Deliverable D5.4
First Market Analysis & Exploitation Report

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	15 November 2016	
Dissemination Level:	Public	
Lead beneficiary	ALBLF[1]	Linas Maknavicius <linas.maknavicius@nokia-bell-labs.com>
Authors	NOKIA: Linas Maknavicius TIIT: Luciana Costa, Madalina Baltatu Trust-IT: Stephanie Parker, Roberto Cascella	

[1] NOKIA Bell Labs since Jan 14, 2016

Executive summary

5G-ENSURE project drives the 5G security vision and its enablement through security and resilience enablers needed to build the necessary trust and confidence in 5G networks. To this extent, it is important to identify the different implications on potential revenue streams of 5G security components and services, as well as for profitability across the value chain and related business models.

The present version of the deliverable D5.4 introduces a first market analysis, impact scenarios, regulatory landscape and some preliminary insights into market opportunities and Business Models for 5G-ENSURE enablers. It will be complemented by the subsequent extended versions, some of them being confidential since containing sensitive information provided by the partners.

Foreword

5G-ENSURE belongs to the first group of EU-funded projects which collaboratively develop 5G under the umbrella of the 5G Infrastructure Public Private Partnership (5G-PPP) in the Horizon 2020 Programme. The overall goal of 5G-ENSURE is to deliver strategic impact across technology and business enablement, standardisation and vision for a secure, resilient and viable 5G network. The project covers research & innovation - from technical solutions (5G security architecture and test bed with 5G security enablers) to market validation and stakeholders engagement - spanning various application domains.

Disclaimer

The information in this document is provided 'as is', and no guarantee or warranty is given that the information is fit for any particular purpose.

The EC flag in this deliverable is owned by the European Commission and the 5G PPP logo is owned by the 5G PPP initiative. The use of the flag and the 5G PPP logo reflects that 5G-ENSURE receives funding from the European Commission, integrated in its 5G PPP initiative. Apart from this, the European Commission or the 5G PPP initiative have no responsibility for the content.

Copyright notice

Contents

1 Introduction

The European Commission's strategy for the Digital Single Market (DSM strategy) [20] and the Communication Connectivity for a Competitive Digital Single Market: Towards a European Gigabit Society [21] underline the importance of very high capacity networks like 5G as a key asset for Europe to compete in the global market place.

According to ABI Research, mobile broadband operators will reap 5G revenues of €227 billion in 2025 with North America, Asia-Pacific, and Western Europe being the top markets [22]. Another study suggests that the introduction of 5G across four key industries, automotive, health, transport and energy, could generate €114 billion/year [1].

Within this context, it is important to identify the different implications on potential revenue streams of 5G security services, as well as for profitability across the value chain and related business models.

The present version of deliverable D5.4 introduces a first market analysis and preliminary insights into the exploitation strategies for the 5G-ENSURE project's exploitable foreground. Therefore, the document first collects and assesses market situation, including partner industry studies and external sources, capturing trends in the marketplace, potential competitors, updates on regulations of direct interest and introduces a set of impact scenarios as part of the market analysis, SME concerns based on recent surveys, and socio-technical and economic opportunities.

Careful attention is given to evaluating the impact of regulations on the exploitation activity, and this is captured in the section dedicated to the exploration of the regulatory landscape.

Subsequently the document proposes an initial list of 5G-ENSURE exploitable results and proposes a template to be adopted in order for the partners to start investigating on the possible exploitation strategies for each identified project asset. The exploitation strategies include market-oriented exploitation, but also internal deployment and open source releases. Since the 5G network is still under definition special attention is given to standardization activities. As a consequence, the effort invested in the standardization of exploitable results is considered a keystone work towards the effective exploitation of the results produced by the 5G-ENSURE project.

Individual partner exploitation plans and exploitation plan of the consortium as-a-whole will be further elaborated in the subsequent versions of the deliverable, and in particular in its accompanying CONFIDENTIAL (extended) versions.

Finally, business models of the 5G-ENSURE results are sketched. This version proposes an example business model over a selected 5G security enabler.

2 Preliminary analysis of 5G market

2.1 Generic 5G market trends

2.1.1 Socio-economic impact of 5G in Europe

The large **EC supported study SMART 2014/0008** [1], released in October 2016, is forecasting the benefits, impacts and technical requirements to assist strategic planning for the introduction of 5G in Europe. It used a methodology including group workshops with over 80 experts from four main verticals (automotive, healthcare, transportation and energy). One of the goals of the study is to provide a basis for regulators, governments and public authorities and policy makers in planning future strategies such as spectrum allocation planning and future market regulation.

Main study findings are:

- In 28 EU Member States the total cost of 5G deployment could reach approximately €56 billion in 2020. Investment in 5G could achieve potential **annual benefit to the EU member states of €113.1 billion from 2025**, with 'trickle-down' benefits from 5G investment across the whole of the economy (multiplier effects) totalling as much as €141 billion.
- 63 per cent of these benefits will arise for business and 37 per cent will be provided for consumers and society.
- The deployment of 5G is expected to **create 2.39 million jobs** in the 28 countries.

While 5G benefits and capabilities are broad and varied, the study identified three main capabilities that will bring beneficial changes and development:

1. *50Mbit/s everywhere*: Truly ubiquitous coverage is expected to help overcome the "digital divide" caused by poor broadband coverage.
2. *Scalable solutions for sensor networks*: Support for large scale M2M/IoT networks is a priority for all verticals and environments, in particular the four key verticals covered by the study.
3. *Ultra-tactile Internet*: This has the potential to unlock new applications and services including real-time "sense-respond-actuation" cycles that enable human-device and device-device interactions.

The study identifies two main groupings of benefits across these key verticals – direct economic benefits attributed to each sector, and secondary socio-economic and environmental benefits arising from four "environments": Smart Cities, Non-Urban, Smart Homes and Workplace.

The first order economic benefits account for €62.5 billion of the identified total €113.1 billion benefits by 2025 and are distributed as follows:

- Automotive: €13.8 billion.
- Transport: €5.1 billion.
- Healthcare: €1.1 billion.
- Utilities: €775 million.

The second order benefits arising from the different environments total €50.6 billion. They are broken down as follows:

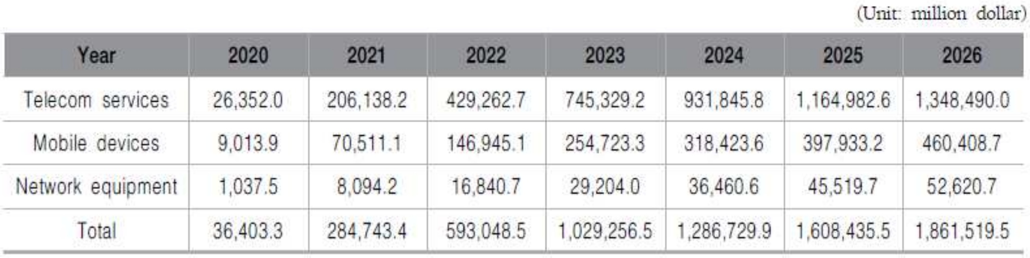
- Workplace: €30.6 billion.
- Non-Urban: €10.6 billion.
- Smart City: €8.1 billion.
- Smart Home: €1.3 billion.

In further findings from the report, 63% of the total €113.1 billion benefits will arise for business and 37% will be provided for both consumers and society.

2.1.2 Global 5G mobile devices/network equipment/telecom service sizing

5G network & services market size

It is expected that 5G network will be commercialized in 2020, and then replace the legacy network and services step by step. The market size of the global 5G services will post a high growth rate with a CAGR of 92.7% (from USD 36.4 billion in 2020 to USD 1,861.5 billion in 2026).



