SE vendors have extensive and proven experience in ensuring the security of remote management capabilities. This expertise, flexibility and reactivity will be essential to ensuring the long-term security of connected vehicles.

Data encryption

Sensitive data transmitted and stored by a connected vehicle can be encrypted by the eUICC, to prevent it being accessed by unauthorised parties.

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

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

Connectivity

As the automotive industry increasingly looks to leverage evolutions in cellular technology, and benefit from the vast and well-established systems landscape that supports it, the eUICC (based on the proven, secure UICC platform) is certified and specified by the GSMA.

Remote profile provisioning and management

eUICCs offer OTA remote provisioning capabilities. This enables OEMs to ship vehicles directly to the location of sale, where the correct network profile can be downloaded OTA upon connection to the GSMA Remote SIM Provisioning for M2M system. If a change of MNO is subsequently required, OTA remote provisioning can again be used to remove an existing profile and download a new network profile directly to the vehicle.

Reduced servicing requirements / costs

Remote management capabilities remove the requirement for regular time-intensive, costly manual software updates and upgrades. Indeed, it is estimated that remote management capabilities will save OEMs more than \$35 billion by 2022 (Source: [IHS Markit](#)). Consumers will also benefit from increased convenience, such as reduced visits to dealerships for vehicle servicing.

Ruggedisation

Since it is embedded, and capable of being managed remotely, an eUICC is a prerequisite for devices to be effectively ruggedised for use in extreme physical environments.

CHALLENGES OF CONNECTED CAR DEPLOYMENTS

<i>eUICC features / functionality</i>	<i>Security Challenges</i>							<i>Logistical Challenges</i>			
	Hacking & hijacking	Authentication	Privacy breaches	Data authentication & integrity	Software / firmware authenticity & integrity	Remote updates & upgrades	In-car entertainment piracy	Connectivity	Regulation	Post-issuance mgmt	Extreme physical environments
Remote provisioning & mgmt	X	X	X	X	X	X	X		X	X	
Tamper resistant	X	X	X	X	X	X	X				
Isolated	X	X	X	X	X	X	X				
Encryption	X	X	X	X	X	X	X				
GSMA certified	X	X	X	X	X	X	X	X	X	X	
Multiple connectivity profiles								X	X	X	
Soldered											X
Miniaturised											X
Ruggedised											X
Quality controlled									X		



THE ROLE OF THE SE INDUSTRY

The reliance of connected car deployments on evolving cellular technologies, and the growing importance of security spanning all use cases, means that the existing assets of the SE industry are critical to the continued expansion of this ecosystem.

These assets include:

- ▶ The most widely distributed secure application delivery platform in the world;
- ▶ An established IT infrastructure capable of remotely managing the lifecycle of global UICC / eUICC deployments;
- ▶ An advanced understanding of cellular connectivity / MNO requirements;
- ▶ Developed 'trust' relationships with MNOs;
- ▶ A long-established and secure process landscape.

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 connected cars, leaving the SE industry best placed to deliver the strongest available vehicle security, as well as reduced complexity for both consumers and manufacturers.



CONCLUSION

- ▶ The eUICC is already delivering enhanced security and reduced complexity for connected vehicle deployments and from 2018, every new car in Europe will be connected to the mobile network via an eUICC in order to enable the mandatory eCall service.
- ▶ With 5G set to play a vital role in enabling autonomous driving and other connected car use cases of the future, the eUICC provides an instantly available, interoperable infrastructure which is already well established across the globe. This offers huge efficiencies in development and deployment costs and time to market.
- ▶ Its remote management capabilities are also uniquely suited to the mission-critical needs of the connected car industry, particularly when coupled with the renowned and proven security of the UICC as the most secure application delivery platform.
- ▶ SE vendors have established the infrastructure, processes and relationships required to successfully manage the lifecycle of deployed UICCs / eUICCs.
- ▶ The traditional core competencies of the SE industry translate seamlessly to support and facilitate the ongoing deployment and development of connected vehicles.