

*An analysis of the security needs
of the 5G market*

A SIMalliance 5G Working Group marketing white paper

An analysis of the security needs of the 5G market

Paper created by
the SIMalliance
5G Working Group: ↓

- Patrice Beaudou, Gemalto
- Paul Bradley, Gemalto
- Elodie Clement, OASIS
- Remy Cricco, Morpho (Safran)
- Claus Dietze, Giesecke & Devrient
- Eric Laffont, Comprion
- Daniela Lopez, VALID
- Ruben Martinez Gonzalez, VALID
- Dragan Vujcic, Oberthur Technologies
- Tomasz Wozniak, Oberthur Technologies

About SIMalliance

SIMalliance is the global, non-profit industry association which simplifies aspects of hardware-based device security to drive the creation, deployment and management of secure mobile services. The organisation promotes the essential role of a dedicated tamper resistant hardware module in delivering secure mobile applications and services across all devices that can access wireless networks. By identifying and addressing related technical issues, and both clarifying and recommending existing technical standards relevant to the implementation of hardware security, SIMalliance aims to facilitate and accelerate delivery of secure mobile applications globally.

SIMalliance members represent 90% of the global SIM card market. As such, SIMalliance's membership is responsible for delivering the most widely distributed secure application delivery platform in the world (UICC/SIM/USIM).

SIMalliance members are Card Centric Solutions, Eastcompeace, Gemalto, Giesecke & Devrient, Incard, Kona I, Morpho, Oasis Smart SIM, Oberthur Technologies, VALID, Watchdata, Wuhan Tianyu and XH Smartcard (Zhuhai) Co. Ltd.

SIMalliance strategic partners are Comprion, Linxens and Movenda.

Table of Contents

1. Executive summary	4
<hr/>	
2. Introduction	4
<i>2.1 5G: its definition and standardisation</i>	4
<i>2.2 Significant actors in the 5G ecosystem</i>	5
<i>2.3 SIMalliance findings about 5G</i>	5
<hr/>	
3. Potential security requirements in 5G	6
<i>3.1 Network operations</i>	7
<i>3.2 Examples of use cases and their diverse security needs</i>	7
<hr/>	
4. A hardware based approach to meeting the 5G security challenge	10
<i>4.1 Segment summary</i>	10
<i>4.2 A potential solution</i>	11
<hr/>	
5. Conclusion and next steps	12

1. Executive summary

It is early days for 5G. While the industry has a clear vision of services that it hopes 5G will facilitate, much remains to be determined on the technical front with standardisation activities just beginning. However it is clear that security and privacy will remain fundamental requirements, with the changes foreseen for 5G likely to broaden the range of attractive attack targets.

This paper sets out to provide a high level analysis of the main potential market segments where 5G will have a transformational impact and to assess the diverse security requirements for those markets.

Four main segments for 5G have been defined: Massive IoT, Critical Communications, Enhanced Mobile Broadband and Network Operations (which underpins the three other areas).

Across these segments, security requirements will vary, both at the network access level and at the service level, where demands may range from those posed by low level sensors to those of high-end use cases like real-time remote controls, driverless mobility and remote surgery.

Needs will differ around how frequently communication occurs, the amount of data to be managed and communicated, speed and latency and around how frequent authentication has to be.

For example, critical communications will require much more frequent authentication than IoT and will involve far more sensitive data. Conversely, massive IoT will provide a scenario where devices will communicate infrequently, use low power and may require extended lifespans. In enhanced mobile broadband and in critical communications, performance demands may open the way to enhanced and highly efficient security mechanisms.

Changes in the business aspect of the 5G ecosystem and other technological developments, some likely, others hypothetical such as the possible arrival of quantum computing, will also combine to add to the complexity of the security challenges.

According to the demands of the segment, a broad range of security solutions or changes in feature sets of those solutions are likely to be needed. However based on the analysis laid out in this paper, the SIMalliance proposes that dedicated tamper resistant hardware may offer value in many aspects of 5G. In addition, much is yet to be determined, including the need for backward compatibility with earlier generations of communications.