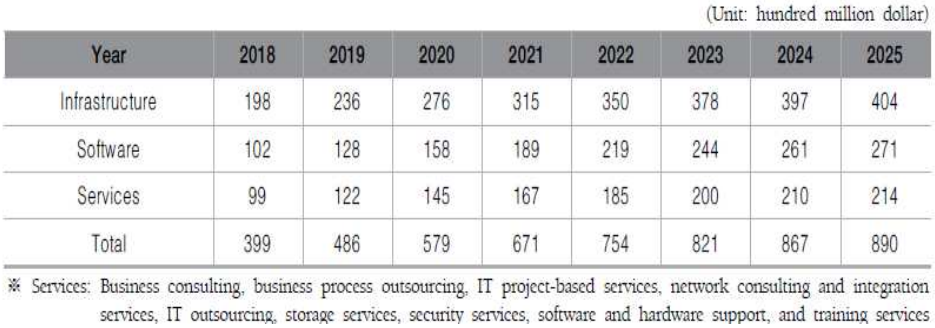
(Unit: million dollar)

Year	2020	2021	2022	2023	2024	2025	2026
Telecom services	26,352.0	206,138.2	429,262.7	745,329.2	931,845.8	1,164,982.6	1,348,490.0
Mobile devices	9,013.9	70,511.1	146,945.1	254,723.3	318,423.6	397,933.2	460,408.7
Network equipment	1,037.5	8,094.2	16,840.7	29,204.0	36,460.6	45,519.7	52,620.7
Total	36,403.3	284,743.4	593,048.5	1,029,256.5	1,286,729.9	1,608,435.5	1,861,519.5

Table: Forecast of the global 5G market (Source: ETRI [2])

Intelligent 5G services

IDC forecasts that the next generation platform (mobile, social, cloud, big data), which is the next-generation IT environment, will account for 1/3 of the entire world's ICT investment. First, the big data market will grow continuously, since global IT companies are currently making a lot of efforts to take initiative in big data market. Especially in 5G, various types of information including data generated from machines as well as humans are expected to be effectively and systematically collected and processed, and finally used for creating new business values. Accordingly, the global market of big data is expected to grow from USD40 billion in 2018, to USD89 billion in 2025.

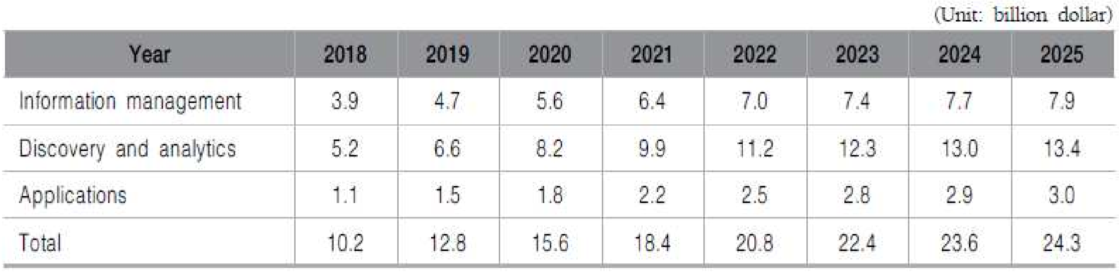


(Unit: hundred million dollar)

Year	2018	2019	2020	2021	2022	2023	2024	2025
Infrastructure	198	236	276	315	350	378	397	404
Software	102	128	158	189	219	244	261	271
Services	99	122	145	167	185	200	210	214
Total	399	486	579	671	754	821	867	890

※ Services: Business consulting, business process outsourcing, IT project-based services, network consulting and integration services, IT outsourcing, storage services, security services, software and hardware support, and training services

Table: Forecast of global big data market (Source: ETRI / IDC [3])



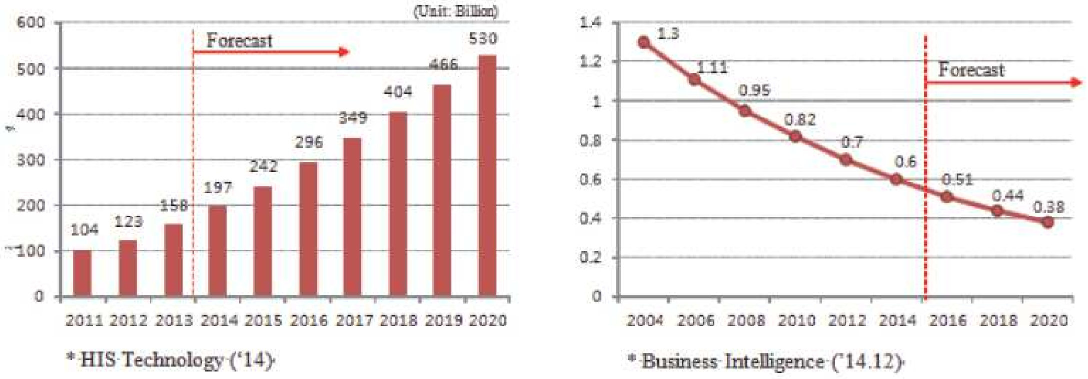
(Unit: billion dollar)

Year	2018	2019	2020	2021	2022	2023	2024	2025
Information management	3.9	4.7	5.6	6.4	7.0	7.4	7.7	7.9
Discovery and analytics	5.2	6.6	8.2	9.9	11.2	12.3	13.0	13.4
Applications	1.1	1.5	1.8	2.2	2.5	2.8	2.9	3.0
Total	10.2	12.8	15.6	18.4	20.8	22.4	23.6	24.3

Table: Forecast of the global big data software (Source: ETRI / IDC [3])

Omnipresent 5G services

Currently, the hyper-connected innovation based on IoT (Internet of Things) is under way all over the world, aiming at connecting everything to Internet. Putting together the forecast of major companies such as Cisco, Ericsson and Gartner [4], the ratio of things connected to network as of now is estimated to be less than 1% of the connected things in the future. As the price of sensors becomes cheaper and number of things connected to Internet increases, the value and utility through disruptive innovation in various fields of society is expected to take place. In particular, this innovation based on IoT will significantly improve the productivity and efficiency of the legacy industries, create new business through big data and efficient data processing, and solve various social issues, leading to much better quality of life.



* HIS Technology ('14)

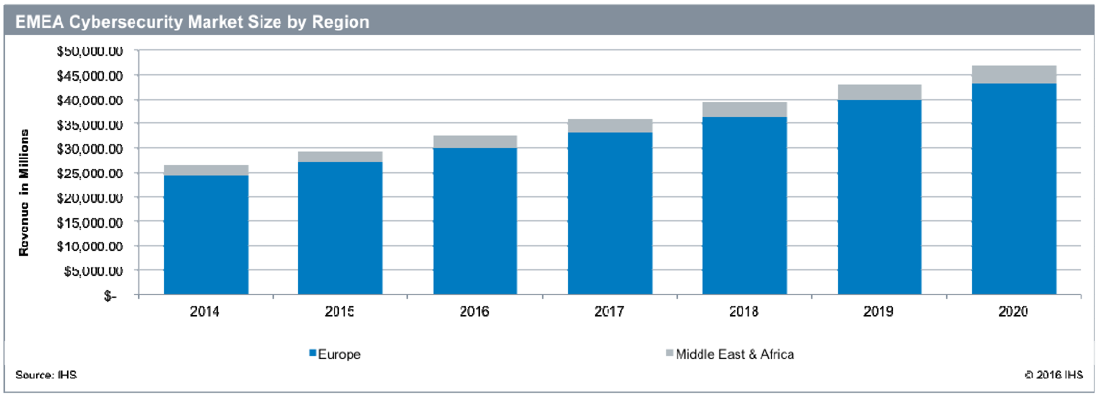
* Business Intelligence ('14.12)

Figure: Increase of devices connected to Internet and fall of unit cost of sensors [4]

