Hochschule
München
University of
Applied Sciences

M5GA
6G – making 5G great again?

Alf Zugenmaier

Hochschule München

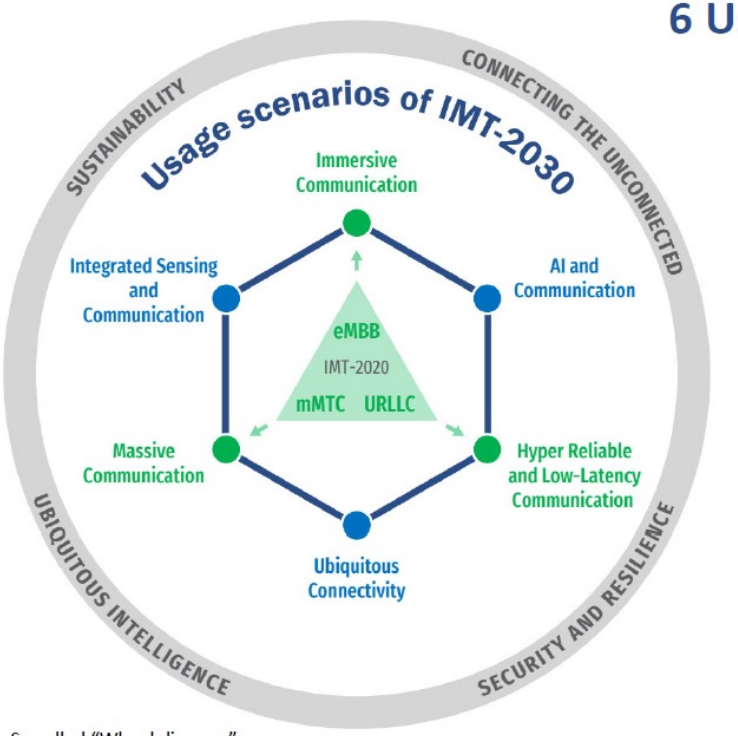
Agenda

- 6G
- Security design in 5G
- Problems in security standardization
- Take away for 6G standardization

6G

- IMT 2030 framework (June 2023)

Usage scenarios



So called "Wheel diagram"

6 Usage scenarios

Extension from IMT-2020 (5G)

- eMBB ➡ Immersive Communication
- mMTC ➡ Massive Communication
- URLLC ➡ HRLLC (Hyper Reliable & Low-Latency Communication)

New

- Ubiquitous Connectivity
- AI and Communication
- Integrated Sensing and Communication

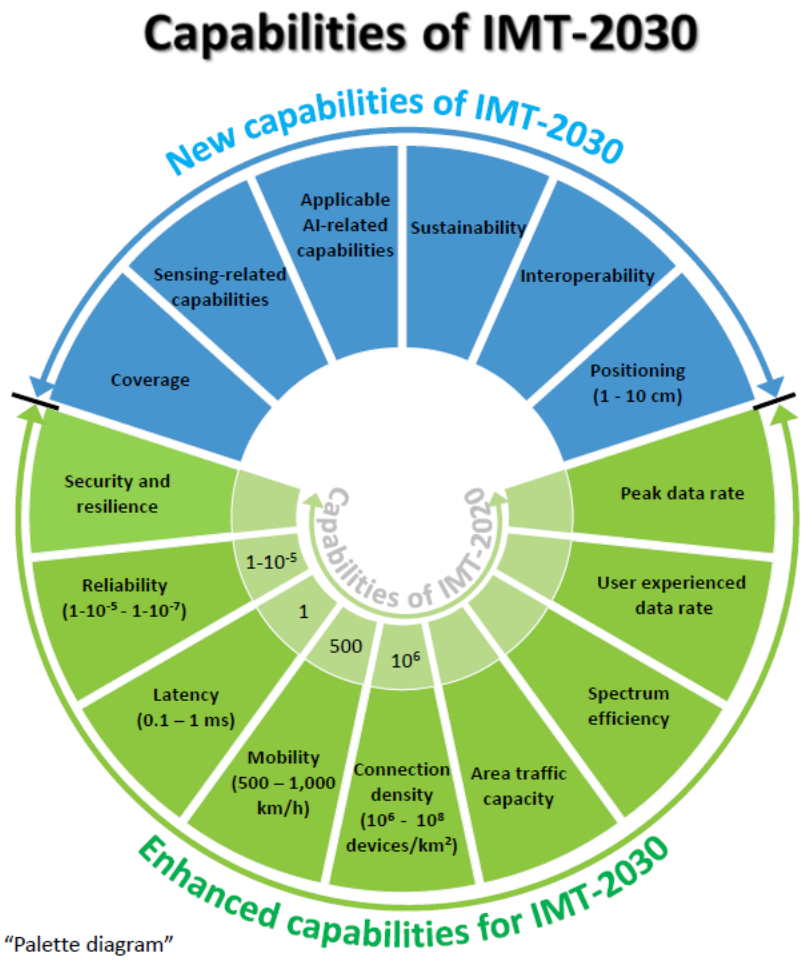
4 Overarching aspects:

act as design principles commonly applicable to all usage scenarios

Sustainability, Connecting the unconnected,
Ubiquitous intelligence, Security/resilience

https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx

6G



So called "Palette diagram"

The range of values given for capabilities are estimated targets for research and investigation of IMT-2030.

All values in the range have equal priority in research and investigation.

For each usage scenario, a single or multiple values within the range would be developed in future in other ITU-R Recommendations/Reports.

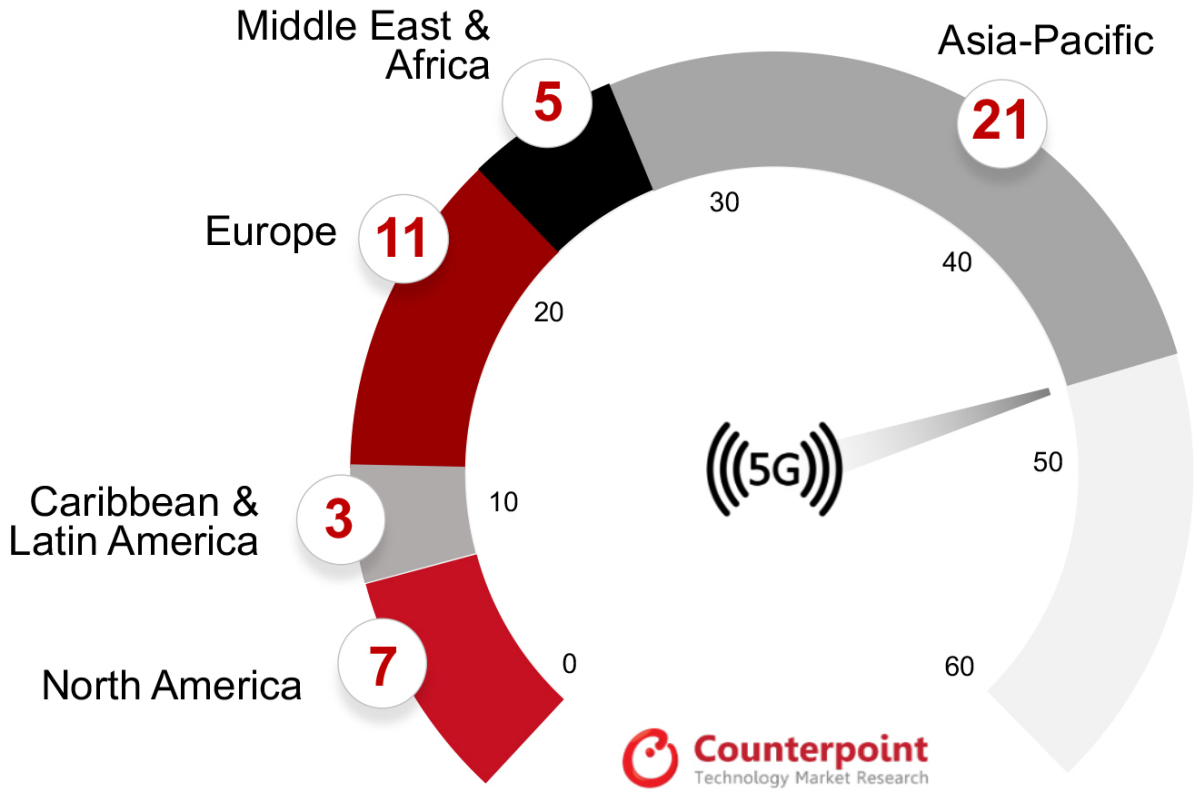
https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx

6G – a natural evolution of 5G

- More of the same!?

Seriously?

