Results of the Open Consultation on "5G Security"

1st International Workshop on 5G Security
Sophia Antipolis, France, 16 June of 2016

This research has been performed within 5G-ENSURE project (www.5GEnsure.eu) and received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 671562.

Context of the Open Consultation (1/2)

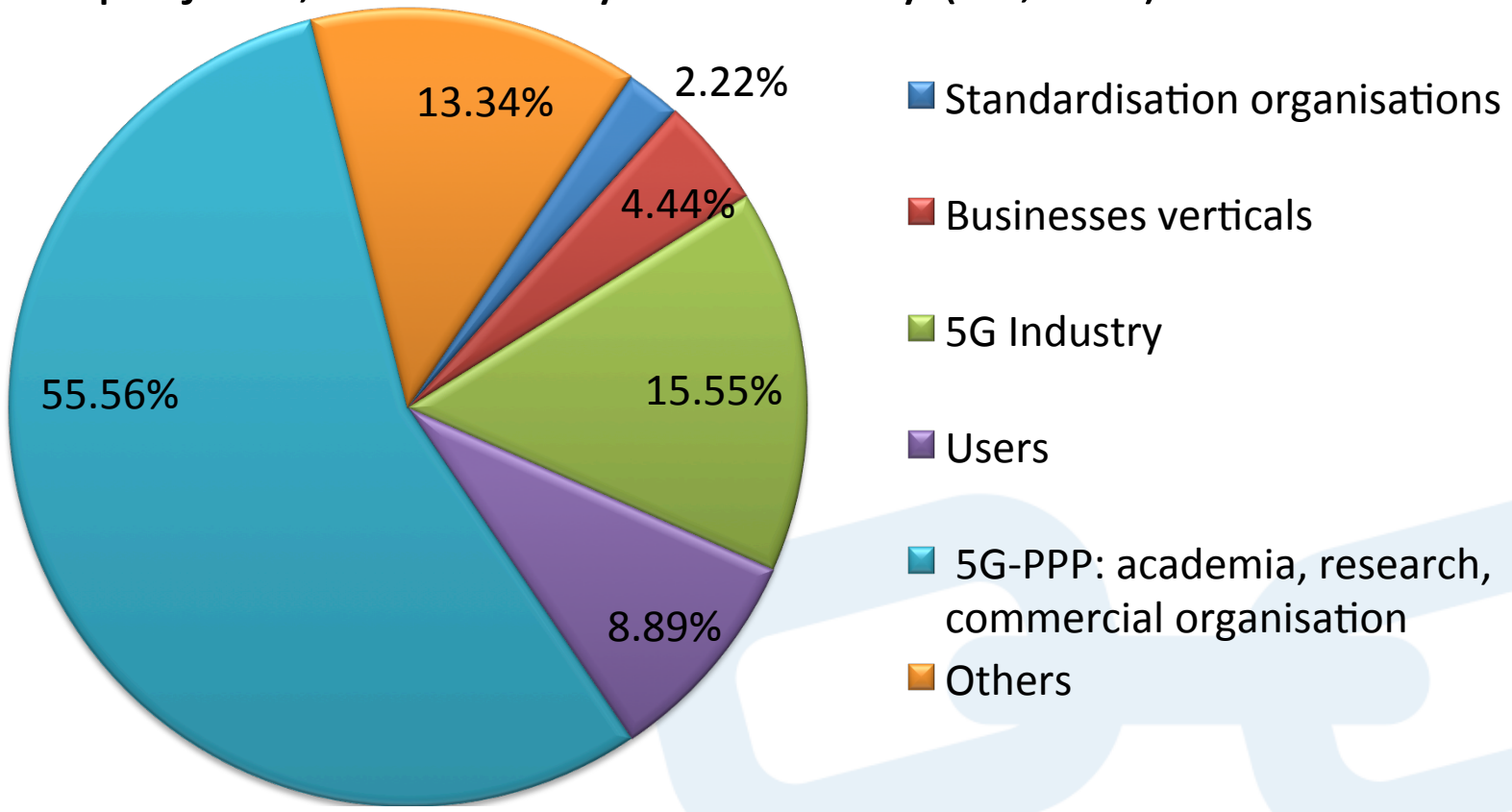
- As part of the 5G-ENSURE project's wider efforts to listen to relevant stakeholders and the general public on 5G security topics, an Open Consultation on 5G Security has been launched between 20 of March 2016 and 27 of May 2016.
- The consultation sought input from security experts and potential 5G stakeholders, to obtain the different points of view and perspectives on:
  - security and privacy challenges
  - security and privacy priorities
  - security impacts due to the adoption of technological advancements in 5G
  - the actions towards security standardization
- The Open Consultation is considered as a valuable source of information to evaluate if security aspects in 5G are being addressed in line with the 5G stakeholders expectations, if and where research improvements are needed.

