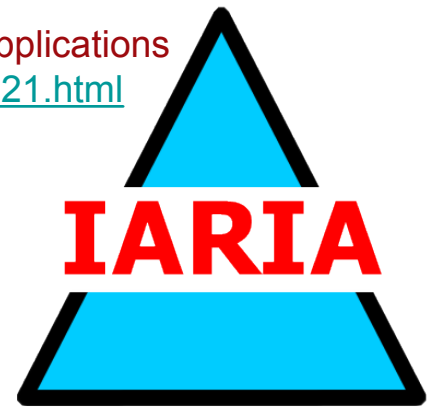




The Tenth International Conference on Intelligent Systems and Applications
INTELLI 2021: <https://www.iaia.org/conferences2021/INTELLI21.html>
July 18, 2021 to July 22, 2021 - Nice, France



Security Threats from superfast networks

Ioannis A. Pikrammenos, Dr. Ing.
(former) Mediterranean College associate
ioannispikrammenos@teemail.gr

Presenter's presentation

Ioannis A. Pikrammenos, Dr. Ing., MBA, has graduated Electrical Engineering and Computer Technology at Patra's University, Greece and has acquired his doctoral thesis as well as his MBA diploma from National Technical University of Athens, Greece. He has been employed as scientific associate from numerous research and educational institutions as well as central and local government. His involvement into public affairs led to the participation in fourteen (14) public interest committees, the last one as president, the evaluation in seven (7) co-funded programs and the employment in five (5) as scientific responsible. He has participated in thirty (30) research projects in the field of ICT, four (4) co-funded projects in the fields of ICT, energy and education/training, summing up to 20 scientific publications, being reviewer in one (1) scientific periodical. He has been employed as lecturer on ICT for over 20 years in numerous universities (national and/or international) and institutions, summing up to more than 10,000 teaching hours (EQF 5-6-7), certified as lecturer in adult training and distance learning. He is an enthusiast of entrepreneurship and of sustainable development, pioneering in the area of entrepreneurship cohesion, has supervised more than 100 business plans and 1 patent application. Ioannis is married, father of three children.



5G security

Research interest

- His research interest is focused on computer and communication networks, their secure and sustainable deployment and utilization, digital applications towards cultural heritage dissemination, as well as distant learning with emphasis on time and space incoherent learning methodologies.