2.2 5G security market orientations

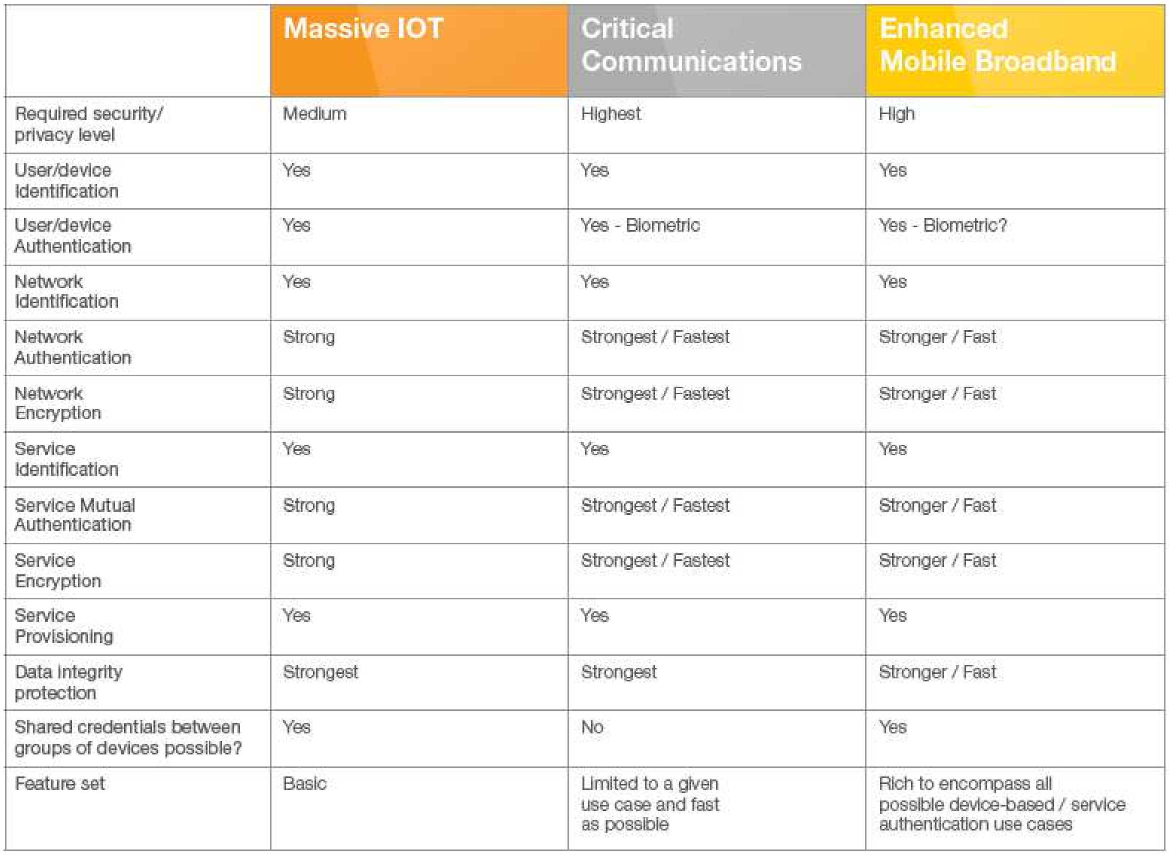
2.2.1 Cybersecurity product market prediction

The cybersecurity product market in Europe, Middle East and Africa (EMEA) is expected to grow at a compound annual growth rate (CAGR) of 7.2 percent, from $11.2 billion in 2015 to $15.9 billion in 2020. With the adoption of the new General Data Protection Regulation (GDPR) in the European Union revenue from encryption products is expected to grow most quickly, at a CAGR of 8.8 percent from 2015 to 2020, according to the IHS Cybersecurity Report [5]. This covers global and regional markets for cybersecurity hardware, software and services.



2.2.2 Hardware based approach to meeting the 5G security challenges

SIMalliance analyzed the main potential market segments where 5G will have a transformational impact and assessed the diverse security requirements for those markets [6]. Four main segments for 5G have been defined: Massive IoT, Critical Communications, Enhanced Mobile Broadband and Network Operations. Across these segments, security requirements 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.



	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

Table: 5G security and operational challenges (Source: SIMalliance [6])

SIMalliance suggests that a dedicated hardware entity, along with its associated processes, data generation, management and ecosystem, can play a positive role in managing device, network and service access security, in particular [6]:

- *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. 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.
- *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.
- *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.

Therefore, SIMalliance affirms that 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.

2.2.3 Security and privacy issues in different market segments

Security and privacy are cornerstones for 5G to become a platform for the networked society, driving new requirements due to new business and trust models, new service delivery models, an evolved threat landscape and an increased concern for privacy. Security and privacy are transversal across the new verticals that are expected to benefit from 5G.

Here we analyse reports covering security and privacy concerns across such verticals that may impede or slow down innovation and investment. Reports include SMART 2014/0008 [1], “Opportunities in 5G” [7], the “Connected Car Report 2016” [8] and GSMA Intelligence/CAICT report on mobile operators [9].

The table below shows key findings from such reports, including references to the regulatory environment.

Vertical	Security and privacy issues that could off-set expected benefits and business value
Automotive	Potentially huge market for ICT and 5G-enabled advances. However, innovation comes from a good understanding of data privacy issues, which are key to user trust, as well as effective frameworks fostering the integration of systems and business propositions. New definitions of data privacy may also need to take into account interpretations of future generation users/drivers [1]. The business value of 5G comes mainly from increased performance (low latency for quick reaction times for autonomous and semi-autonomous vehicles), increased security, and device-to-device communications. Security is imperative to keep malicious hackers from creating dangerous situations on the road [7]. Connected cars are vulnerable in part because they are complex machines made up of many different digital systems, any of which might be a weak link. Built through a combined effort, no single company has been responsible for securing them, and much of the current lack of security can be traced to the organisational difficulty of orchestrating the complex effort of making these cars. Future cyber attacks could affect more than one car at a time, disrupting traffic flow or targeting an entire fleet of cars. Other risks include the theft of increasing amounts of personal data flowing between the car and the cloud through car-based consumer apps and services. Hackers could also use the car to access IT systems of the car's OEM and/or suppliers. Theft of software code could be used for new functions offered free to users (disturbing the business case). Consumer awareness is growing and could lead to mistrust [8].
Transport	Transport data sharing and access is fundamental to fully realise the benefits of 5G in this sector. Benefits and economic gains will only be fully realised with friendly government policy and a highly motivated industry [1].
Healthcare	5G can be a change agent for services such as remote diagnosis and medical care, virtual reality for medical training. However, the pervasive use of remote systems to sense and actuate technologies increases the need for cyber security. Furthermore, to realise the full potential, this vertical will require a very supportive regulatory framework and common standards for recording, sharing, transferring and anonymising health-related data. From a regulatory perspective, different policies need to underpin developments in healthcare, ranging from issues like transparency, data ownership, privacy, data exchange, permissions around offering services, and liability issues [1]. Implementing new services and improving the quality of life for the general public are important drivers for 5G implementations. However, security is just as important as performance in terms of real business value [7].
Utilities	Future generation networks will enable very fast and reliable distribution and consumption of energy and water, leveraging spare capacity to meet impacts of population growth, urbanisation and change of life style. To promote investment

	and competition, this vertical will require strong support from governments and a stable regulatory environment based on EU-driven regulation and policies. It will also require trust in connectivity [1]. Reducing costs and increasing security are dominant concerns in the utilities sector. Given the regulatory environment and tight margins within which the utilities operate, increased productivity, faster time to market and boosted efficiency are key business drivers for incorporating 5G. Increased security is required to protect valuable assets from attacks.
Public safety	This vertical can benefit from 5G and the IoT to increase public safety while gaining cost efficiencies. Improving citizen experience, increasing productivity and faster time to market are key business drivers. Investments currently planned focus on creating value citizens and operational efficiency. Real business value is considered to come from increased performance, increased security and device-to-device communication, which are all important in an emergency situation. Increased performance is imperative for timely message transmission, while increased security will help reduce the risk of hackers slowing down reaction time of first responders [7].
High-tech manufacturing	To reduce the threat of disruption and new entrants, high-tech manufacturers can use 5G technologies to increase productivity, improve customer experience and accelerate time to market. Key concerns are risk and the security of manufacturing assets, with the need to expand video surveillance/streaming of manufacturing assets, develop better machine-to-machine sensors and improve remote site security [7].
Internet/Digital native companies	The financial implications of cyber-attacks are significant. At a global level, the impact is estimated to be around $445 billion per year or 0.6% of GDP [9]. Operators are undertaking a range of security enhancements, particularly in areas such as enterprise platform scanning and advanced networks. The nature of the threats has become more complex, agile and diffuse, making it more difficult to respond or pre-empt. PC-era hacking techniques such as Trojans and viruses are now being iterated on to spawn new variations (chargeware, for example). Recent denial of-service attacks have targeted enterprise and government, with motivations ranging from customer fraud to industrial and state espionage. Exacerbating all of this, bring your own device (BYOD) and a lack of rigorous security protection systems with patch updates for third-party apps have combined to increase the vulnerability of individual enterprises. NTT Group estimates that it takes an average of 200 days for organisations without a vulnerability management system in place to remedy vulnerabilities [9].
Financial services	Threat and attack levels generally rise in proportion with the economic value of the sector. Financial services are the most vulnerable, they account for around 20% of detected cyber-attacks on SMEs and enterprises (18000 clients) [9].

	This sector can benefit from 5G to boost real-time mobile trading and high frequency trading. Business efficiency, increased productivity and enhanced customer experience are the main business drivers. Security is a top priority, where 5G could power more secure transactions. Secure cloud-based services are the top priority for financial services companies, with secure, remote sessions with financial advisors also being important [7].