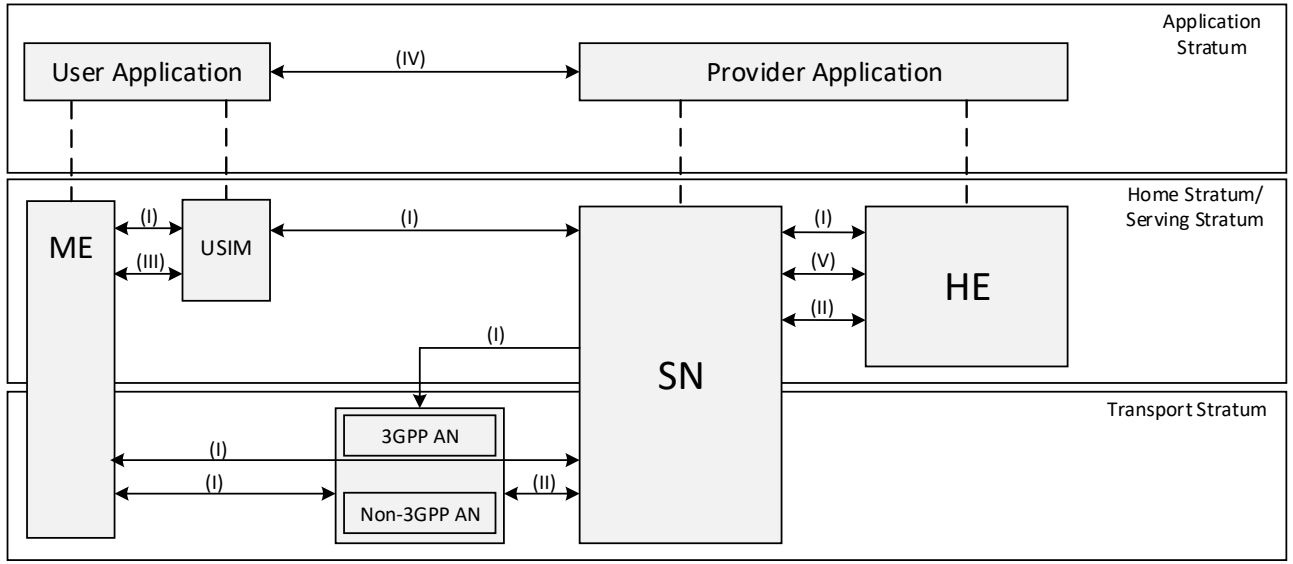
Extended due to great success?
5G Standalone rollout



https://www.counterpointresearch.com/insights/5g-sa-core-deployments-2023/

Security architecture in 5G

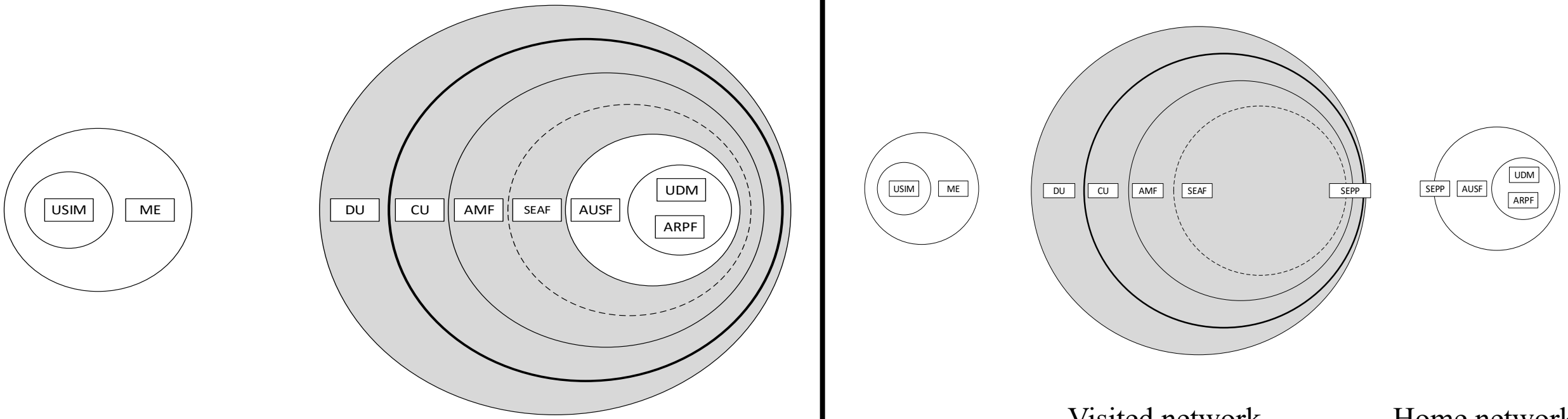
- End to end architecture?



- Application domain security is out of scope of the present document.

TS 33.501

Security domains within the operator network



Security problems
Example: ill defined trust model

Attackers inside operator domain?