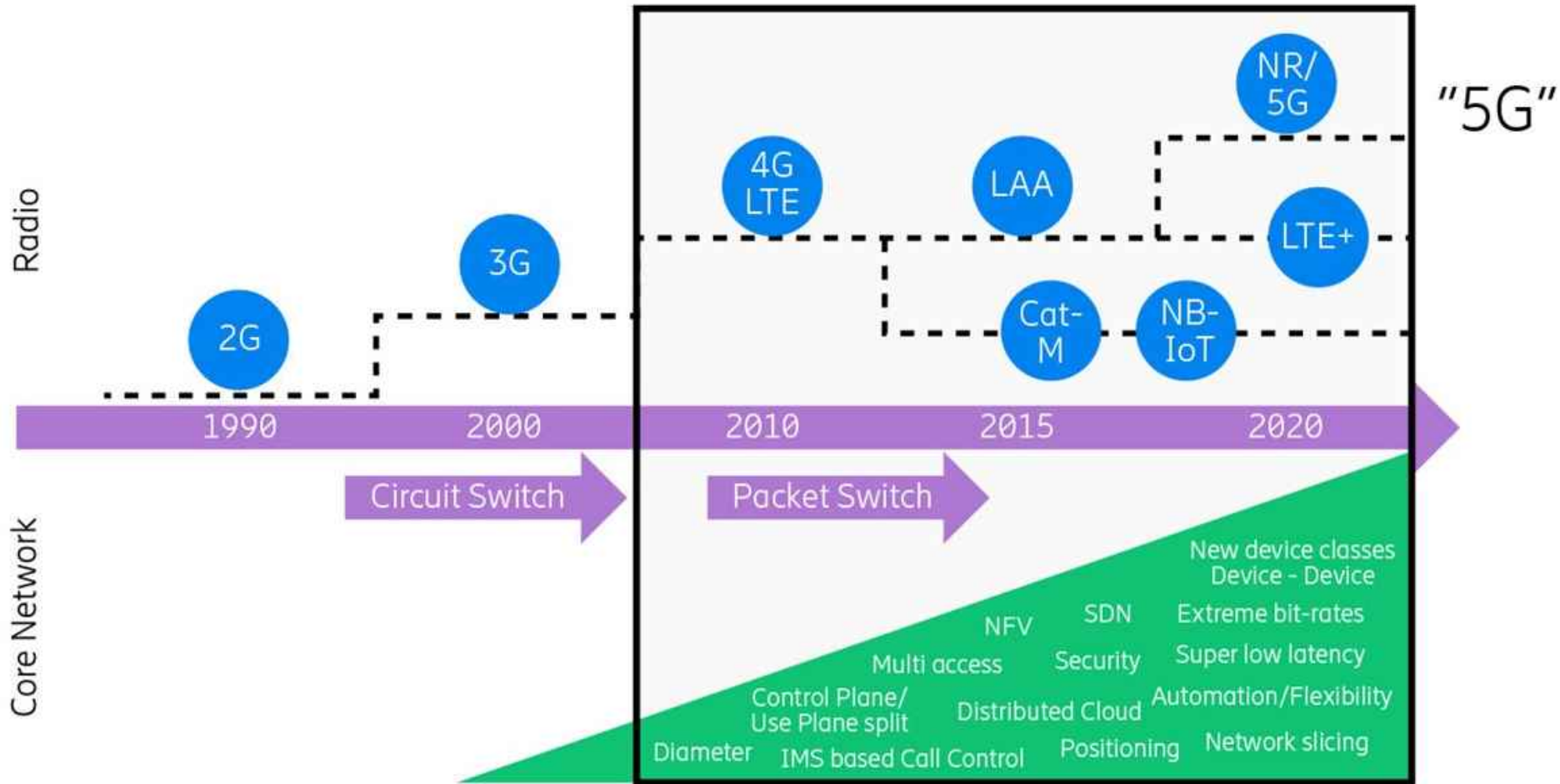
INTRODUCTION

- Today we live in the era of Teraflop, PetaByte, Gigabits, Mega-Data Center consuming KiloWatts of energy. The technology evolution in the field of “new technologies” and we mean ICT is so vast that the end user finds it hard to adapt to. At this point threats appear against systems and data security.
- Target of the seminar is to present the range of modern technological solutions and their security issues.

WHAT IS 5G

- 5G is the short term for the fifth generation network.
- These generations are the evolution of cellular network. Each one of the previous ones brought a new level of connectivity, the latest focusing on data. 5G continues on this leeway targeting to bring broader connectivity to mobiles.

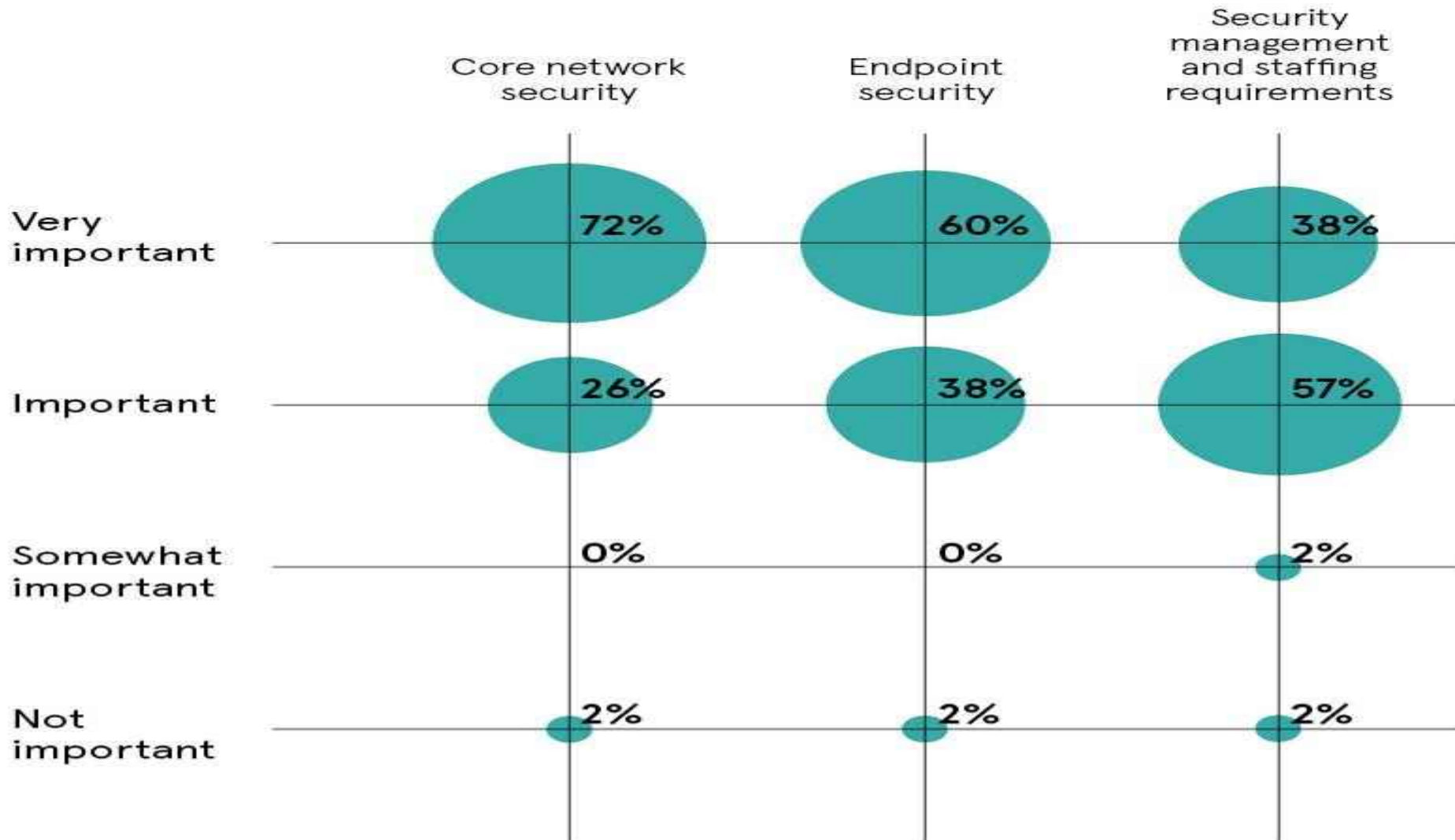
Evolution towards 5G



Why 5G

- The heavy usage of the 4G LTE network in urban environments lead to connection speed degradation at peak hours.
- IoT brings billion of wireless devices into the network meaning that they should enjoy broadband access.
- Evolving wireless technologies promise higher transfer rates with lower power consumption and in shorter range
- New spectrum allows for more devices

SECURITY ISSUES OF 5G



Decentralized security

- In 5G technology base stations are limited, regarding to prior ones, allowing for easier security checks and maintenance.
- Contrary to prior technologies, 5G requires more routing points and dynamic systems. Those topologies should be monitored in order to remain secure.
- In case this is proved difficult, security flaws at the end point can be transformed as security issue for the whole network.