2. Introduction

Since the early days of digital mobile communications, security and privacy have been fundamental underlying requirements for mobile applications and services across devices that access wireless networks. Now, work is starting on defining the technology behind 5G communications where enhanced levels of security and privacy foundations will be required to take the industry smoothly through the next 15-20 years.

The intention of this paper is to examine the main potential market segments where 5G will have a transformational impact and to assess the diverse security requirements for those markets around user, service and network-level identification, authentication and privacy as well as data integrity and protection.

2.1 5G: its definition and standardisation

It is important to understand that today in 2016, 5G is not a technical standard. Instead it is defined by a set of aspirations around desired services intended to be commercially available around 2020. These services are expected to place new requirements on connectivity, flexibility, cost efficiency and performance. Some companies have already announced that they intend to launch 5G capable networks commercially in 2018.^①

According to Next Generation Mobile Networks (NGMN) Alliance^②, this means that where needed, 5G networks will provide lower latency, greater reliability, greater throughput, higher connectivity density, better coverage and higher mobility range. These features will be provided by different network layers leading to the need to provide security, privacy, trust and identity within a highly diverse technical and functional environment.

① <http://www.ericsson.com/thecompany/press/releases/2016/01/1980613>

② https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf

2.1 5G: its definition and standardisation (cont.)

Currently, there is still debate about what 5G actually is. GSMA[®] identifies two views:

1. A service led view, painting 5G as a consolidation of previous standards and innovations, providing greater coverage and reliability;
2. Sub 1ms latency and >1 Gbps download speed.

Standardisation body 3GPP has split down 5G into four major areas on which to focus during the standardisation of the technology:

- Massive IoT;
- Critical communications;

- Enhanced mobile broadband;
- Network operations (which underpins the three areas above).

SIMalliance has set out to review each of the above areas in terms of their security requirements. Irrespective of which view of 5G or indeed a combination of views, prevails, it is clear that security is a major requirement for 5G in these areas as it has been for previous standards in an ever more connected environment.

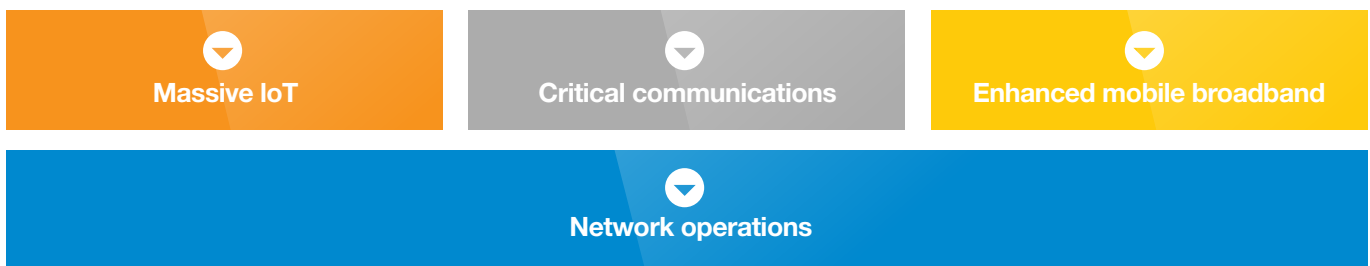


Figure 1 – 5G market segments

2.2 Significant actors in the 5G ecosystem

5G and its development is of considerable interest to government, standardisation bodies, industry manufacturers, including OEMs and chipset manufacturers and designers, telecommunications operators, service providers, application providers, operating system providers, SMEs and researchers, amongst others.

Significant actors in the ecosystem include:

- 3GPP, which unites seven telecommunications standards bodies ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC and will develop the dominant standard;
- NGMN, a grouping of leading operators, vendors and universities;

- GSMA, the industry body of mobile operators;
- Regional bodies such as 5G-PPP, a public private partnership initiated by the European Commission involving operators, vendors, service providers and universities;
- Other standardisation or industry bodies such as oneM2M, IEEE, IETF;
- Manufacturers;
- Regulatory bodies.

All of these bodies are likely to have an input into the eventual technical definition of 5G standards.

2.3 SIMalliance findings about 5G

It is clear that irrespective of how 5G develops, security will continue to be a major requirement. SIMalliance recognises that the changes involved in 5G will present different but at least as great security challenges compared to those present today. Many aspects of 5G have the potential of broadening the range of attractive attack targets identifiable by potential threat actors.