Context of the Open Consultation (2/2)

- The open consultation was distributed through the project web-site and has been conducted in an anonymous way.
- Special announcements in the most relevant events have been done and several communication tools have been used to promote the open consultation.
- The open consultation results were combined into a single set of results in order to draw global conclusions on the main 5G security topics:
  - Security
  - Privacy
  - Trust
  - Network Virtualization
  - Standardization

Organization type of respondents

- In total 45 answers were received
- The majority of the respondents (55,56%) represent research centers (universities) and public-funded research 5G-PPPprojects, followed by 5G Industry (15,55%)

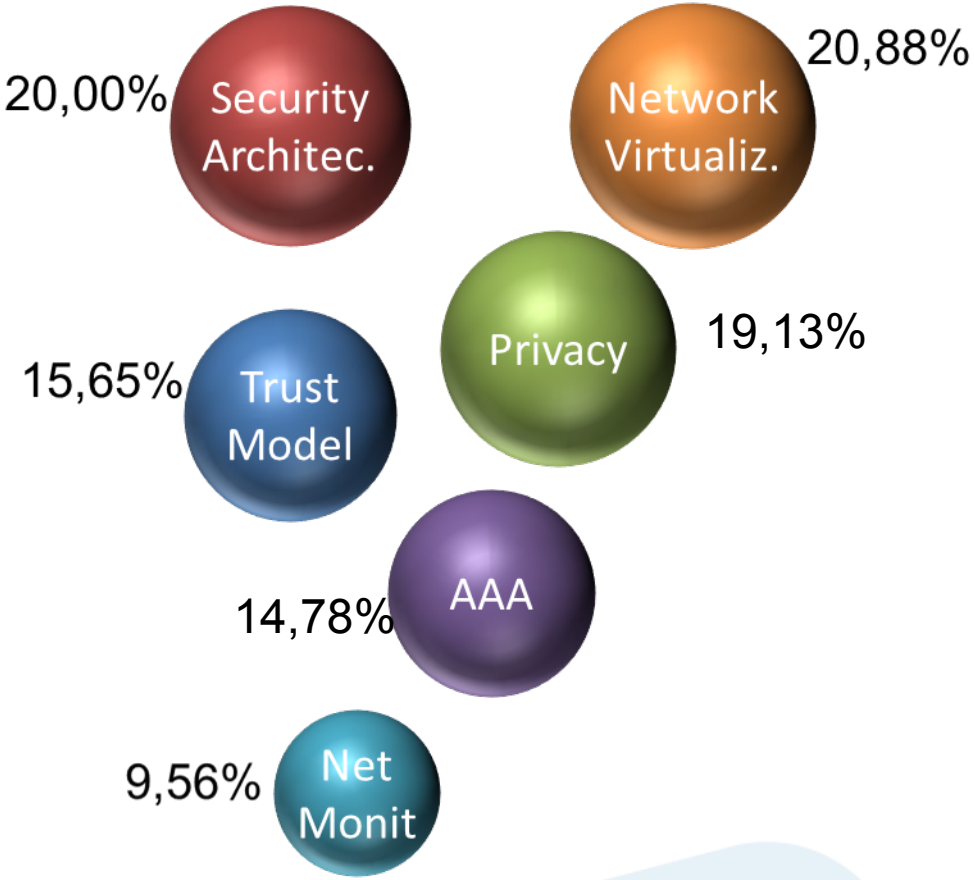


Security in 5G

Respondents to our open consultation were asked to indicate:

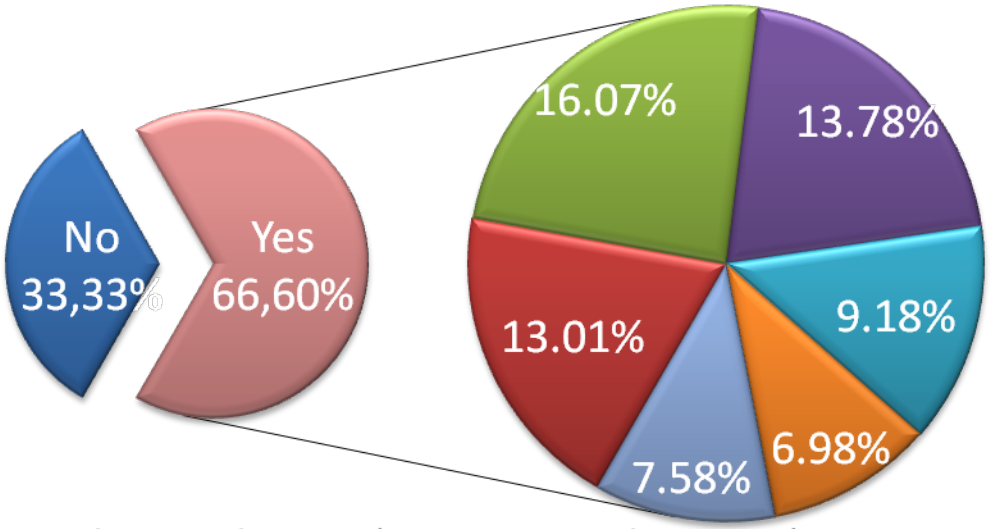
- The biggest security challenges in 5G network.
- If the 5G security should build on previous networks and in this case what can be reused
- The others (new) security priorities for 5G.

The biggest security challenges in 5G network



No significant differences in the answers: this means that all aspects are relevant enablers for 5G security

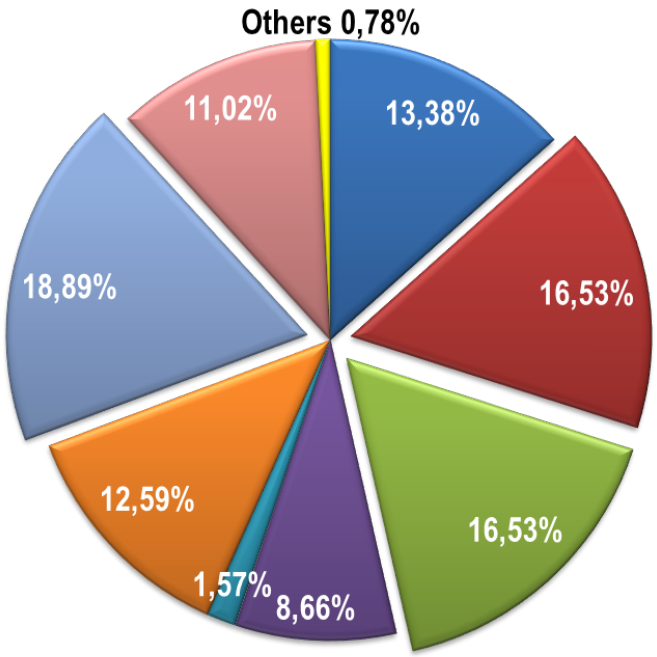
Security in 5G should build on previous networks.