Virtualization

- Higher layer functions that were implemented in physical appliances are in 5G migrating to virtual ones. Nevertheless, the protocols utilized are well known and standard, like IP, allowing for attacks either from hackers or for monitoring from governments. This makes security more complicated.

Security monitoring

- Limited capacity and speed of current networks allowed for the operators to monitor security in real time mode. 5G speed and wideness may alter the way security is monitored. To the worst direction, as there will be experienced lack of resources, but to the best as well, as new methods of security monitoring and threat handling shall evolve.

IoT standard-less devices

- As more connected devices enroll the cloud, a vast diversification on security standards is experienced. As such, degraded security of a smart TV or a thermostat in a fish pool may result to an intrusion point of the network. This could easily be elevated to an uncontrolled security Armageddon.

Lack of cryptography

- Standard communication of network devices with service providers include information about the device itself or the operating system it is running. This information is valuable to attackers in order to target their attacks. Lack of cryptography allows anyone to access such information.

Backward compatibility

- Whenever 5G are not available, devices are falling back to 4g, or even 3G, in order to acquire services. This opens a hole in security management as all services are not backward compatible, exposing security flaws.

Identity
management



IoT security

Applications of 5G

Enhanced mobile broadband



Non-SIM devices



Smart phones



Homes, enterprises and venues (mobile/wireless/fixed)