As a result SIMalliance has formed a Working Group to analyse the security requirements of each of the 5G segments identified above with the intention of then making market appropriate recommendations of relevant solutions. This paper lays out the findings of the SIMalliance to date.

③ <https://gsmaintelligence.com/research/?file=141208-5g.pdf&download>

3. Potential security requirements in 5G

Security implies three main qualities – confidentiality, integrity and availability. The 5G building blocks as described by 3GPP today imply complex security requirements across these qualities that have to be addressed on different layers within the system.

It is important to avoid confusing network level access with the data security requirements of the service level, as each level will have different security requirements.

That means that following high level types of security requirements can be distinguished:

- Network access security;
- Network application security;
- Service layer security;
- Authenticity, integrity and confidentiality of data transmitted at different network layers.

Just as 5G will bring new services, new capabilities, new technologies and new regulatory requirements, it will also bring new types of security threats and an increased attack surface. More and different actors and device types with different security postures will become involved, requiring superior attack resistance to new types of threat. The use of cloud and virtualisation may become more prevalent. Trust models will change.

That means that security methods currently applied to 4G and below will most likely have to be extended both to meet the performance and power efficiency requirements and lifespan of 5G and to match and exceed the high levels of trust and security previous generations of telecommunications technologies have enjoyed.

It deserves to be mentioned that prerequisites not only cover required precautions on the device side, but also need to consider the end-to-end aspects of related identity and credential management processes over the lifespan of the devices and services. In the light of an expected exponential increase in types of devices from all sorts of industries, this end-to-end scope

must provide a maximum of interoperability and scalability under affordable conditions.

Clearly security requirements will vary greatly by service because service specific technologies will themselves vary in terms of complexity and speed, from simple sensors requiring daily polling to surgery being carried out remotely requiring extreme real-time communications.

As a result SIMalliance sees a range of potential security requirements in 5G, including:

- Identifying the device, user, network, application, service and service platform;
- Faster handling of security procedures for use cases that require extremely low latency;
- Data authenticity, confidentiality and integrity for low complexity, low throughput services and sensors;
- Maintaining customer identity, location and privacy;
- Seamless authentication across multi access networks or shared infrastructure, avoiding decryption and re-encryption at intermediate nodes;
- Data verifiability.

These requirements can be met by measures such as:

- Identity and credentials provisioning and management;
- Integrity protection and secure storage of user data;
- Compliance monitoring;
- Security assurance;
- Management of and the ability to update security mechanisms.

However examining each segment in greater depth will highlight where these requirements are relevant as will considering potential technical solutions.

3.1 Network operations

Underlying and horizontal to each 5G market segment is the operation of the 5G network. There will be a number of significant ecosystem differences, compared to 3G and 4G. For example 5G technology is expected to be built around a “network of networks” concept and real-time handover between the network technologies involved will be key to success. 50 Mbps access is likely to be a requirement and the network will need to be optimised for data rate, latency, power efficiency and connection numbers. Network slicing and virtualisation are required to meet these needs. In addition network operations covers access to licensed and unlicensed, public or private networks. All these scenarios as well as the new features require security mechanisms

that ensure authenticated access to the network both for regulatory reasons and for liability. They are applicable for all services utilising the 5G network.

New features and scenarios will also lead to new security threats as detailed in the previous section, with MNO profiles (representing the credentials to access the network) being the main data to protect. With reduced MNO control over many areas of operations, security certifications will become important. There may also be a need to increase authentication key length to maintain robustness for the next 15-20 years in the face of threats arising from the potential development of quantum computing.

3.2 Examples of use cases and their diverse security needs

3.2.1 Massive IoT

The Massive IoT segment is extremely broad, covering not just M2M but consumer based services too. It is likely to consist of an ecosystem of potentially very low cost devices such as sensors or trackers. Projections suggest that there may be as many as 20.8 billion connected devices by 2020^④. Market participants will come from historical cellular network and device manufacturers but potentially also from new entrants from the IT industry.