- The confidentiality of device and user identity (temporary identities)
- The Authentication and Key Agreement AKA mechanism
- The crypto algorithms
- The network security architecture (e.g. RAN access)
- The confidentiality and integrity protection for signalling
- others

Security of previous networks is considered good enough and more aspects can be reused in 5G like crypto algo and AKA mechanism.

5G security priorities are mainly related to:

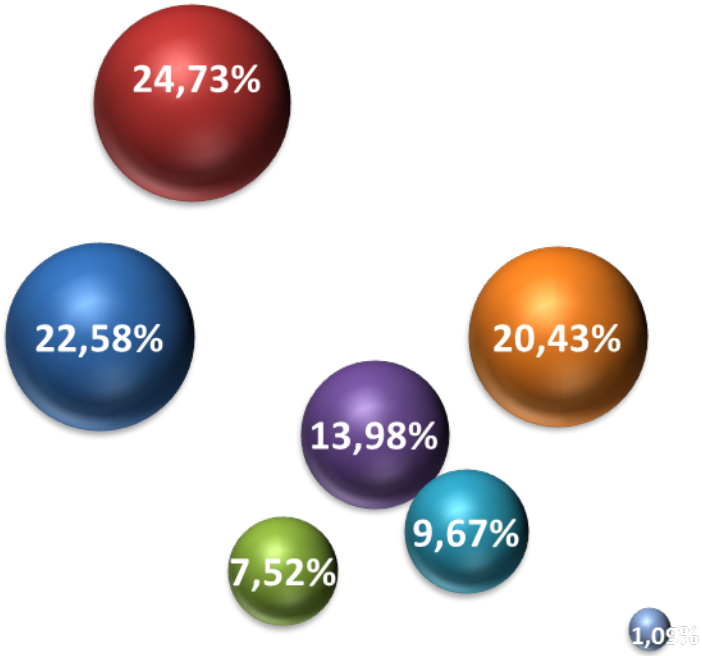


- Faster handling of security procedures for use cases that require extremely low latency
- Data authenticity, confidentiality and integrity for low complexity, low throughput services and sensors
- Seamless authentication across multi access networks or shared infrastructure
- Single user identification across multiple devices, services and networks
- Data verifiability
- Protection against (D)DoS attacks to core and radio access network
- Security mechanisms for NFV infrastructure
- Definition and adoption of trust models for multi-tenant scenarios

- **Security mechanism for NFV infrastructure**
- **CIA for low-end devices**
- **Seamless authentication across different networks**

Privacy in 5G

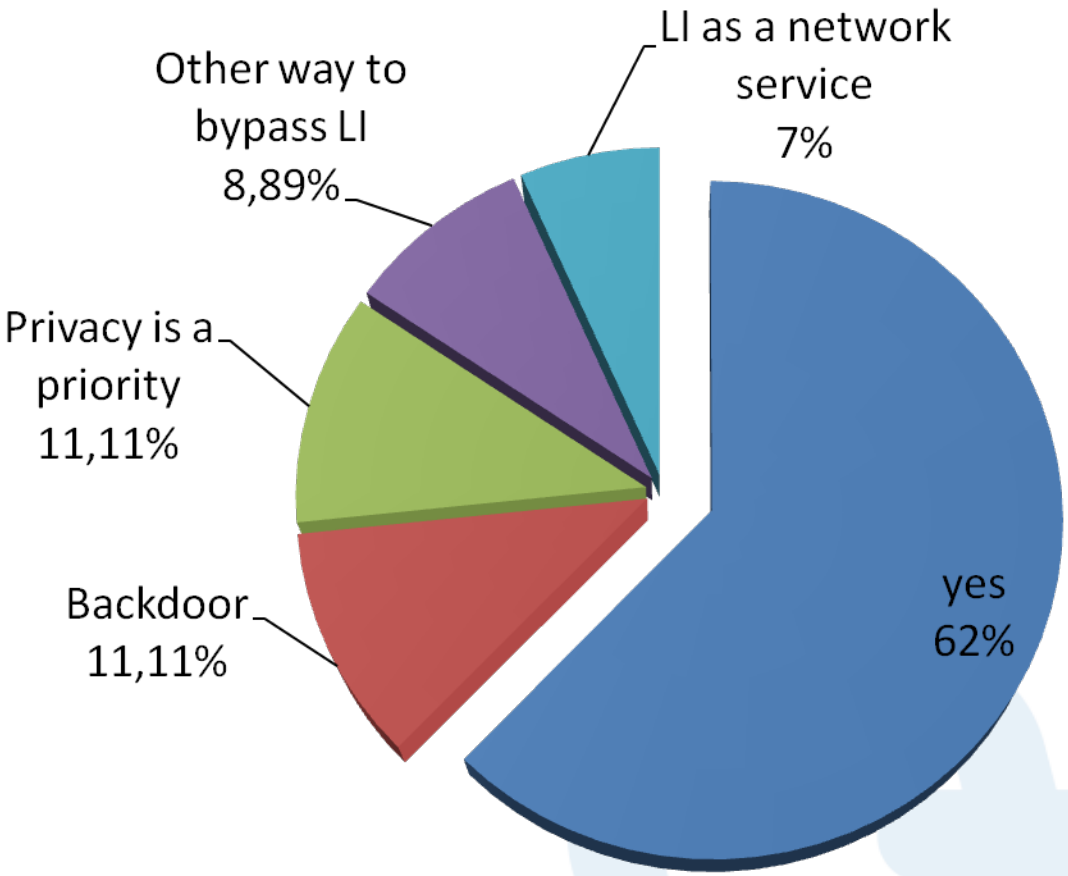
The biggest privacy challenges in 5G network are:



