

GRUPPO TELECOM ITALIA

5G Secure

June 16 2016

# The role of security in 5G standards: a look at ITU-T and an ETSI example

Luca Pesando



# Agenda

ITU-T FG IMT2020 overview


FG workplan, activities and outcomes

Security aspects in FG IMT2020

ETSI WG M493 and security

The common points

# Overview of 5G in ITU-T: FG IMT2020

- Created one year ago by SG 13 (Future networks including cloud computing, mobile and next-generation networks)
- Mandate: individuate the gaps in standards that need to be filled, by ITU-T in particular, for the 5G to become reality
- Short term mandate: outcome expected by the end of 2015   
  - 4 meetings in 6 months for completion of the Gap Analysis document
  - Presentation and approval of the document at the SG13 plenary in december
  - Proposal of new ToR for a phase 2, extending till the end of 2016 WTSA- (hard deadline) approved as well

Work focusing mainly on (fixed) network aspects relevant to SG 13

# Phase 1 and Phase 2 outcomes

- Gap analysis of existing technologies wrt 5G requirements done in the following 5 areas:
  - High Level Architecture
  - Network 'Softwarisation'
  - New Networking Technologies (ICN/CCN)
  - Front/Back Haul (FH/BH)
  - End-to-end QoS
- Total of 85 gaps identified (even if with some overlaps)

Minimum Target: prepare the ground for follow up activities in the relevant ITU-T SGs and the development of recommendations in

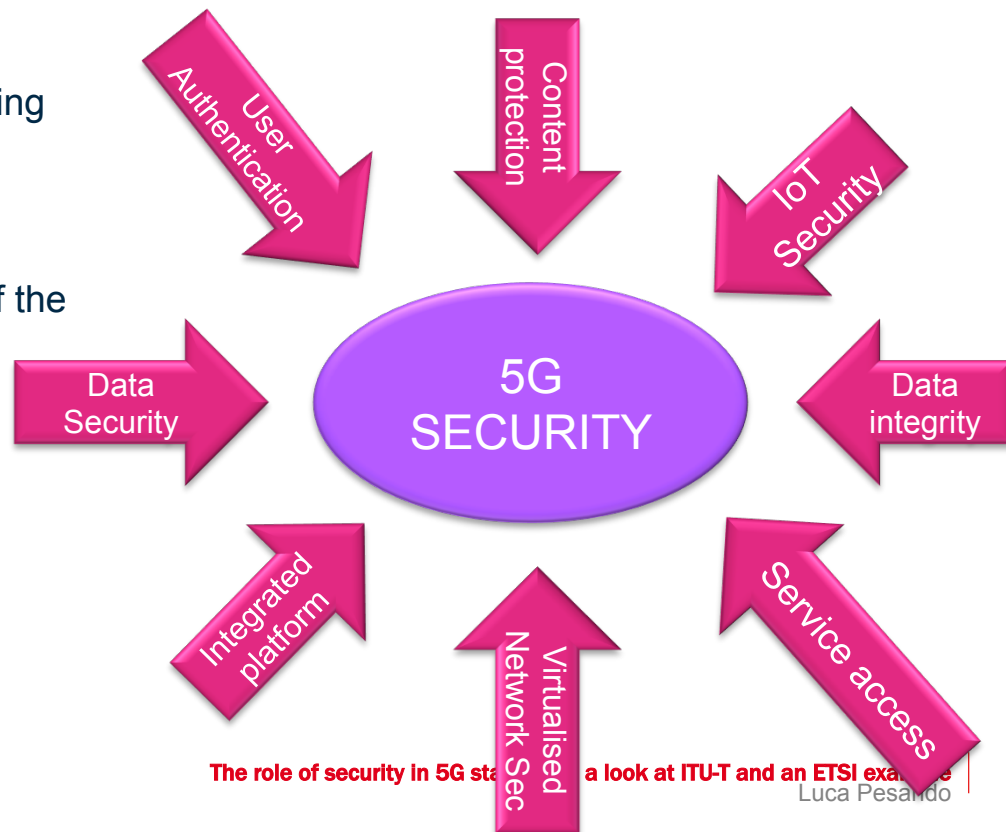
those

- For phase 2 The ToR for the FG have been revised and they include the development of Draft Recommendations

Address the GAPS of phase 1 to move towards solutions in phase 2

# Security in FG IMT 2020

- There is no specific WG on security
- Security aspects are addressed by the existing groups as a part of their activity
  - No comprehensive view
  - Focus on specific parts in the scope of the WGs