Data is likely to encompass geolocation data, sensor data such as meter readings and private consumer data. Location and privacy protection for data must be enforced to ensure for example in the case of a meter that a thief cannot determine if the premises are occupied are not.

Communications will be either:

- Long range, low power, low bandwidth and infrequent; or
- Focused on speed.

Devices may be connected to the network either directly or indirectly, for example via a gateway. How this is done may have implications for security requirements.

Typical use cases are highly varied and may include drones, driverless cars, home appliances, some wearables and machine type communications including metering, sensors and alarms.

Security requirements in this segment will be based around devices, the network and backend. Appropriate certification and qualification will therefore be an important prerequisite in many use cases for those providing such devices – for example Germany^⑤ already requires smart meter certification. They will include secure authentication to network resources and security, integrity and confidentiality of network data.

In use cases such as smart metering the data transferred needs to be protected against manipulation, as, compared to voice communications, data can be more easily attacked and modified. Because the value comes from the integrity of the data, integrity protection becomes more important for 5G IoT. In particular mechanisms previously developed in 3G and 4G to primarily protect voice need to be enhanced.

The service layer security necessary has to be based on the nature of the service rather than the constraints of the device. However at this point, some of the newer entrants to the sector seem to be unaware of the need for anything more than negligible security, irrespective of the service. This has led to a rash of headlines and critiques about security breaches^⑥.

Because these devices are connected to the network, if they lack adequate security they offer the possibility of being used as an entry point to the network for attackers, who may have little interest in the device or service itself except as an entry point.

④ <http://www.gartner.com/newsroom/id/3165317>

⑤ <https://www.openlimit.com/en/products/smart-meter-gateway.html>

⑥ <http://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things>

3.2.1 Massive IoT (cont.)

Managing initial network connectivity securely will require secure provisioning of unique device and user identities for both network and service level access, network and service authentication credentials and communication cryptographic keys as well as application identifiers. The content of the securely provisioned data will likely depend on the device's location as well as agreements between integrators, service providers and mobile network operators.

Managing identities on the network will require identification of the application and corresponding application provider. It will also need secure storage of the unique identity on the device.

Mutual authentication of the device and network will also be necessary (it has been mandatory since 3G) as may mutual authentication for applications back to their service platforms.

There is also a risk of equipment cloning, leading to potential massive attacks to overload the network leading to denial of services. Carefully managing the identity of the device and securing the authentication to the network is therefore key to ensuring a good network quality of service.

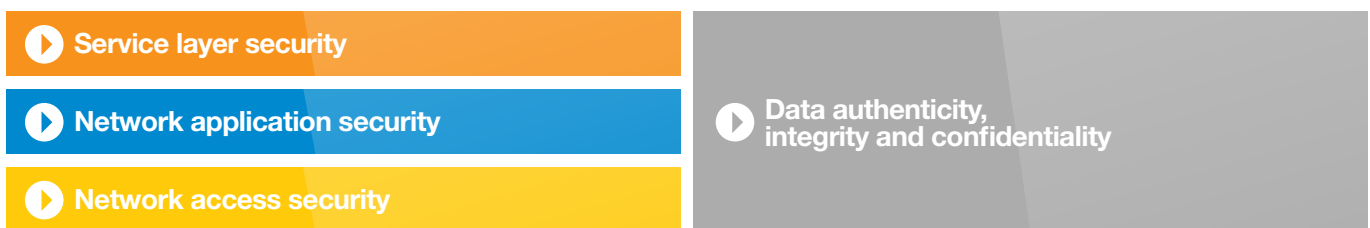


Figure 2 – high level security requirements in 5G

3.2.2 Critical communications

5G networks are likely to play an even more fundamental role in critical infrastructure than did previous generations. They will participate in what will be a highly complex ecosystem, involving drones and air traffic control, cloud driven virtual reality, smart multi node factories, cloud driven robots, public safety, transportation and e-health. Major players will come from public service providers, MNOs, device manufacturers, infrastructure providers and chipset providers.

This segment will provide different security requirements at the access and service layers – identification, enrolment, message authentication and non-repudiation, data integrity and key and identity management. Several layers of security may be required, depending on the use case and the type of communication (device to device or device to network) and the result may be a diverse and complex security infrastructure.