2.2.4 Security and privacy issues in smart environments

In the SMART 2014/0008 report, examples of smart environments include cities and non-urban environments, as well as micro-scale homes and workplaces, clearly with some overlap with verticals [1]. Other reports provide data on public safety [7].

- *Smart cities:* 468 cities in the EU with a population over 100,000. The level of digitisation is above 75% and expected to reach 80% by 2020. Expected general benefits of 5G include enhanced communications and information access for policymakers, citizens, businesses and other inhabitants. One major benefit is enhanced social capital, such as using enhanced wireless communications to improve transport and reduce congestion, with potential to lower hydro carbon consumption, emissions and CO2.
- *Non-urban environments:* Over 77% of the EU's territory is classified as being rural (47% farmland; 30% forest), and has historically lagged behind its urban and suburban counterparts in terms of access to and exploitation of cutting-edge broadband access and digital technologies. Major benefits expected from 5G are: sustainable capEX spending and ICT-dependent industry, including agriculture as a more sustainable business. Shared networks are a key environmental benefit that could reduce costs and increase the economic feasibility of the network.
- *Smart homes:* 214 million households in the EU. By 2020, most of the connected smart homes could have more than 200 radio equipment devices. Key benefits of 5G include reduced energy spending and time saving. From an environmental perspective, smart homes can reduce energy consumption and CO2 emissions, as well as reduce waste, while better and informed electronic waste could be negative (e.g. increased wastage).
- Smart workplace: 25.6 million active businesses in the EU, employing 141 million people. The most connected SMEs could have more than 750 radio equipment devices (1 device/1.5sq.m). More integrated information is expected to have the greatest impact as one of 5G's greatest values could be the sharing of massive amounts of information sharing.

A larger scale infrastructure supporting the easy movement and sharing of massive amounts of information could be the greatest value of 5G. However, this value proposition requires that 5G and related technology innovation provides security and privacy solutions to make the data anonymous. Without this, the large economic potential of integrating behavioural information into the operation of transport systems, utility systems and even telecom systems will not be realised.

A summary of key findings is presented in the table below.

Smart cities	Better information for administrators: enhanced wireless communications (with reduced costs and/or more reliable connectivity) has potential for growth in the development of information platforms for enhanced big data analytics. Barriers due to trust and privacy concerns will increase in the future [1].
Public safety	5G and IoT are expected to improve citizen experience, increase productivity, and achieve faster time to market for new products and services. Business value for executives are increased performance for rapid response and increased security are primary concerns. increased security is important to reduce risks of hackers slowing down reaction time of first responders [7].

2.2.5 The threat landscape

In early October 2016, **ENISA** published its **Annual Incidents** report, providing an overview of the root causes of incidents and an aggregated level of which services and network assets are impacted [10]. The report is based on data sent by the Telecom Regulators under Article 13a of the Framework Directive (2009/140/EC) to ENISA and the European Commission. Main findings are:

- *Number of incident reported:* 138 major incidents from 21 EU countries and 2 ETFA members. 9 countries reported no significant incidents.
- *Most affected services:* Mobile internet represented 44% of reported incidents, followed by mobile telephony.
- *Most dominant root cause of incidents:* 70% of incidents are caused by system failure or technical failures, continuing the trend in recent years. In the system failures category, software bugs and hardware failures are the most common cause affecting switches and routers and mobile base stations.
- *Cause of errors:* Human errors affected on average more user connections per incident. Human errors were the root cause category involving most users affected, accounting for almost 2.6 million user connections on average per incident. System failures was the second highest cause, with 2.4 million user connections on average per incident.
- *Objectives of malicious attacks:* Malicious actions are not focused on causing disruptions: the total number of incidents caused by malicious actions fell from 9.6% to 2.5% in 2014. This figure suggests that malicious actions may have other objectives than causing the unavailability of services. However, DDoS incidents had the most impact in terms of duration (on average 2 days per incident).
- *New services affected:* TV broadcasting/Cable TV Networks (14%), SMS/MMS (13%), public email (5%), IPTV (4.4%), VOIP (3.7%).

The patterns are important for risk and vulnerability assessments. At the policy level, incident patterns can shape strategic measures to improve security in the sector.

Impact of incidents

Most reported incidents usually have an impact on more than one service in the same incident. For example, a faulty hardware change/update caused fixed internet and mobile internet to fail for millions of users (duration: hours, connections: millions, cause: human error). A misconfigured router hardware replacement performed incorrectly affecting mobile data capacity approximately 60-70%. Although both fixed internet and mobile internet user connections were affected, mobile internet user connections affected were four times more. Incident was resolved by configuring the new equipment correctly, however it took a few hours to recover connectivity.

With regard to national user base affected, mobile Internet outages impacted on average 18%. For example, a faulty hardware change/update caused mobile internet to fail for more than an hour impacting a significant number of user connections (duration: hours, connections: millions, cause: system failure). Incidents may also impact on the ability to communicate with an emergency service (20% in 2015).

In the light of the report, ENISA has called for increased transparency and clarity on incidents as essential for risk management and improving the level of security. ENISA will continue to foster and support transparency on incident reporting, promoting a systematic approach towards improved security measures in the sector.

Threat Landscape and Good Practice for Software Defined Networks/5G

Another report from ENISA [11] aims to create awareness by identifying key valuable assets of the SDN infrastructure that are needed to ensure proper network function and interoperability. However, these assets may become the target of attacks and therefore become the main driver of a threat analysis aimed at securing SDNs. The main findings of the report are:

- SDN/5G brings a brand new level of innovation to networking with key attributes like logically centralised intelligence, programmability and network abstraction paving the way to the communications of tomorrow.
- While significant improvements may be achieved in network security by centralisation and programmability, but they will also attract a new level of threats and attacks.
- Security within the SDN paradigm will be challenging as all layers, sub-layers and components will need to communicate according to strict security policies.

The main technical recommendations are:

- Recommendation 1 (for Network providers): Mandate encryption and authentication in NBI, SBI and EWBI.
- Recommendation 2 (for Network providers): Identify and monitor exposed functionalities of SDN controllers.
- Recommendation 3 (for Network and Service providers): Control and monitor running application resources.
- Recommendation 4 (for Network, Service providers and End users): Holistic Support for Security policies.
- Recommendation 5 (for Administrators): Access control, Credentials, System updates
- Recommendation 6 (for Developers): Sandboxing, Application Isolation.

The main organisational recommendations are:

- Recommendation 7 (for Service providers): Develop incident response capabilities and information sharing practices among telecom operators.
- Recommendation 8 (for Administrators): Keep systems up to date.
- Recommendation 9 (for Network and Service providers): Use adequate security methods.

3 The new regulatory landscape

Art. 13a is part of the current Telecom Framework, a regulatory framework which is currently under review by the EU Commission, while a new draft is being expected by the end of the year 2016. As a consultative body for the EU Commission, ENISA sustains a more harmonised approach between the newly adopted NIS Directive and the upcoming regulation [12]. ENISA has an extensive expertise in the telecom sector, as activities in this area have been carried out for many years, which in the telecom area cover: incident reporting, security measures, threats and assets, power supply dependencies, national roaming for resilience, ICT procurement in the telecom sector, and mitigating cable cuts.

3.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) was formally approved by the EU Parliament on April 14, 2016 [13]. Being a regulation rather than a directive, it doesn't require enabling laws to be passed by member states. The GDPR will be enforced two years from the date of entry into force, i.e., approximately in early July 2018 and it will replace the data protection directive from 1995 [14].

The majority of the GDPR's core principles are much the same as those in the current Data Protection Directive. However, the GDPR covers a wide range of issues relating to personal data including privacy, monitoring and security.
Primary objectives of the GDPR are to give individuals back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

The approval of the GDPR is significant since it intends to strengthen and unify data protection for individuals within the European Union (EU) but unlike the current Directive that was implemented differently between member states, the regulation will be common across all states and will also applies to organizations based outside the EU if they process personal data of EU residents. The regulation does not apply to the processing of personal data for national security activities or law enforcement ("competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties").

The GDPR sets out a number of principles aimed at ensuring that data is gathered for legitimate purposes, that only data needed for those purposes is held, that the data is fairly and lawfully processed, and that it isn't held for longer than necessary.