# Security aspects addressed by the FG IMT 2020

Virtualised Network  
Management Security

Unified OSS: who is  
in control, how to  
assign rights and  
credentials

- Increase of the number of players
- IEEE, 3GPP, TMF, NGMN, ...
- Infrastructure management

Single Authentication

Allow the subscriber a  
simplified access to  
different services of  
interest (phone, mail,  
video, IoT related)

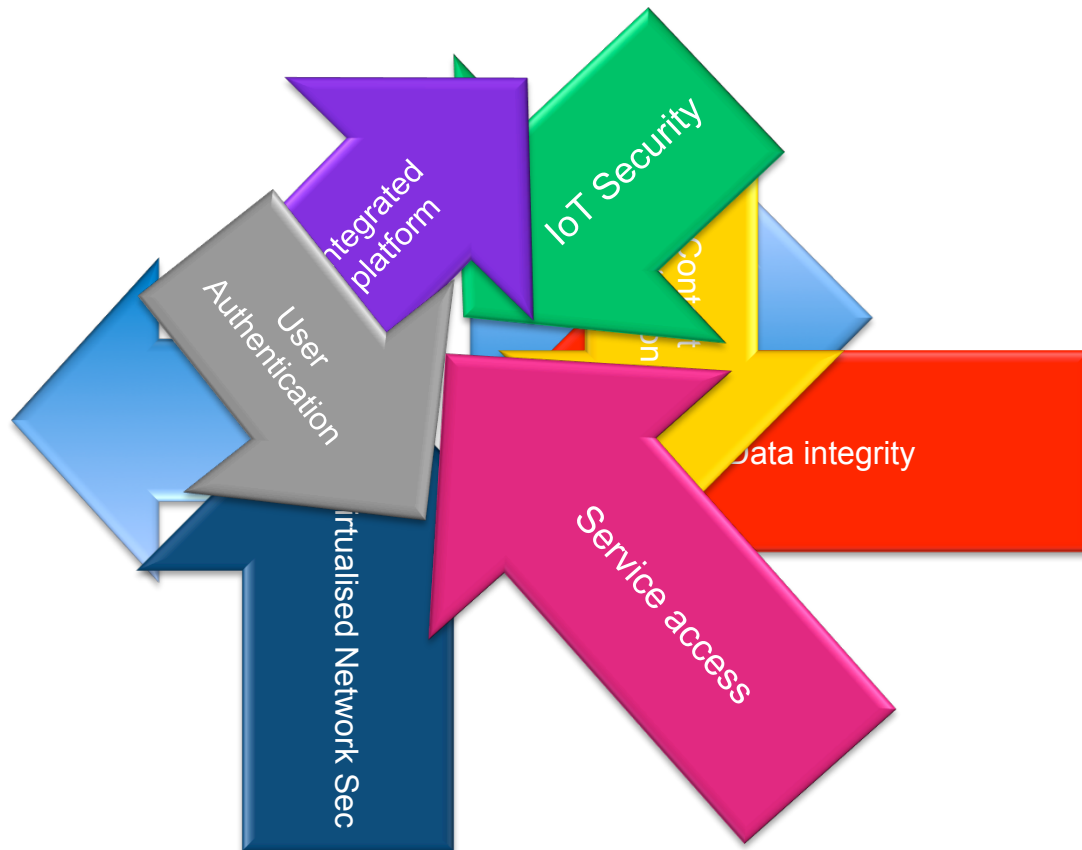
- USIM, eSIM, MIFARE, NO SIM..?
- ETSI, 3GPP, NGMN, GSMA ...
- Infrastructure business