4K/8K, UHD, broadcasting, virtual reality, augmented reality

Massive machine-type communication



Smart building



Logistics, tracking and fleet management



Smart meters



Smart agriculture



Capillary networks

Critical machine-type communication



Traffic safety and control



Remote manufacturing, training and surgery



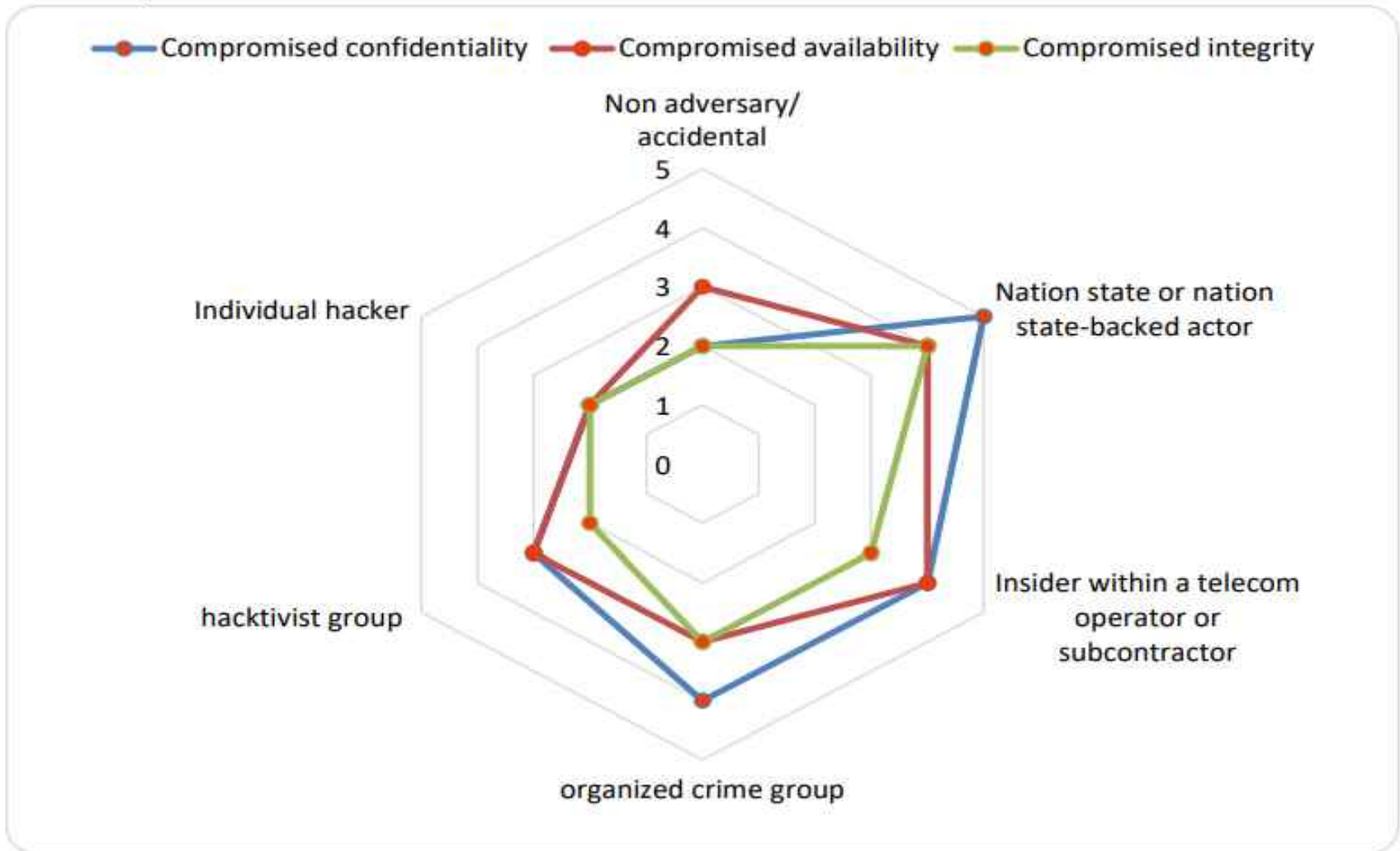
Industrial applications and control

EU strategy

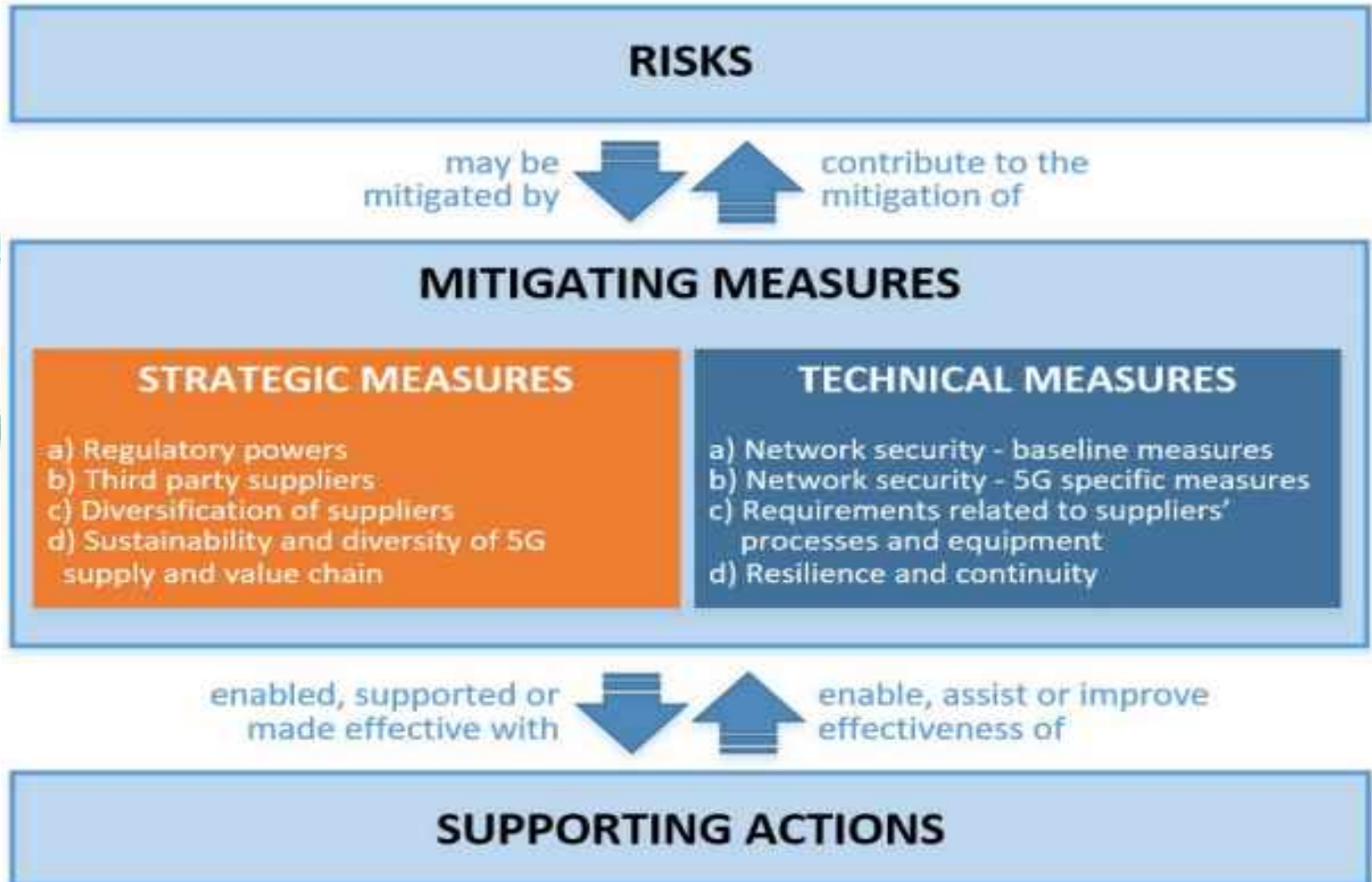
- EC has approved the common toolset for moderation of the 5G related security threats, following requirements for coordinated approach towards 5G evolution.