The enforcement of GDPR will give a number of rights to individuals such as:

- right of information and data access: this enables individuals to demand access to all of the information stored by an organization, to discover how data were initially sourced and how long they will be kept,
- right to rectification of data: this enables individuals to request that any errors on information held on them be corrected
- right to data portability: this allows individuals to confirm that the data is correct, has been collected via consented methods, and to pass the information to another controller if they wish
- right to erasure: this allows individuals to request that data relating to them is erased on various grounds including withdrawal of consent and unlawful processing. This right can apply also in case

an individual believes that the data is no longer necessary in relation to the initial purpose of collection. Businesses must then ensure its removal from any databases to prevent future processing by either themselves or by partner data processors

Other relevant aspects of the Regulation are:

- The definition of 'personal data' has been widened to include any information that can be used to identify an individual, either by itself or in conjunction with other data. Previously, some countries had their own interpretation of what constituted personal data; now a consistent definition of personal data has been set out with the new regulation.
- The regulation's scope has been increased to include any organisation that collects (controller) or stores and processes (processor) data on EU individuals
- Data controllers and processors share joint liability for any data loss incidents: in the past, only data controllers (usually the organisations who gathered the data) were responsible for loss. Now, it is a joint responsibility with the data processor, (i.e. a cloud service provider or outsourcer of data), that process data on behalf of someone else and that includes data on EU individuals.
- Fines are increased to "up to 4% of global turnover": the consequences of breaching EU data protection law escalate dramatically under the GDPR, which sets the maximum fine for a single breach at the greater of €20 million, or four percent of annual worldwide turnover.

Finally, according to the GDPR, each country shall establish its own 'supervisory authority' which is responsible for enforcing the rulings, advising organisations on the requirements and administering fines where necessary. Supervisory authorities should work with the EU Data Protection Board in order to enforce the EU GDPR. This is a different approach of current directive where member states already have their individual regulators promoting and enforcing the current Directive, however, the interpretation has differed between countries. Some have enforced the current laws strongly, issuing relatively large fines and naming and shaming penalised organisations; while others have taken a more advisory role, placing a large emphasis on education and training. The differences in approach is a large reason for the variation in awareness and concern around data protection across the region.

3.2 NIS Directive ("Network and Information Security Directive") on security of network and information system

The Directive on Security of Network and Information Systems ('NIS Directive') [15] entered into force in August 2016 after the adoption of the European Parliament (6 July 2016). The goal of the NIS directive is to establish a baseline for network and data security by introducing a minimal set of rules aiming to ensure a common level of network and information security across the EU.

All the Member States have a 21 month period to implement the Directive into their national laws.

The NIS Directive refers to two different categories of market players:

- the Operators of critical infrastructures. According to NIS, they are "any entity that provides a service that is essential for the maintenance of critical societal and/or economic activities" so long as "the provision of that service depends on network and information systems" and for which "an incident to the network and information systems of that service would have significant disruptive effects on the provision of those services". The operators of essential services may be public or private entities operating within the sectors like energy, transport, banking, financial market infrastructure (trading venues, central counterparties), health, water, digital infrastructure (internet exchange points, domain name system service providers, top level domain name registries).

- the Digital Service Providers (DSP). According to NIS, DSPs are any provider of an online marketplace, online search engine or cloud computing service. DSP that are based outside the EU but provide services within the EU will fall under the scope of application of the NIS Directive. Micro and small enterprises are excluded from the scope.

According to NIS directive, operators of critical services and DSPs need to implement security measures appropriate to the risks posed to the security of network and information systems which they use for the provision of essential services (in the case of operators of critical services) or in the context of offering services within the Union (DSPS). These security measures shall include:

- technical and organisational measures to manage the risks posed to the security of network and information systems security
- appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used to provide the services with a view to ensuring the continuity of those services.

Given the fundamental differences between operators of essential services, (in particular their direct link with physical infrastructure) and digital service providers (in particular their cross-border nature) the Directive take a differentiated approach with respect to the level of harmonisation. According to the NIS Directive, "Digital service providers should ensure a level of security commensurate with the degree of risk posed to the security of the digital services they provide, given the importance of their services to the operations of other businesses within the Union". In practice, the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, is higher than for digital service providers. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems. Therefore the security requirements for DSPs should be lighter which need to report security incidents they experience where those incidents have "a substantial impact on the provision of a service they offer within the Union". In contrast, operators of essential services must report "incidents having a significant impact on the continuity of the essential services they provide".

The NIS Directive also requires the Member States to adopt their own cybersecurity/NSI strategies defining the strategic objectives and appropriate policy and regulatory measures and to designate national authorities (Computer Security Incident Response Teams (CSIRTs)) that are competent for monitoring the application of the NIS Directive at national level and to ensure cross–border cooperation with the relevant authorities in other Member States.

To support and facilitate strategic cooperation and the exchange of information among Member States, the NIS Directive also establishes a so-called Cooperation Group composed of representatives of Member States, the Commission and the European Union Agency for Network and Information Security (ENISA).

3.3 BEREC guidelines on the implementation by regulators of new net neutrality rule

The Body of European Regulators for Electronic Communications (BEREC) has published on 30 August 2016, the "Guidelines on the Implementation by National Regulator Authorities (NRAs) of European Net Neutrality Rules" [16].

In 2015, the European Union adopted the Regulation 2015/2120 commonly referred to as the 'Telecoms Single Market Regulation', concerning measures for safeguarding open internet access [17]. The Regulation laid down net neutrality rules in general terms, asking the National Regulatory Authorities (NRA) to ensure compliance and to impose the appropriate measures on providers of ISPs. In order to ensure a consistent implementation across member states, BEREC has been assigned by the Regulation to set up the now published Guidelines. As BEREC does not exercise any regulatory power itself, the Guidelines are not legally binding, neither for the NRAs nor directly for ISPs. However, the Guidelines will most likely have a decisive influence on the implementation of the Regulation across the EU.

The new net neutrality rules relate to:

- providers of internet access services. These are defined in (Art. 2 (2) of the regulation) as *"a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used."* For 'publicly available' the BEREC means (page 5, para. 10*)"Electronic communication services or networks that are offered not only to a predetermined group of end-users but in principle to any customer who wants to subscribe to the service or network should be considered to be publicly available. Electronic communication services or networks that are offered only to a predetermined group of end-users could be considered to be not publicly available."*
- so-called specialised services defined as "*services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality*". Specialised services include VoLTE and live IPTV broadcasting.

Outside the regulation's scope is activity on private networks, which includes Wi-Fi and corporate networks. In addition, interconnection between networks are not considered by BEREC as an internet access service; anyway BEREC considers interconnection practices relevant in so far as they "have the effect of limiting the exercise [of] end-user rights" in the case where interconnection is "implemented in a way which seeks to circumvent the Regulation" (page 4, para. 6).

The Regulation establishes the:

- right in relation to the *open internet for "end-users".* "End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service". The rights are available to both individual consumers and businesses using internet access services. The businesses enjoying this protection include content and application providers (CAPs) insofar as they use an internet access service to provide content or applications to other end-users. A CAP is a company which makes content (e.g. webpages, blogs, video) and / or applications (e.g. search engines, VoIP applications), and / or services available on the internet.

- *equal treatment of traffic*, in the sense that there can be no prioritisation traffic in the internet access service. Blocking, throttling (e.g., slow down lawful traffic) and discrimination of internet traffic by Internet Service Providers (ISPs) is not allowed, save for three exhaustive exceptions: traffic management to comply with a legal order, to ensure network integrity and security, and to manage congestion provided that equivalent categories of traffic are treated equally.
- *Implementation of reasonable traffic management measures* providing such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary
- *the condition for offering specialised services.* These are can be allowed only if there is sufficient network capacity to provide them in addition to any internet access service and if such a provision does not affect the availability or general quality of internet access services for end-users.
- the condition for zero-rating. Such practices should be “agnostic” and applicable to a generic categories of services, and not to a specific service. The use will be judged on a case by case basis to ensure the practice does not harm competition or choice.

The Regulation requires NRAs to "*closely monitor and ensure compliance*" with the new rules, and to "*promote the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology*". NRAs will provide their first annual report on implementing BEREC’s guidelines by June 2017.

4 Business model for 5G security enablers

"*A business model describes the rationale of how an organization creates, delivers, and captures value*". (Alex Osterwalder, http://alexosterwalder.com/).

Alex introduces "The Business Model Canvas" [18]. It's a one-page tool, in which we find the nine elements that constitute any business model.