- Give user control over user data
- Provide end to end data confidentiality
- Provide privacy-aware Lawful interception and Data retention
- Counteract privacy violation by mobile malware
- Counteract user tracking
- Provide privacy protection in IoT scenarios

e2e data confidentiality & user control together with privacy aware LI

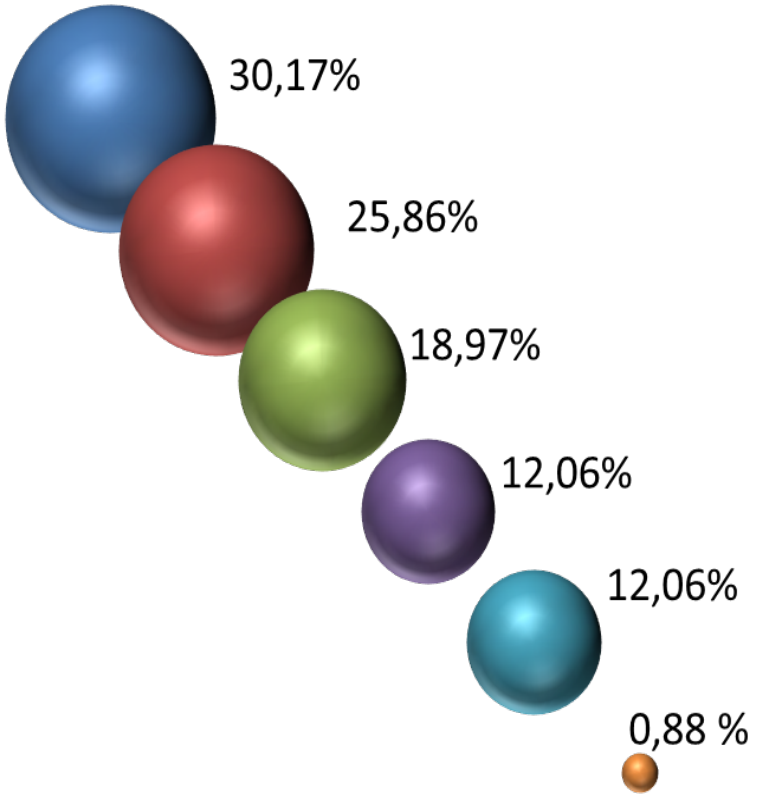
Privacy and anonymization techniques shall also provide built in data recovery capabilities for LEA



Anyway lot of respondents express several concerns for possible abuse

5G Trust

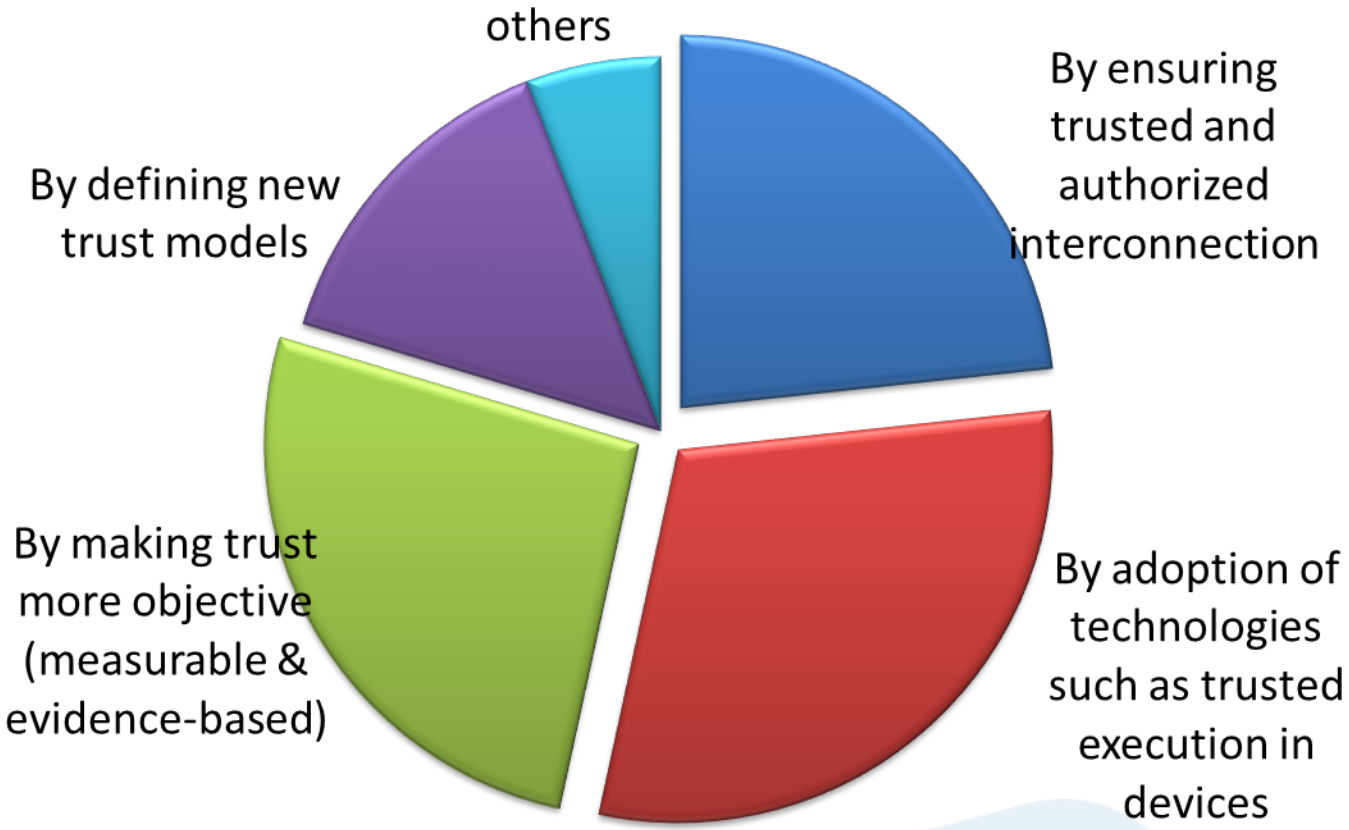
Trust complexity in 5G networks is mainly due by:



- The support of new business models with new actors and new relationships
- The adoption of virtualisation technology e.g. third party VNFs running inside 5G network
- The support of new "devices" e.g. sensors nodes
- Massive adoption
- The lack of definition and adoption of a common trust model
- Verifiability (both in terms of machines and humans)

The adoption of new business models & the use of virtualization technology

Trust in 5G network can be built by:



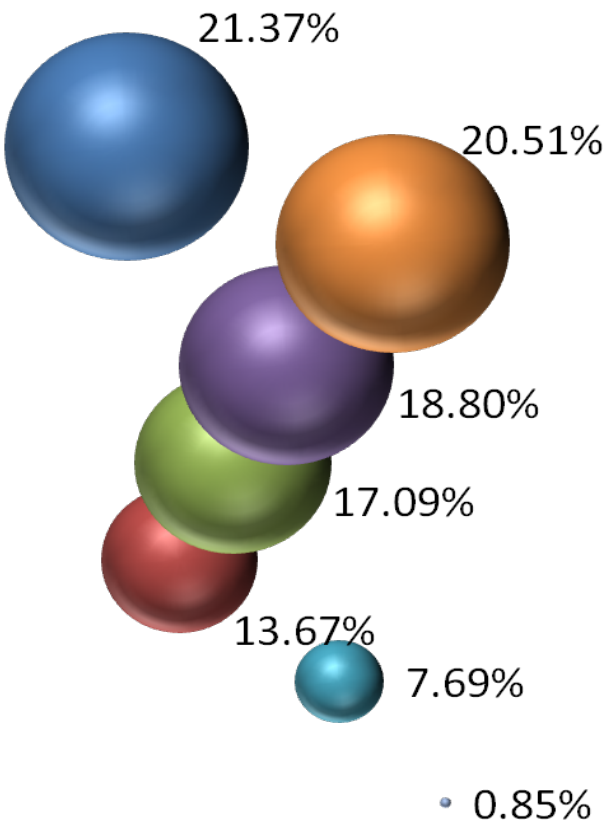
- **Adopting technology such as trusted execution environment (TC).**
- **Making trust more objective**
- **Ensuring trusted and authorized interconnections**

5G virtualization and multi tenant environment

Respondents to our open consultation were asked to indicate:

- The relevant issues raised by the adoption of virtualization
- The relevant security risks raised by a multi tenant environment
- The requirements needed to ensure security in multi-tenant virtualization scenarios

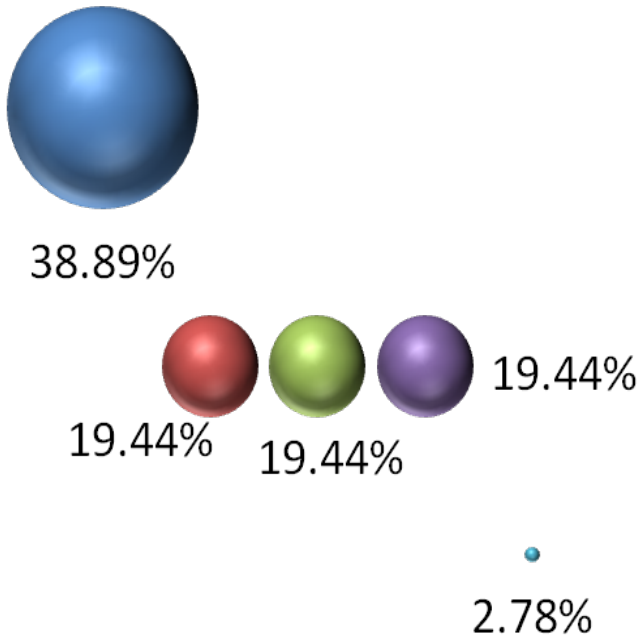
The adoption of virtualization raises security concerns in terms of:



- Lack of logical and physical isolation between distinct virtual network functions
- Potential impact of vulnerabilities which can affect the segregation of virtual instances
- Lack of authentication between the virtual functions
- Issues related to interoperability with legacy networks (3G, 4G)
- Starvation of resources allocated to virtual network function with the intent to create DoS
- Integrity of Virtualization Platform
- Others

- **Lack of logical and physical isolation between virtual network functions**
- **Integrity of Virtualization Platform**