Threat evaluation



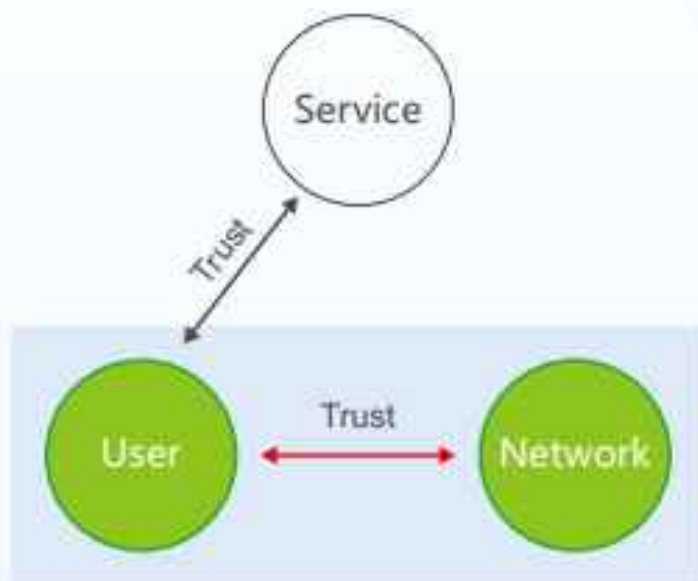
Common toolset



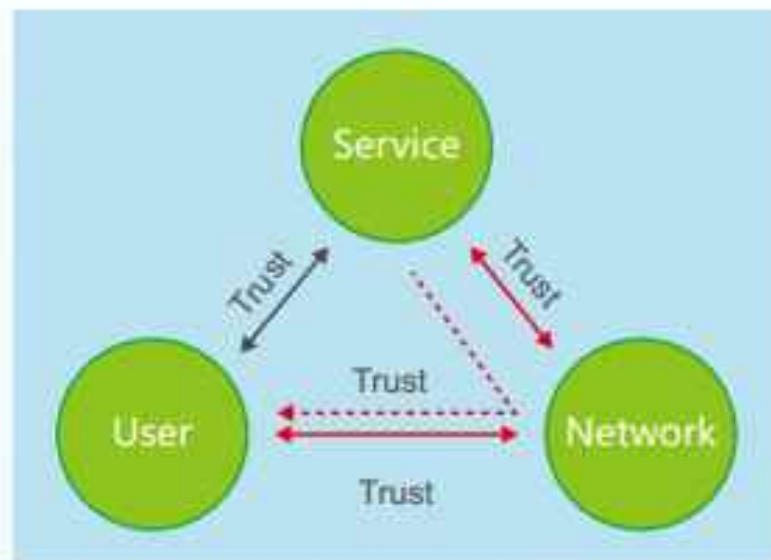
MEASURES	Indicative implementation timeframe	Potential implementation factors	SPECIFIC MEASURES	RISKS							
	Short-term Medium-term Long-term	Resource costs Sector specific economic impact Sector specific economic impact Broader economic / societal impact		R1: Misconfiguration of networks	R2: Lack of access controls	R3: Low product quality	R4: Dependency on a single supplier	R5: State interference through 5G supply chain	R6: Exploitation of 5G networks by org. crime	R7: Significant disruption of crit. Infras. services	R8: Massive failure due to power interruption
a) Regulatory powers	✓	✓ ✓ ✓ ✓	SM 01	■	■	■	■	■	■		
			SM 02	■	■	■	■	■	■		
b) Third party suppliers	✓	✓ ✓ ✓ ✓	SM 03		■			■			
			SM 04		■			■			
c) Diversification of suppliers	✓ ✓	✓ ✓ ✓ ✓	SM 05				■				
			SM 06				■				
d) Sustainability and diversity of 5G supply and value chain	✓ ✓ ✓	✓ ✓ ✓ ✓	SM 07				■				
			SM 08				■				

New trust model

- New trust model requires two ways authentication among service consumer and provider as well as network, something that 4G does not support



4G Network



5G Network

Diversified identity authentication

- Past cellular networks rely on SIM (U) cards in order to manage identities.
- IoT devices are too small or too cheap to house a SIM
- New methods of identity management required
 - Combination of device and application id
 - Management of users and devices

Diversified security for different services

- Critical services, like remote medical treatment, relay on robust security
- IoT would enjoy relaxed security
- Diverse security standards for different applications