Stream Encryption/App  
protection

Make session security  
higher and  
implementation lighter

- Referring to existing tech
- IRTF
- Manifests to protect Apps

# Need for a rational approach!



# A step back .... EC Mandate 493 in ETSI

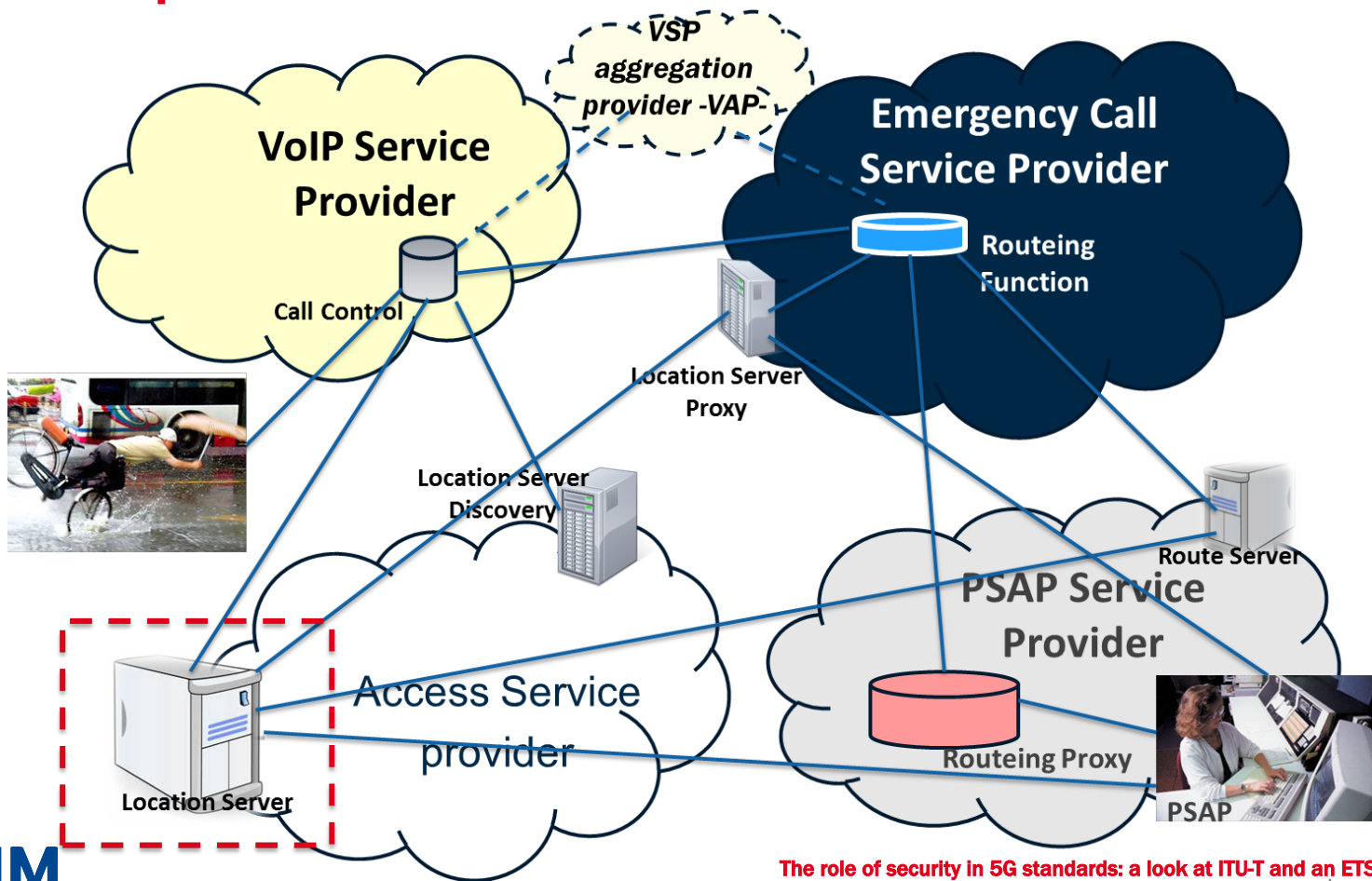
- Mandate 493 was issued in 2011 – group created
- It requests to provide a standard to extend the support of **caller location** to **VoIP calls**
- The solution must be for deployment today (2011!!) and must work with the existing PSAP and emergency service implementations (POTS in many cases)
- But...It must be as much as possible future proof
- Security and privacy are of course of top importance

Balance between security and access openness  
Involve several players collaborating to provide the service

- After a troubled path, the Architecture has been finalised, now working at protocol definition, aiming at a state of art solution that works with current and new generations



# M493: the picture



# M493 in ETSI – the essential aspects about security

- The solution provided is based on protocols that are defined for and adopted in the networks
- As for most of 5G applications there is a variety of players with different interests:
  - Traditional network operators and OTT, and other service operators specific to emergency services – Market opening creates many new roles
- Information has to be accessed by other parties besides the original owner
- Security must be guaranteed both from the end user's standpoint and the provider's
- The final user's interest can be in contrast with the correct management of information from a public interest perspective (e.g privacy)
- Regulation plays a very important role

All of the considerations above apply in the 5G scenario: the balance between contrasting interests is very important and it is what security standards need to take care of to be effective

Thank You