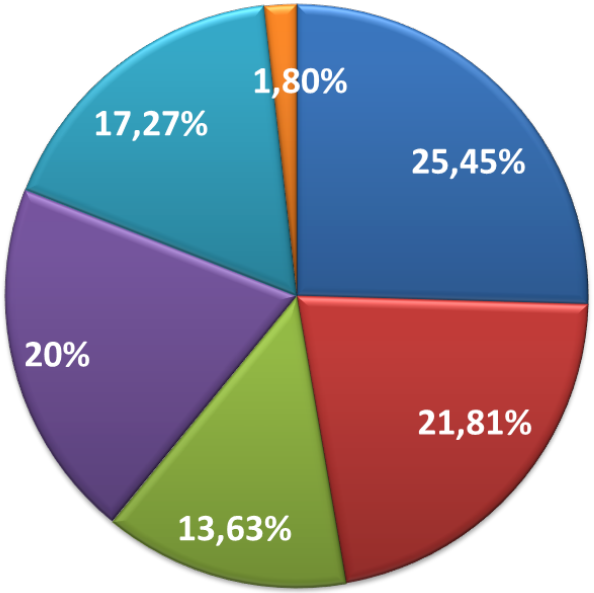
Multi-tenant environment raises security concerns mainly in term of:



- Data confidentiality and integrity due by lack of isolation
- Performance and availability risks based on the activities of other tenants on the same infrastructure and platforms
- Side channel attacks due to lack of authorization mechanisms for sharing physical resources
- Uncoordinated change controls and misconfigurations (i.e. one tenant to gain access to another tenants data or resources)
- others

data confidentiality and integrity due by lack of isolation

Security in 5G virtualization and multi-tenant scenarios can be provided:

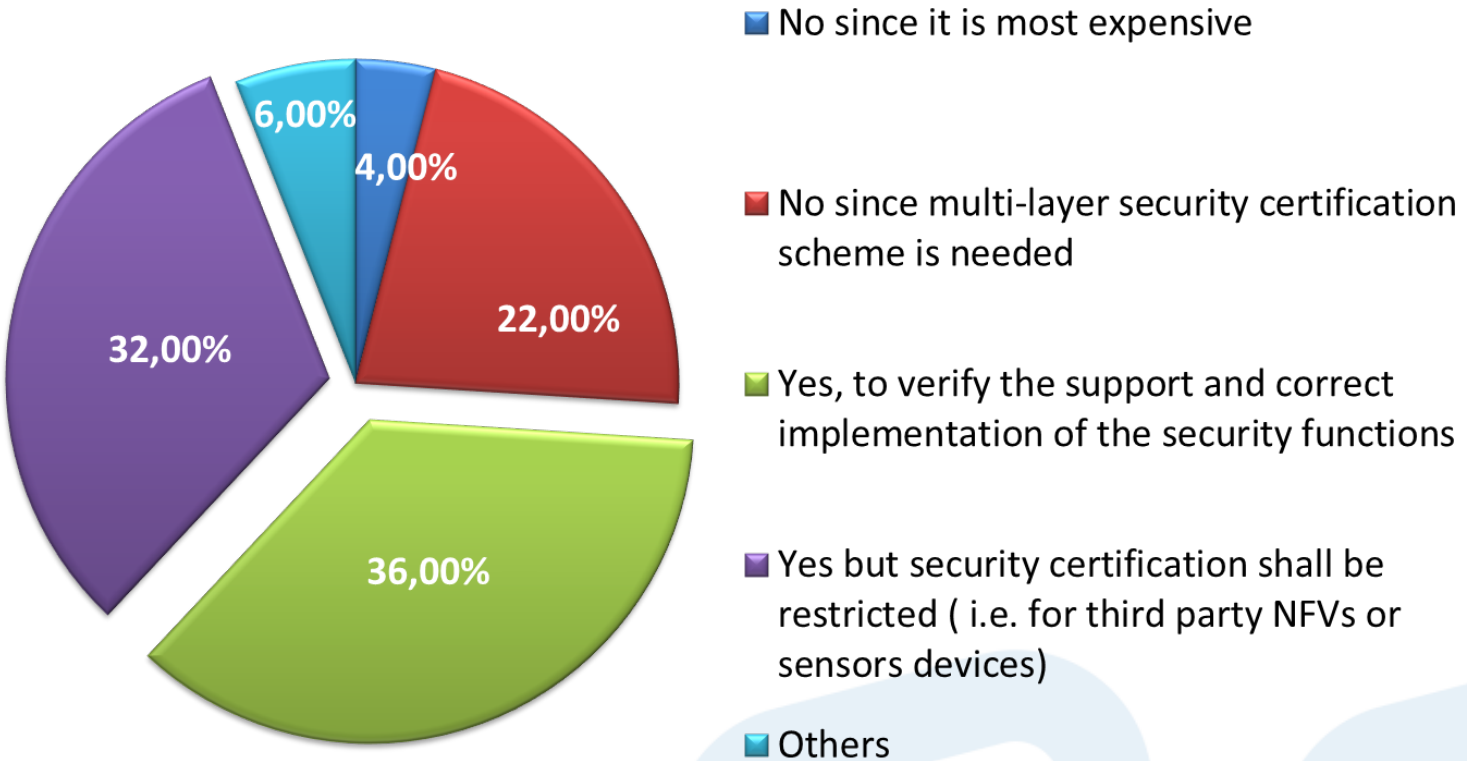


- By relying on properly implemented isolation at virtualization layer
- By implementing monitoring mechanisms to control the allocation of virtual network functions to physical computing resources
- By implementing mechanisms able to ensure traffic types segregation, e.g. between data, control and management planes
- By providing a capability to verify the integrity and confidentiality of images of virtual network function implementations, at start-up as well as run-time
- By implementing access control mechanisms to limit the reachability/visibility of the VNF components
- Others