Different services will also require different levels of security and security assurance, with e-health and autonomous vehicles for example falling into market sectors with compliance requirements.

Breaches or man-in-the-middle attacks in use cases such as drone deliveries, connected vehicles, remote surgery, public safety and first-response networks would be detrimental to the image of any company or public body deploying such technologies and therefore security must be treated as paramount in the above area. Appropriate certification and qualification will therefore once again be important in many of these use cases.

Managing network connectivity securely will require a tamper-resistant hardware element and associated servers to initially securely provision credentials. Privacy management, group management and user and device authentication will be needed to manage identities on the network. There may be several layers of encapsulated authentication required at both network access and service levels and authentication may be required much more frequently than in segments such as IoT.

Data is likely to include geolocation data, instructions to elements in cloud based interactions and medical, operational and situational data. Some of this data will be highly sensitive and will be communicated more frequently than in segments like IoT.

3.2.3 Enhanced mobile broadband

This 5G segment encompasses the use of tablets, mobile phones and other portable devices. It offers a range of very diverse scenarios, with indoor and outdoor use, fast moving versus slow moving devices, use on trains and planes, hotspots such as offices, crowds and high density areas, low density areas and varying levels of network capacity requirement, depending on time and other factors.

Ecosystem players are likely to be similar to those of today – device manufacturers, chipset providers, cellular infrastructure providers, networks, service providers and consumers. However new players may become involved in the role of MNOs.

Security requirements in this sector will come from protecting access to the network and to services, protecting data and guaranteeing privacy at network and service level.

Breaches may occur at both a service level (e.g. gaining a user’s account credentials to log in to a service) or at a network access level, were identities and credentials to be compromised if stored outside a tamper-resistant hardware element.

However there is a risk that performance and throughput requirements may be met at the cost of security, particularly since the major requirements for managing connectivity are convenient and instant access to high bandwidth services.

Identities and credentials will be shared amongst multiple devices and services can either have many unique or shared sets of identities/credentials. Credentials must therefore be protected both while at rest and in transit. Device and user identities may need to be separated, particularly as MNOs are likely to remain keen to maintain control of user identity within the system. The security requirements of each service will depend on the use case and the business model but strong authentication is required for high value services, incorporating user, device and network elements. It is also likely that the arrival of enhanced mobile broadband will fuel the pressure to move away from usernames and passwords as authentication mechanisms. Mutual authentication to the network will continue to be mandatory.

There may be a need for new security solutions for key exchange or derivation protocols upon handover or when interworking with other Radio Access Technologies (RATs). Data will vary but is likely to be user data, usage data and geolocation data.

Smart appliances	First responder networks	Wearable devices
<p>▼ Threat</p> <p>Used as network access point by hackers, equipment cloning</p>	<p>▼ Threat</p> <p>Man in the middle attacks</p>	<p>▼ Threat</p> <p>Theft of account credentials</p>
<p>▼ Mitigation</p> <p>Secure provisioning of device identifiers, authentication credentials and cryptographic keys</p> <p>Mutual authentication of device and network</p> <p>Secure on-device storage</p>	<p>▼ Mitigation</p> <p>Secure provisioning of credentials</p> <p>Layers of encapsulated authentication</p> <p>Frequent authentication of users for network access</p> <p>Certification and qualification</p>	<p>▼ Mitigation</p> <p>Separation of device and user identities</p> <p>Strong, mutual authentication</p> <p>Move away from usernames and passwords</p>

Figure 3 – Sample use cases, threats and mitigations in 5G

4. A hardware based approach to meeting the 5G security challenge

4.1 Segment summary

	Massive IOT	Critical Communications	Enhanced Mobile Broadband
Required security/privacy level	Medium	Highest	High
User/device Identification	Yes	Yes	Yes
User/device Authentication	Yes	Yes - Biometric	Yes - Biometric?
Network Identification	Yes	Yes	Yes
Network Authentication	Strong	Strongest / Fastest	Stronger / Fast
Network Encryption	Strong	Strongest / Fastest	Stronger / Fast
Service Identification	Yes	Yes	Yes
Service Mutual Authentication	Strong	Strongest / Fastest	Stronger / Fast
Service Encryption	Strong	Strongest / Fastest	Stronger / Fast
Service Provisioning	Yes	Yes	Yes
Data integrity protection	Strongest	Strongest	Stronger / Fast
Shared credentials between groups of devices possible?	Yes	No	Yes
Feature set	Basic	Limited to a given use case and fast as possible	Rich to encompass all possible device-based / service authentication use cases

Figure 4 – 5G Segment summary

As we've seen from the previous chapter, each 5G segment poses different security and operational challenges. Needs will differ around frequency of communication, speed and latency and around frequency of authentication.