- OAuth framework
- But no defined attacker model

Network slicing

- Resource isolation
- But common RAN network

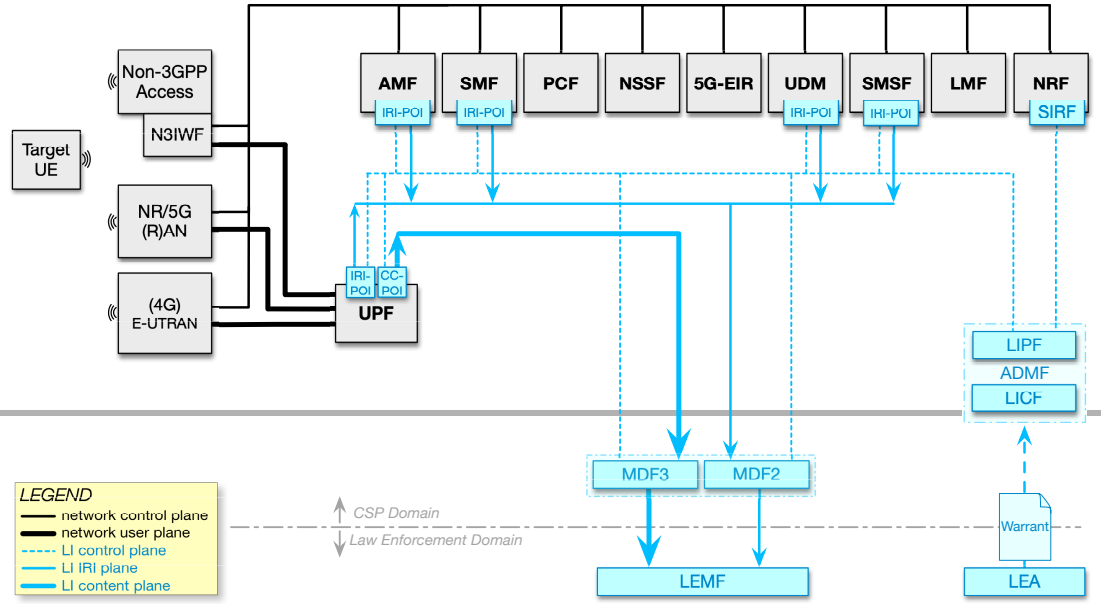
Know your enemy and know yourself
- Sunzi

https://de.wikipedia.org/wiki/Sunzi#/media/Datei:%E5%90%B4%E5%8F%B8%E9%A9%AC%E5%AD%99%E6%AD%A6.jpg

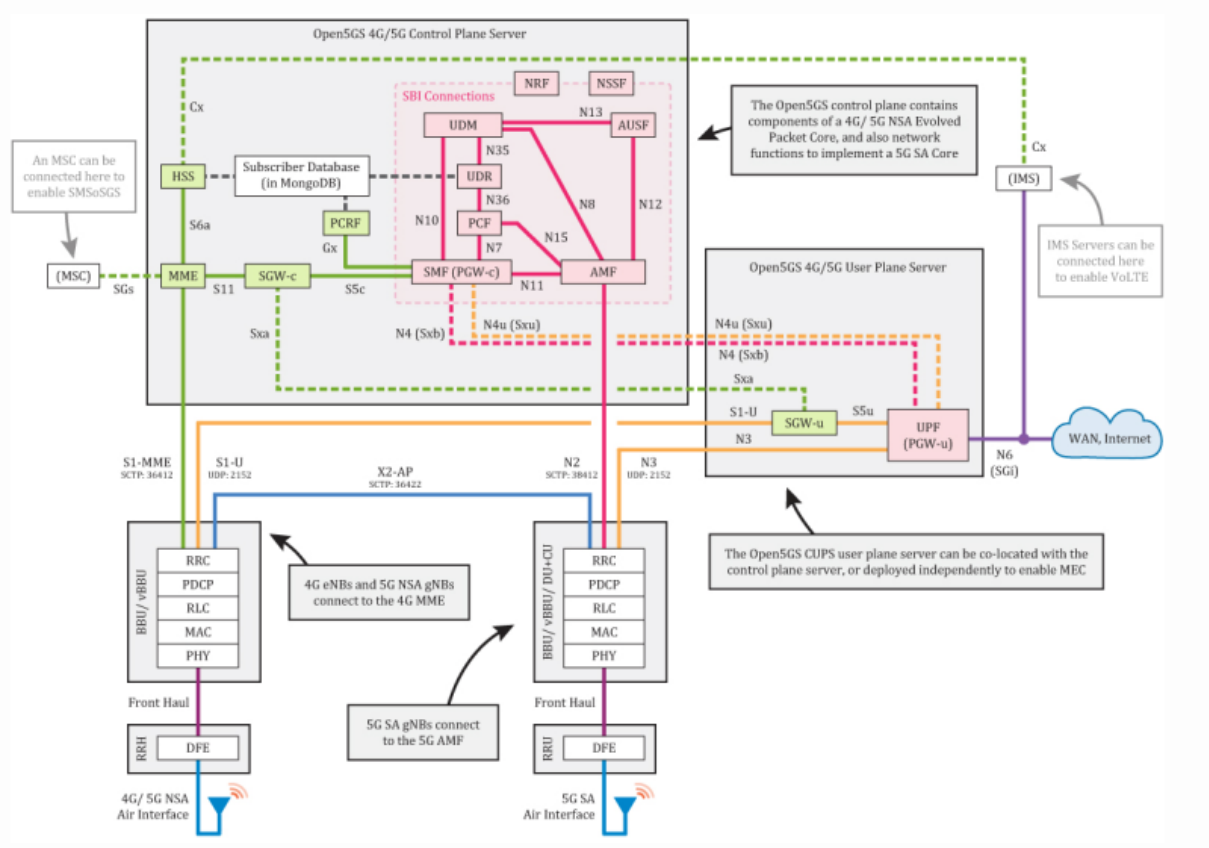
Regulatory requirements
Example – lawful intercept