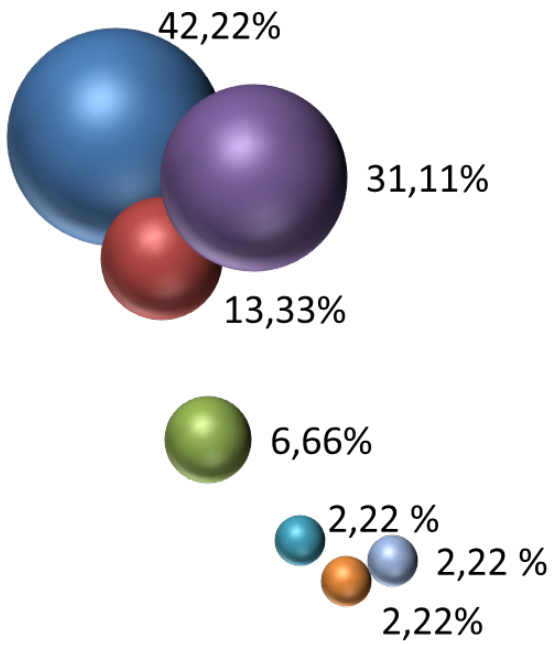
- **Properly implemented isolation at virtualization layer**
- **Verification of VNFs integrity**
- **Monitoring mechanisms to control the allocation of virtual network functions**

5G Certification

74% of respondents think that Security Certification in 5G network is needed



Security assurance can be provided by:

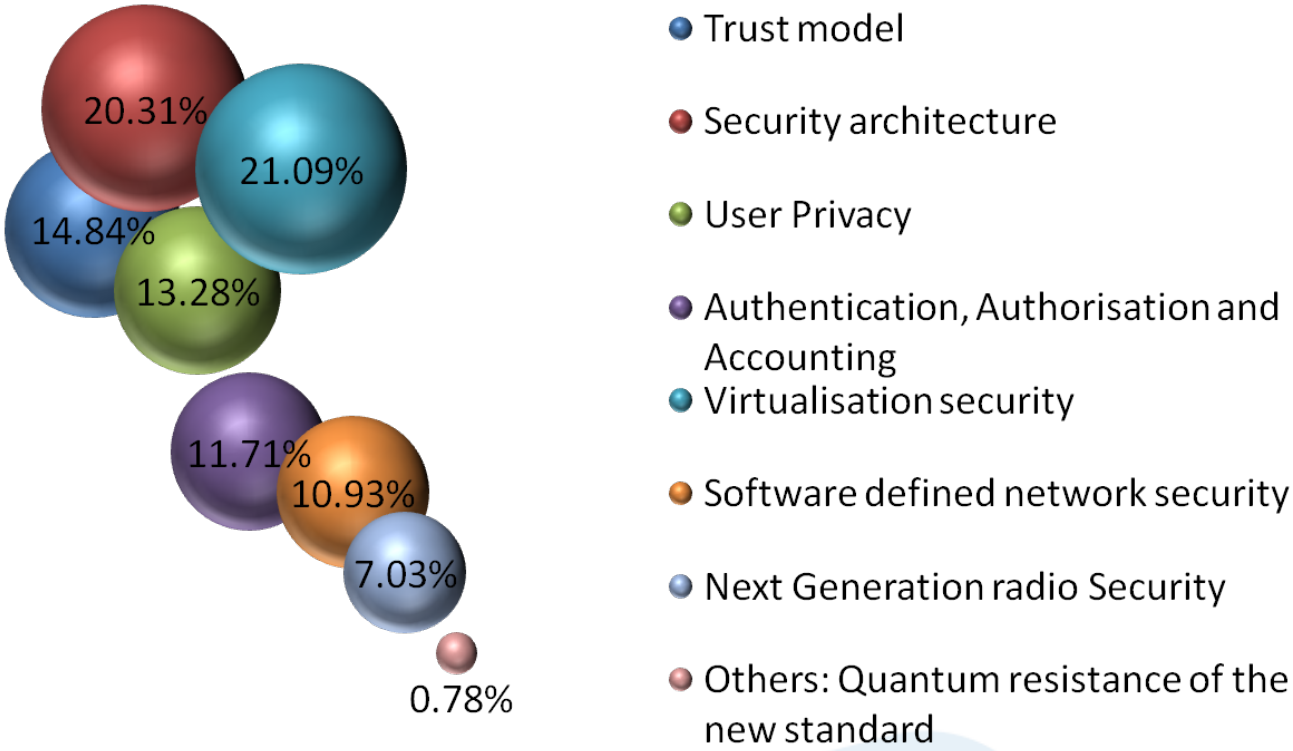


- By use of Trusted Computing techniques (i.e., Root-of-Trust, Attestation, and Secure Storage)
- By requiring security certification
- By shared responsibility agreements
- By creating a security assurance standards to be applied, recognized, and accepted
- right architecture
- Verifiable computing in addition to trusted computing
- by introducing bnew security concept based on Physical Layer Security (Secret Key Generation, Secrecy Coding)