Flexible security architecture

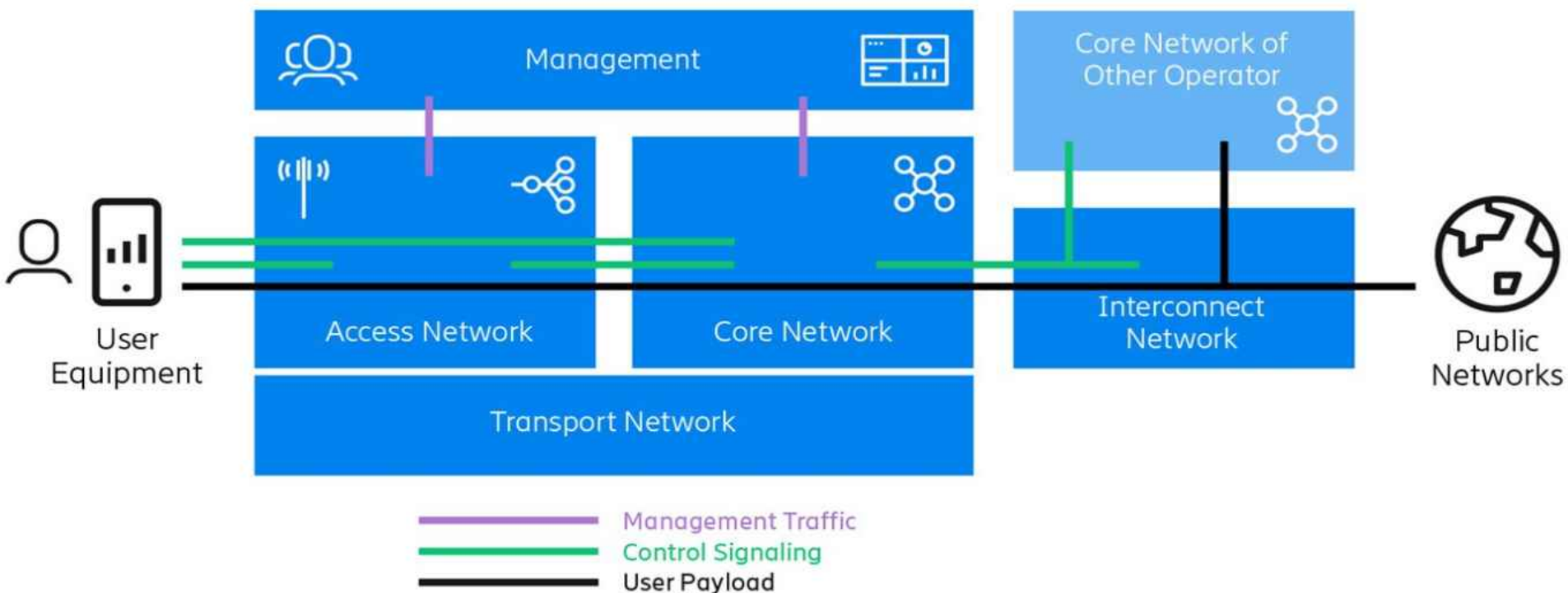
- Diversified security requires flexible architecture to support E2E security for services, according to network concatenation architecture. Various E2E security capabilities are available, like security algorithms, secret keys retrieval and management as well as integrity and confidentiality mechanisms.

Unified security management

- In a cloud environment, infrastructure and software comes from diverse manufacturers. This makes security management harder, as it complicates it. In order to cope with it, an end-to-end security chain should be supported, reducing the dependency of the users and applications from the intermediate nodes.