4.1 Methodology

The methodology applies only for enablers which have been identified for commercialization

The 5G-ENSURE consortium has agreed to use the "Business Model Canvas" proposed in [18], a template that helps to clearly and simply define and develop the business model in all its categories. The canvas is illustrated in the Figure below and explained in the rest of this section.

According to the most common definition, a business model is the first step that has to be undertaken in order to be able to create a business able to create value, and, therefore, produce monetary revenue to its owners. In fact, the economists sustain that the success of an innovative product in the service market strictly depends on the quality of its Business Model (BM).

The creation of the business model implies the following steps:

- The identification of the value proposition and the unique sales proposition. This basically means responding to the question: which are the key factors able to attract and retain each revenue stream;
- The identification of the key factors that facilitate a profitable and consistent delivery of the value propositions, also called delivery or funding model;
- The identification of the capabilities, the relationships and the knowledge that result from the previous steps.

Several theories on effective business model identification are available in literature, but the general concept is that the creation of a business model starts by answering to questions that can be mapped to the following seven categories:

- Value proposition
- Customer segments
- Key activities
- Key resources
- Key partners
- Channels
- Customer relationships.

It is therefore evident that building successful business models means the formulation of a sustainable strategy for the new business. For this purpose different BMs have been identified for the 5G-ENSURE solutions and they will be presented in the following.

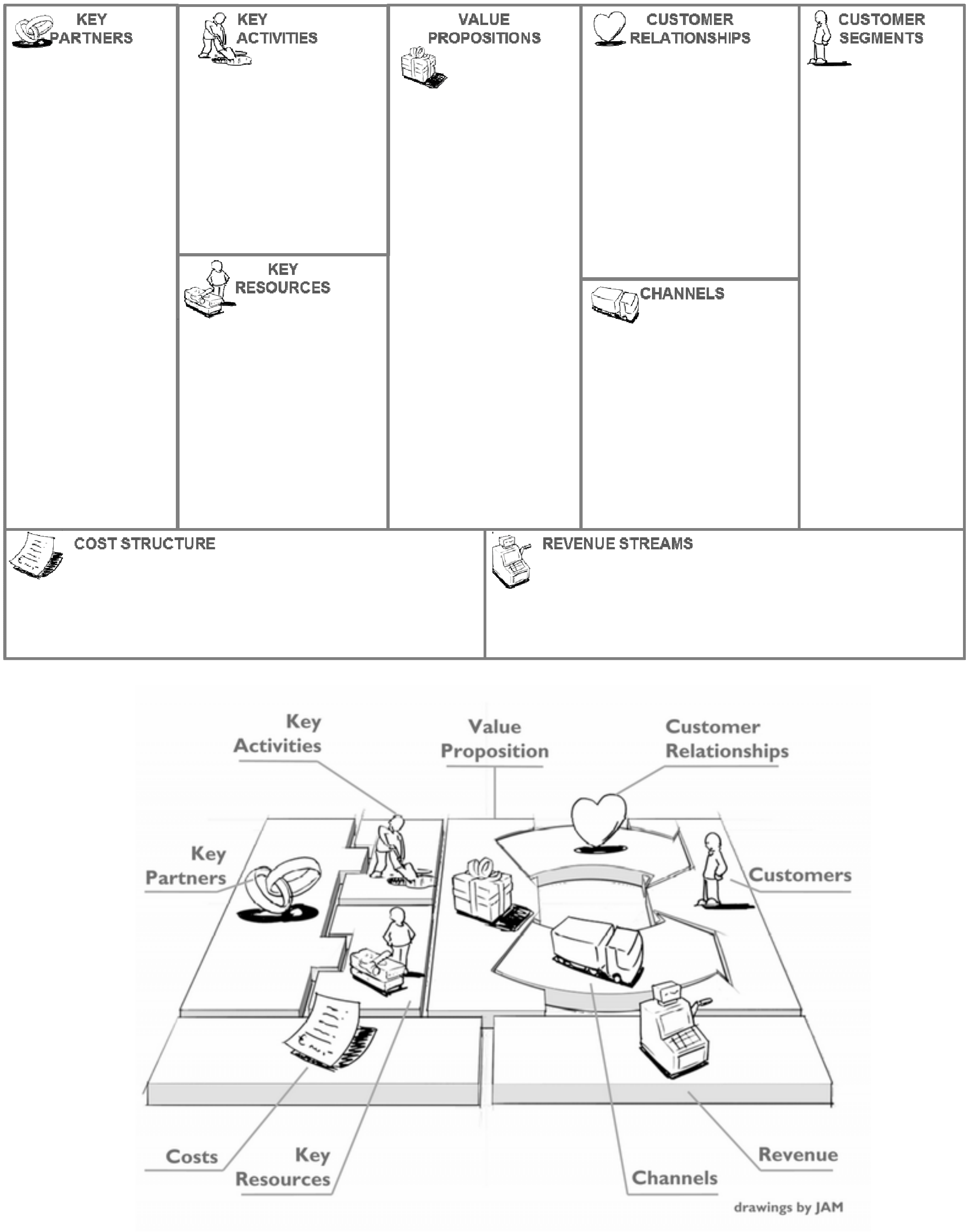


Figure Osterwalder's business model canvas.

The first step is identifying the **Key Partners** needed for the development of the proposed business. This also implies further on the definition of the key suppliers, the key resources acquired from partners and the key activities do partners perform.

The motivations for partnerships are the optimization and economy, the reduction of risk and uncertainty, the acquisition of particular resources and activities.

Subsequently the **Key Activities** have to be identified; these are all the sine qua non activities that the value proposition requires. The categories of the key activities can be the following: production, problem solving, and platform/network.

The identification of **Key Resources** is also very important, because all value propositions are based on existing resources. The types of resources can be physical, intellectual (brand patents, copyrights, data), human, and financial.

Value Proposition is then identifying the value that is delivered to the customer, which one of the customer's problems is the value proposition helping to solve, which customer needs are satisfied and what bundles of products and services are offered to each customer segment.

The characteristics of the value proposition can fall in one of the following categories: newness/innovation, performance, possibility of customization, "getting the job done", design, brand/status, optimizing price, cost reduction, risk reduction, accessibility, convenience/usability.

Customer Relationship identification is answering the questions related to the type of relationship that each of the identified customer segments expects to establish and maintain, how are the relationships integrated with the rest of the business model and how costly are they?

Some examples of customer relationships are: personal assistance, self-service, automated services, communities, and co-creation.

Channels identification means to establish through which channels the customer segments want to be reached, how are we reaching them now, how are our channels integrated, which ones work best, which ones are most cost-efficient and how are we integrating them with customer routines.

Different channels can be used depending on the business phase.

The identification of the **Customer Segments** means answering to the questions: for whom are we creating value and who are our most important customers? These segments can be the mass market, a niche market, segmented, diversified, multi-sided platform.

The identification of appropriate revenue streams and the cost structure in the canvas are usually filled in when a business plan has to be created. Therefore, since 5G-ENSURE must only provide possible business models, we do not address these categories for all the solutions described in the present document.

In the last section, each partner uses the canvas illustrated above to present the business models for 5G-ENSURE exploitable results that they are interested in vending to the mobile security market.

4.2 Business Impact of new regulatory landscape

4.2.1 GDPR

The regulation on data privacy will have several impacts on business. Some of the changes introduced by GDPR [13] can have a broadly positive effect for most businesses such as:

- *Greater harmonization*: businesses will face a more consistent set of data protection obligations from one EU Member State to the next, thanks to a single-legal framework that applies across all EU Member States without the need for national implementation. This should aid overall compliance. As a direct consequence, this harmonization will enable easier expansion of businesses across Europe. According to the currently directive, a small advertising company that wants to expand its activities from one EU country to another is subjected to a separate set of rules related to its data processing activities and the company will have to deal with a new regulator. The costs of obtaining legal advice and adjusting business models in order to enter this new market may be prohibitive. With the new data protection rules, the company will scrap all notification obligations and the costs associated with these. The aim of the data protection regulation is to remove obstacles to cross-border trade.

- *The risk-based approach to compliance*: Regulation acknowledges a risk-based approach to compliance, under which businesses would bear responsibility for assessing the degree of risk that their processing activities pose to individuals. Low-risk processing activities face a reduced compliance burden. On the other hand, documented data protection impact assessments still be required for high-risk processing activities. These compliance steps will need to be integrated into future product cycles.
- *The 'One-Stop Shop*': currently, a Data Protection Authority ("DPA") may exercise authority over businesses established in its territory or otherwise falling within its jurisdiction. Under the Regulation, where a business is established in more than one EU Member State, the supervisory authority ("SA") of the main establishment of the business will act as the lead authority for data processing activities that have an impact throughout the EU and will co-ordinate its work with other SAs. Organisations established in multiple Member States may benefit from having a single "lead DPA". In addition, each SA will have jurisdiction over complaints and possible violations of the Regulation in their own Member State.