Trusted computing techniques and security assurance standard

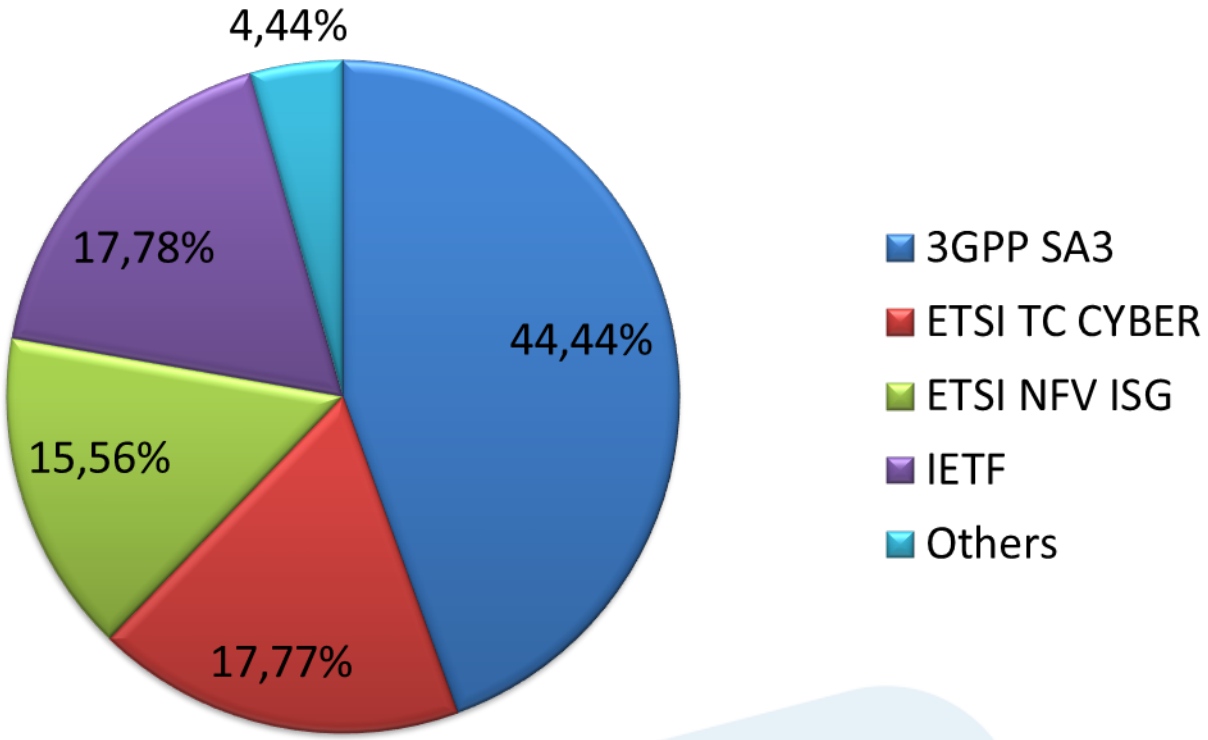
5G Standardization

5G standardization work should focus on:

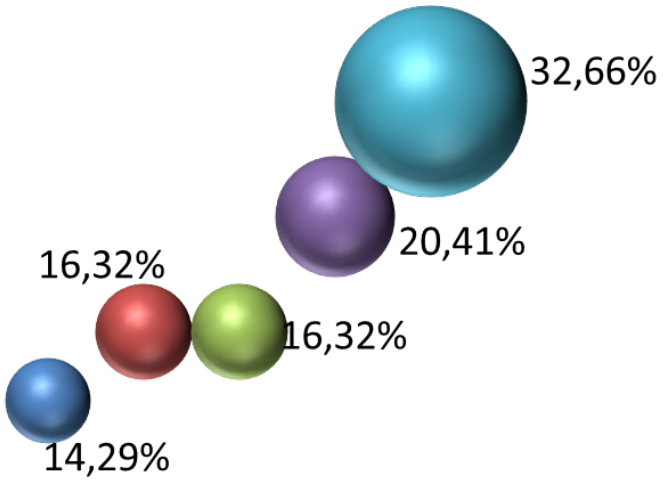


Security architecture and Virtualization security, followed by the Trust model and Privacy

3GPP SA3 is the Key SDOs for 5G security



Standardization effort should be put on the definition of the security architecture that takes into account innovative security solution for emerging 5G technology



- 5G use cases identified as relevant for security and privacy point of view
- Security and privacy requirements derived from 5G use cases analysis
- Improvements and replacements of known insecure protocols
- New innovative and promising security solutions for emerging 5G technologies
- Definition of the 5G security architecture

Conclusions and key findings (1/2)

- **Trust, AAA, Privacy, Security Monitoring, Network Management and virtualization are relevant area for 5G security**.
  - 5G-ENSURE project has identified these areas as enablers for 5G Security and is working in defining innovative solutions

- **Privacy in 5G** should provide end-to-end data confidentiality and increase user control.

- **Trust in 5G** shall be built by the adoption of trusted computing technology at device level.

- **Security certification** is required to provide security assurance in 5G network.

- **Security in multi tenant virtualization scenarios** requires isolation and monitoring mechanisms to avoid abuse

Conclusions and key findings (2/2)

- **Standardization** shall focus on the **security architecture definition**.
  - 5G-ENSURE project is defining a 5G reference security architecture shared and agreed with various 5G stakeholders, and able to support the initial set of security enablers specified within the project..
- **3GPP SA3** is the key SDO for 5G security.
  - 5G-ENSURE standardization plan considers 3GPP as one of the main target SDO

5G Ensure

5G Enablers for network and system security and resilience

5G-ENSURE: http://www.5gensure.eu

contact@5gensure.eu

@5GEnsure

5G ENSURE receives funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562 | Duration November 2015 – October 2017

The 5G Infrastructure Public Private Partnership (SG PPP)