Management and control system

- Security to all data flows, either in network or inside device

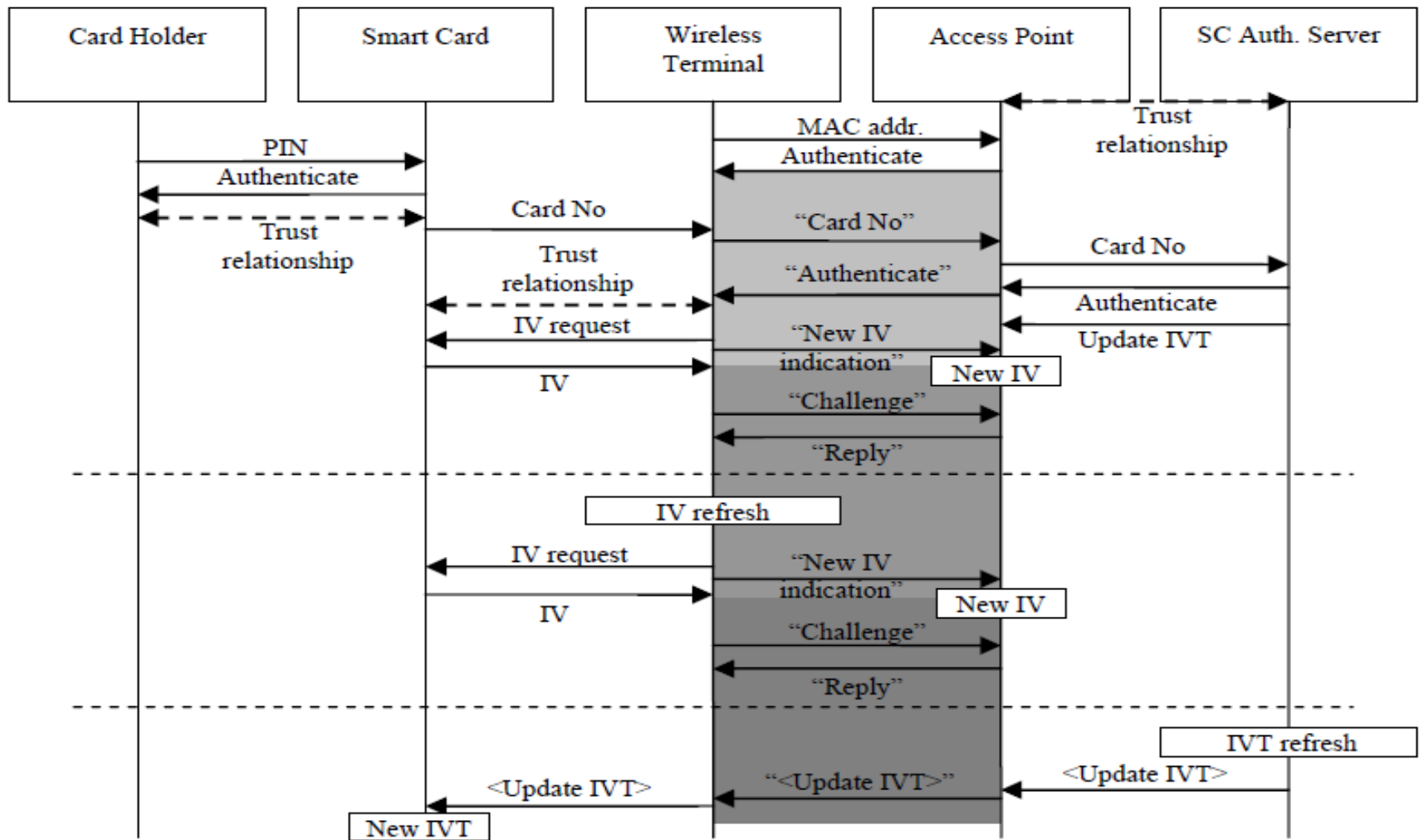


Network fragmentation

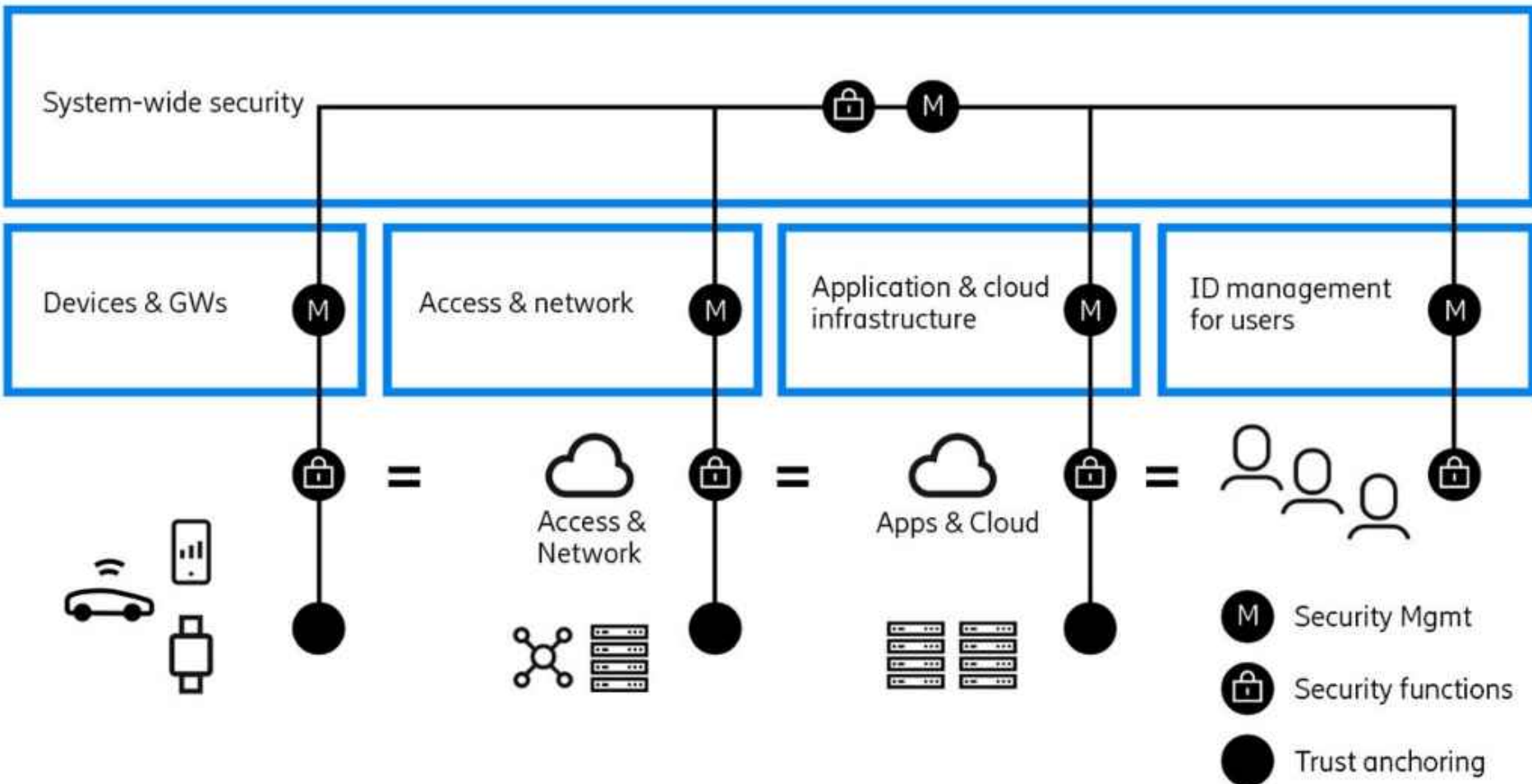
- Logical concatenation of network into segment for integrated management.