However a dedicated hardware entity, along with its associated processes, data generation, management and ecosystem, can play a positive role in each segment in managing device security, network and service access.

4.2 A potential solution

In massive IoT, a hardware based approach offers the following advantages – it is a proven secure platform that provides the best protection from physical tampering and device cloning. As a packaged application platform it can offer end to end management and a standardised life cycle management system for subscription, keys and credentials. However its features will need to be carefully selected to meet the demands of different segments. Scaled down or smaller with low power consumption, able to operate at a wide temperature range and to provide a wide range of physical interfaces, will be the optimal type of hardware solution for massive IoT. Logistics may also need to be taken into consideration, with devices offering easy integration into device manufacturer production lines being favoured.

In critical communications, the requirement for high security to protect critical data will vindicate the use of hardware-based security technology. Potential solutions will meet the need for fast computation, for example for encryption of data, and low latency.

The hardware approach is likely to have many benefits in enhanced mobile broadband, including proven and certifiable security levels, already clarified ownership and responsibilities, interoperability and established and trusted processes. However solutions optimised for power consumption and management, for avoiding performance bottlenecks and for integration with application security mechanisms will be most appropriate. Their value may need to be demonstrated to new players in the segment.

In network operations the hardware approach will provide the flexibility of an e-distribution model with the security of dedicated hardware. Compared to alternative software or TEE and TPM-based approaches, the tamper-resistant hardware element builds on the success and benefits of the existing trust model. It creates multiple opportunities for customisation and innovation. However 5G does present liability issues not present in 3G and 4G, which will need to be contractually clarified.

We can see therefore some patterns emerging. There is a clear need for hardware security for many 5G use cases in order to protect data, securely store it, encrypt it, exchange it securely with the network and authenticate the device.

In some use cases low power SEs could meet needs. In others, appropriate solutions will meet needs for very high computation power and speed and very low latency. Some may not require Java, OTA provisioning or SIM Toolkit or indeed ISO compliance, reducing the number of features. Industry and MNO business practices may need to change to aid the integration of embedded SEs into devices and to clarify questions around ownership and liability.

5. Conclusion and next steps

This paper has examined, at a high level, how security threats associated with specific market segments for 5G point to a role for a dedicated tamper resistant hardware module. Each segment and sub-segment has different business, technical and security requirements and may necessitate different solutions.

Today the tamper-resistant hardware element provides:

- Trusted identity for devices and people;
- A security mechanism that can prove that identity;
- A logistical mechanism to distribute the trust identity;
- Interoperability and scalability;
- Security as a service.

However it seems that there will be a general trend in 5G towards requiring low power and low latency, meaning that the hardware element industry will offer a broad product portfolio to meet these needs. For some use cases, although not all, future hardware elements will provide faster communication interfaces, processing power and more memory.

On the other hand there is a significant risk of falling too short, if we only look to the security and privacy challenges on the device side. A compelling concept for 5G must provide a solid proposition for the end-to end perspective that copes with the mission-critical aspects of interoperability and with scalability challenges.

Much is yet to be determined. For example, the question of the need for backward compatibility with earlier generations of network, if required, may complicate added functionality and capabilities.

Nonetheless it is vital to build security into 5G from the outset, for what is not built in from the beginning cannot easily be added later on.

The tamper-resistant hardware element industry can bring a great deal to 5G, including its neutrality, the trust it has created in different ecosystems, as well as the security, interoperability, diversity and modularity of the hardware element.

SIMalliance invites you to engage with us and help us to fine tune our vision of the role hardware based device security will play in protecting 5G networks and the many new services which will be deployed across the various market segments.

For more information visit

→ www.simalliance.org