On the other hand, the implementation of the EU GDPR will require comprehensive changes of business practices for companies that had not implemented a comparable level of privacy before the regulation entered into force. The GDPR has introduced a number of requirements that may be particularly challenging for businesses which include:

- *Consent, as a legal basis for processing*: one of the most important implications for business is that consent needs to be obtained for collecting data and the purposed for which it's used. According to the Regulation, individuals' consent must be freely given, specific, informed and unambiguous and it may not be valid if bundled with other matters or if it is part of the general terms of conditions. In addition, organisations will be required to demonstrate that consent was given.
- *Data protection by design and by default*: businesses will be required to implement data protection by design (e.g., when creating new products, services or other data processing activities) and by default (e.g., by implementing data minimisation techniques). They will also be required to perform data protection impact assessments to identify privacy risks in new products.
- *The anonymisation and pseudonymisation of personal information*: fully anonymised data will no longer be treated as personal data, and will not be subject to the requirements of the GDPR since it is impossible to identify any individuals from the data. However, full anonymisation is very difficult to achieve in most cases. The regulation introduces a concept of 'pseudonymised data', requiring that the 'key' necessary to identify individuals from the pseudonymised data must be kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person. Pseudonymous data will still be treated as personal data, but they can reduce the risks of non-compliance.
- *The individual right to data erasure*: under the regulation, individuals will have the right to request that businesses delete their personal data in certain circumstances (e.g., the data is no longer necessary for purposes for which it was collected). As a result, businesses will need to ensure that these requests are appropriately addressed.
- *The individual right to Data Portability*: Individuals will have the right to obtain a copy of their personal data. This means that organisations need to offer individuals their personal data in a legible electronic format.
- *Data breach notification* – organisations must publish their security failings. The Regulation will require businesses to notify the SA of data breaches within 72 hours. Businesses will need to develop and implement a data breach reporting and response plan. The breach notification rule is likely to increase the risk profile for businesses, as their security breaches may get into public domain and attract attention of regulators and media.
- *Data Protection Compliance programme*: business will have to implement and be able to demonstrate to the SA that they have comprehensive data protection compliance programmes, with policies, procedures and compliance infrastructure.

- *New obligations of data processors*: The Regulation introduces direct compliance obligations for processors. Under the Directive, processors generally are not subject to fines or other regulatory penalties. In an important change, under the Regulation processors may be liable to pay fines of up to €20 million, or 4% of annual worldwide turnover, whichever is greater.

As a general consideration, businesses that fail to adequately protect individuals' personal data risk losing their trust. This trust is essential to encourage people to use new products and services. Even if some new aspects introduced by the GPDR have an impact on business they can in some way incentivise businesses to innovate and develop new ideas, methods, and technologies for security and protection of personal data. Businesses will have incentives to use techniques such as anonymisation (removing personally identifiable information), pseudonymisation (replacing personally identifiable material with artificial identifiers), and encryption (encoding messages so only those authorised can read it) to protect personal data. If personal data is fully anonymised, it is no longer personal data [19]. Increased demand for privacy friendly products and services will foster new investment and release the single market's potential to provide a greater choice of goods at lower prices.

4.2.2 NIS impact on business

The most obvious effect of NIS is that it will mean additional costs for all businesses covered by the proposed directive in terms of creating new processes and acquiring new technology to comply.

The directive means that, for the first time, companies will be under a legal obligation to ensure they have suitable IT security mechanisms in place, which is likely to boost IT spending across the EU.

Conversely, it will mean additional income for the IT security industry as businesses are forced to find money to invest in whatever additional security technologies they need to become compliant.

First, it will force a technology refresh for most businesses to bring themselves up to standard, and thereafter legal obligations will drive more frequent technology updates than exist today.

Third, as security incident detection capabilities increase so will the number of incidents detected and, consequently businesses will face a new and increasing cost of managing and responding to those alerts.

No one is likely to argue that greater network and information security and resiliency is not necessary, but in pursuit of that ideal, business is likely to face a whole raft of new costs.

4.2.3 BEREC impact on business

The telecom industry warns that the current Net Neutrality guidelines create significant uncertainties around 5G return on investment. In the "5G Manifesto", telco and industry verticals concur that "the implementation of net neutrality laws should allow for both innovative specialised services required by industrial applications and the internet access quality expected by all consumers" and points out "the danger of restrictive Net Neutrality rules in the context of 5G technologies, business applications and beyond". In addition, they consider the new "concept of 'Network Slicing' to accommodate a wide-variety of industry verticals' business models on a common platform, at scale and with services guarantees".

In the meantime, telecom industry has pledged to deliver 5G internet across Europe by 2020, but under the "excessively prescriptive" net neutrality rules (which would exclude "specialised services") this is not ensured. This would delay the roll-out of automated driving, smart grid control, remote healthcare monitoring, etc. 5G would introduce so-called "network slicing", which makes it possible to offer different levels of guaranteed quality to such new applications

4.3 Market opportunities and Business Models for 5G-ENSURE enablers

This section illustrates the Business Models per partner and exploitable result. Specific business models will be prepared for selected 5G-ENSURE exploitable results, namely for the enablers that have been identified to have a market opportunity at the present time.

Each partner or coalition of partners proposes a Business Model for one or more solutions in which they are majorly interested, either in order to sell the solution on the market, or to propose the solution to their own organization.

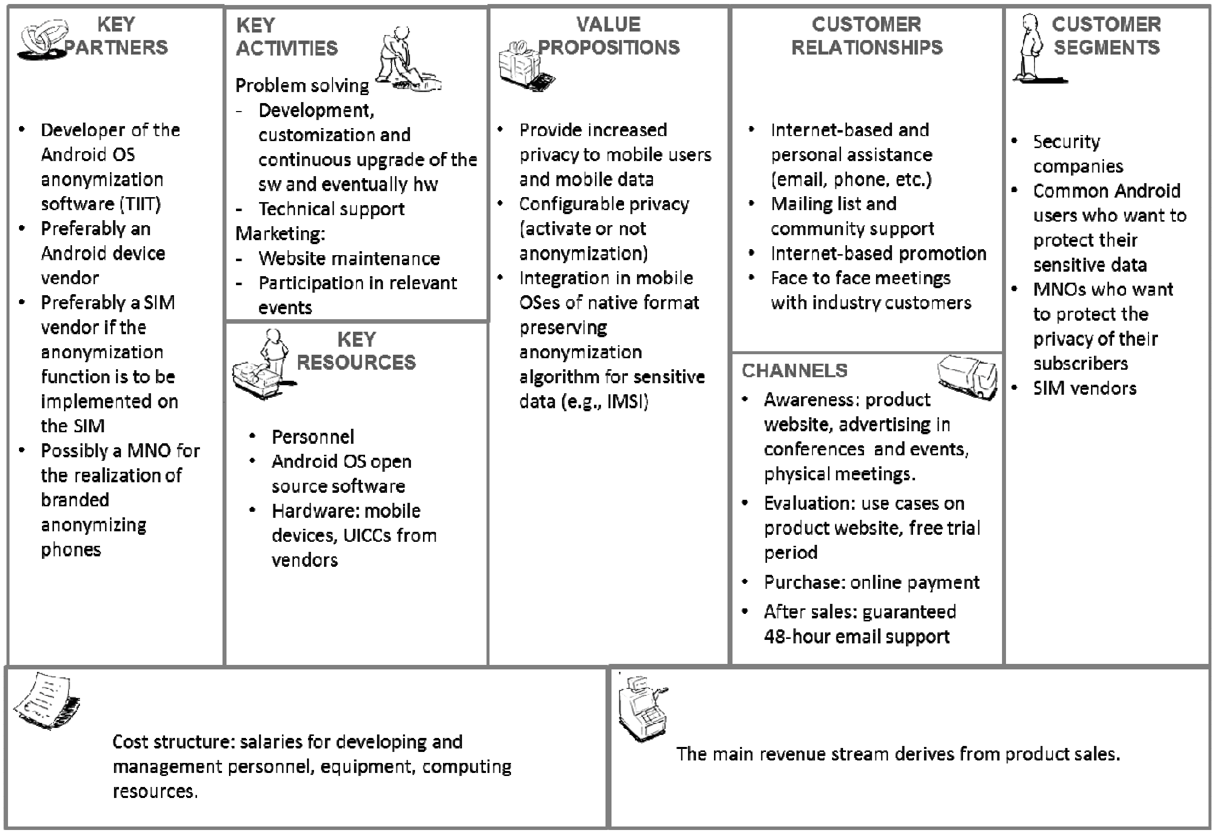
4.3.1 Device-based anonymization - Example Business Model

Based on the 5G-ENSURE achievements (device-based anonymization enabler) and on the analysis of mobile security market, we propose the business model related to an Android OS/device which can, upon user configuration, anonymize sensitive data, especially data stored on the SIM and accessible to user-space applications, i.e. the IMSI (see full description in the 5G-ENSURE deliverable D3.1 "5G-PPP security enablers technical roadmap" [23]).