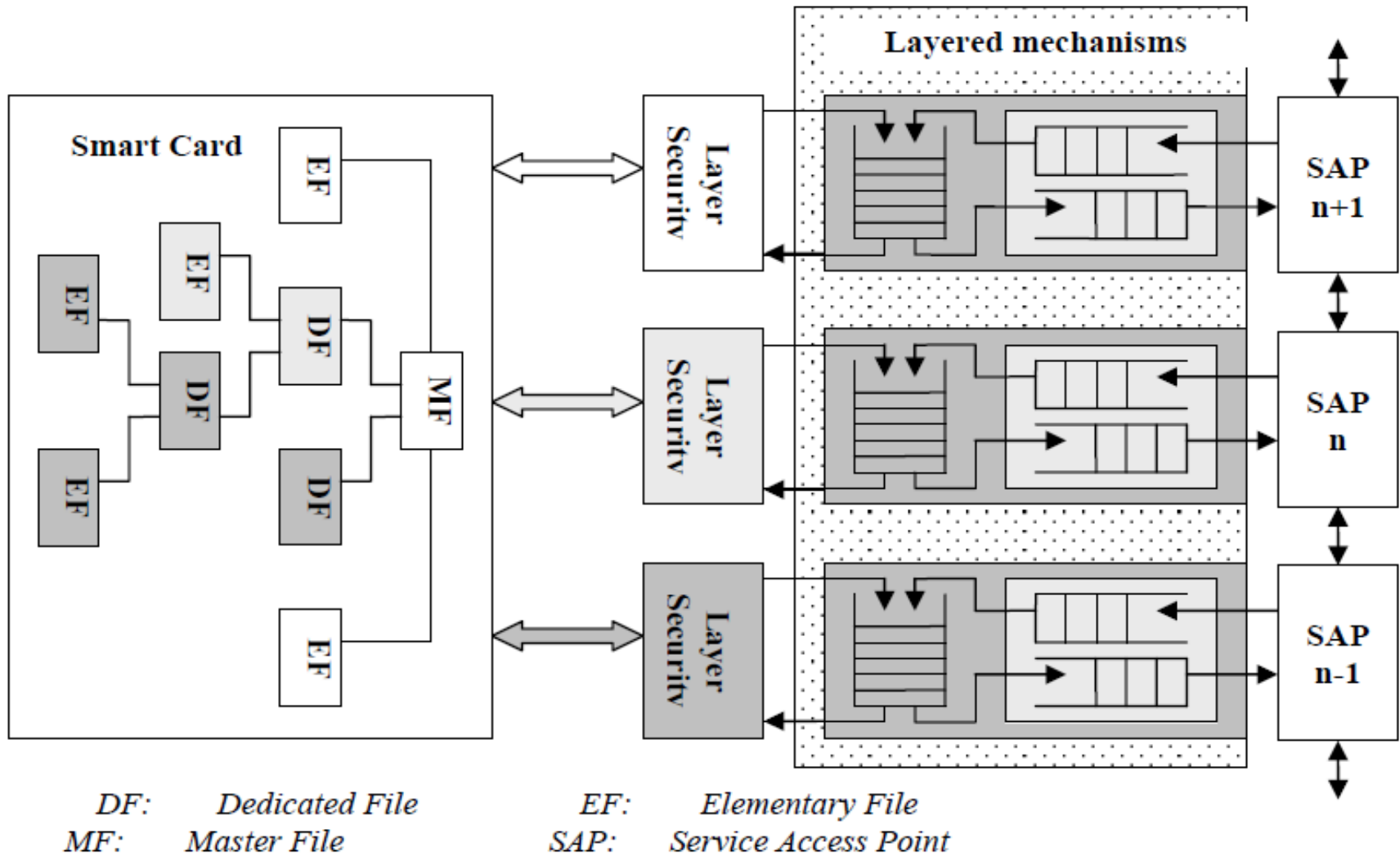
Proposition of application



End to end security (E2E)



Proposition of application



Conclusions

- Hope and courage should light our path to the future
- Past lessons should guide us
 - Forcing new technology into economy shall bring vast cost for handling and rehabilitation of errors
 - User perception should converge technological evolution
 - Distribution of investments towards last mile and user side for better experience
 - Disengage user from security procedures

Bibliography

- <https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons>
- https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123
- <https://www.informationsecuritybuzz.com/articles/security-challenges-next-generation-5g-mobile-networks/>
- https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf
- <https://www.ericsson.com/en/security/a-guide-to-5g-network-security>
- **I. A. Pikrammenos**, C. Lampiris, P. Tolis and P. Perakis, “*Emerging multi-functional, personalized secure environments*,” 10th International Conference on Information, Intelligence, Systems and Applications, July 2019.
- **G. Pikrammenos** et al “*Hidden layer authentication using smart card for WEP based WLANs*” p. 447-451 in “*Security and Privacy in the Age of Uncertainty*” D. Gritzalis et al Kluwer Academic Publishers 2003 IFIP ISBN 1-4020-7449-2.
- **Giannis A. Pikrammenos** “*Smart Media as the Secure Transactions Mediator of the Future*” p. 124 EC Workshop on Trust and Security May 2002 Brussels, Belgium.

Thank you for your attention



- <https://www.linkedin.com/in/ioannis-pikrammenos-18594522/>



- http://mycourses.ntua.gr/course_description/index.php?cidReq=PS TGR1083



- <https://emathisi.army.gr/>



- https://maredu.gunet.gr/main/profile/display_profile.php?id=8060&token=5fb24b6a-f517bbed8c0d7abb2075d63d44e185baeff8ff1e



ΑΣΠΑΙΤΕ



- <https://eclass.aspete.gr/courses/EHN294/>

- https://www.medcollege.edu.gr/ns_speaker/δρ-ιωάννης-πικραμμένος

- <https://www.cost.eu/>

- <http://pesd.econ.uoa.gr/ioannis-a-pikrammenos>