As increasingly powerful smartphones and other mobile devices have invaded enterprise environments in recent years, security professionals have often feared a corresponding rise in mobile malware, similar to what was witnessed on the PC landscape more than a decade ago. Nevertheless, according to a recent report, mobile app data collection is posing a far greater risk to enterprises and users.

Mobile applications, and especially free mobile applications, collect a large amount of users' data. It is of paramount importance that 5G users may be put in control of their own privacy, and therefore, that they can take advantage of mobile OSes/devices that allow the activation of privacy protection functionalities, which are, preferably, also able to provide fine grained privacy configurations.

Based on the 5G-ENSURE Device-anonymization enabler, the example BM proposed herein is related to an Android OS/device that, upon user configuration, can perform user data anonymization.



KEY PARTNERS

- Developer of the Android OS anonymization software (TIIT)
- Preferably an Android device vendor
- Preferably a SIM vendor if the anonymization function is to be implemented on the SIM
- Possibly a MNO for the realization of branded anonymizing phones

KEY ACTIVITIES

Problem solving
- Development, customization and continuous upgrade of the sw and eventually hw
- Technical support

Marketing:
- Website maintenance
- Participation in relevant events

KEY RESOURCES

- Personnel
- Android OS open source software
- Hardware: mobile devices, UICCs from vendors

VALUE PROPOSITIONS

- Provide increased privacy to mobile users and mobile data
- Configurable privacy (activate or not anonymization)
- Integration in mobile OSes of native format preserving anonymization algorithm for sensitive data (e.g., IMSI)

CUSTOMER RELATIONSHIPS

- Internet-based and personal assistance (email, phone, etc.)
- Mailing list and community support
- Internet-based promotion
- Face to face meetings with industry customers

CHANNELS

- Awareness: product website, advertising in conferences and events, physical meetings.
- Evaluation: use cases on product website, free trial period
- Purchase: online payment
- After sales: guaranteed 48-hour email support

CUSTOMER SEGMENTS

- Security companies
- Common Android users who want to protect their sensitive data
- MNOs who want to protect the privacy of their subscribers
- SIM vendors

Cost structure: salaries for developing and management personnel, equipment, computing resources.

The main revenue stream derives from product sales.

Figure 1 Example Business Model for the device-based anonymization enabler.

Value Proposition

The value proposition of this service is the anonymizing OS/device. If an alliance with a SIM vendor is available, the anonymization can be performed on/by the SIM for data which is stored on the SIM itself (e.g., the IMSI – International Mobile Subscriber Identifier).

Key Partners

The key partners are TIIT, preferably a SIM vendor, possibly a device vendor and/or an MNO which may want to sell branded "anonymizing" phones. The product may be sold as a modified Android OS, enhanced with anonymization capabilities (the modified OS + the format preserving anonymization algorithm + the configuration part). If an alliance with a SIM vendor becomes possible the anonymization algorithm may also be ported on the SIM itself for the anonymization of the data contained therein directly at at the source.

Key Activities

The key activities are mainly in the area of problem solving and marketing.

Problem solving activities include:

- Development, customization and continuous upgrade of the software and possibly of the hardware (devices, if specific devices are also sold with the anonymization solution, and SIM, if the anonymization algorithm can also be implemented on the SIM)
- Technical support activities.

In addition to technical activities, marketing aspects are also present in order to promote the solution by maintaining an up-to-date website and participating in relevant events where clients can be encountered. The main marketing activities:

- Product’s website maintenance, advertising
- Participation in relevant events
- Participation to face to face meeting with device and SIM vendors.

Key Resources

The key resources are software engineers who will develop and maintain the anonymization software and provide technical care and support, and devices/servers/SIMs for development, testing.

Customer Segments

Relationship with each of the customer segment will be established and maintained via dedicated personal assistance. These customers can also benefit from the mailing list and community support already available for the simulation platform.

Customer Relationships

The main channels for increasing awareness of the anonymization OS/device are relevant conferences and events where the targeted customer segments can be engaged. Also, a dedicated website can be launched to provide potential customers with up-to-date information about product features and use cases, along with access to a free trial period for evaluating the sw. Products based on the anonymization sw can be delivered in the form of licensed software modules.

Costs and revenues

The business model has fixed costs (salaries of software and web developers), and variable costs (equipment and possibly on-demand rental of devices or computing resources). Revenue will be generated by licensing existing software modules, personalized for each customer segment.

The cost of can be very flexible and adapting to customer needs. The revenues may vary significantly on the specific segments, together with the service/support type, the communication channels and the type of customer relationships.

In summary, the biggest fixed cost is the personnel cost which include:

- Product development
- Product management
- User experience (interaction and graphical design)
- Sales
- Security related research.

The variable OPEX is related to marketing and hosting centres.

Other issues

For exploitable results which were identified to have a vending potential, the final version of this deliverable will include a SWOT analysis and a study of how the weaknesses and threats identified by the SWOT analysis can be addressed by the proposed business model.

5 References

[1] SMART report on the impact of 5G on EU industry: “Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe”, ISBN 978-92-79-58270-7, October 2016. https://ec.europa.eu/digital-single-market/en/news/5g-deployment-could-bring-millions-jobs-and-billions-euros-benefits-study-finds

[2] ETRI Industrial strategy research lab, August 2014.

[3] ETRI Industrial strategy research lab, based on ‘IDC, Worldwide Big Data Technology and Services Forecast', 2015.

[4] K-ICT Strategy to spread IoT, 2015.

[5] IHS Cybersecurity Report, 2016.

[6] An analysis of the security needs of the 5G market. SIMalliance 5G Working Group marketing white paper, 2016. http://simalliance.org/wp-content/uploads/2016/02/SIMalliance_5GWhitepaper_FINAL.pdf

[7] "Opportunities in 5G", Ericsson, 2016, based on a survey of 650 decision makers from 8 verticals.

[8] "Connected Car Report 2016 – Opportunities, risks, and turmoil on the road to autonomous vehicles", PWC, 2016.

[9] "Mobile operators: the digital transformation opportunity", GSMA Intelligence / CAICT, June 2016.

[10] ENISA Annual Incidents report, 2016. https://www.enisa.europa.eu/publications/annual-incident-reports-2015

[11] Threat Landscape and Good Practice Guide for Software Defined Networks/5G, ENISA, December 2015.

[12] ENISA website, accessed on 6 Oct. https://www.enisa.europa.eu/

[13] The General Data Protection Regulation (GDPR), EU Parliament, April 14, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[14] EU Data Protection Directive 95/46/EC, 1995. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046

[15] EU Directive on Security of Network and Information Systems. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=EN

[16] "Guidelines on the Implementation by National Regulator Authorities (NRAs) of European Net Neutrality Rules", Body of European Regulators for Electronic Communications (BEREC), 30 August 2016. http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

[17] EU Regulation 2015/2120 ("Telecoms Single Market Regulation"). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=DE

[18] The Business Model Canvas poster, Alex Osterwalder. http://www.businessmodelgeneration.com/downloads/business_model_canvas_poster

[19] EU data protection factsheet. http://ec.europa.eu/justice/data-protection/document/factsheets_2016/data-protection-factsheet_01a_en.pdf

[20] https://ec.europa.eu/digital-single-market/en/digitising-european-industry

[21] https://ec.europa.eu/digital-single-market/en/connectivity-european-gigabit-society

[22] https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-service-revenue/

[23] 5G-ENSURE Deliverable D3.1 - 5G-PPP security enablers technical roadmap (early vision), March 2016, http://5gensure.eu/deliverables