- Unavailability of E2E security
  - Legal basis (e.g. Germany)
    - Privacy of telecommunications shall be inviolable
    - Restrictions only pursuant to a law

    → Telecommunications provider must have legal intercept capability
- Current discussion:
  - LI for authenticated keys in AKMA



Operational Complexity



Open source 5GS

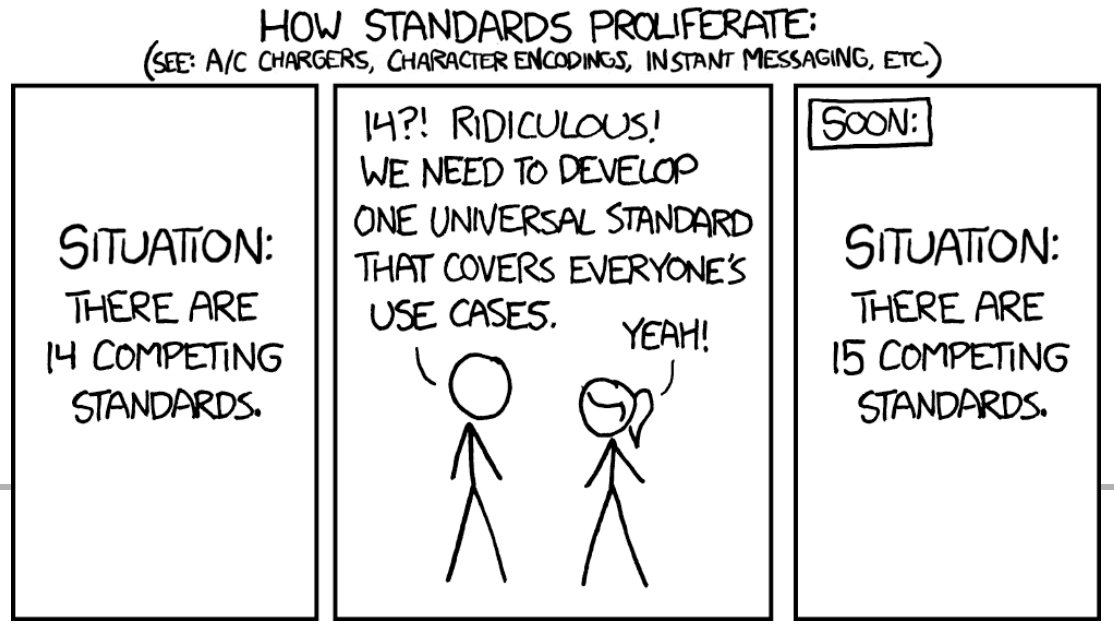
- Telecom grade deployment
  - For minimal network (2 gNBs)
  - >2000 Containers
  - Similar number of virtual networks
- Multiple management layers
  - Kubernetes
  - ETSI NFV
  - OAM
  - …

open5GS: https://open5gs.org/open5gs/docs/guide/01-quickstart/

Too many options:
Example – subscriber authentication in 5G

- Network access
  - 5G AKA
  - EAP AKA‘

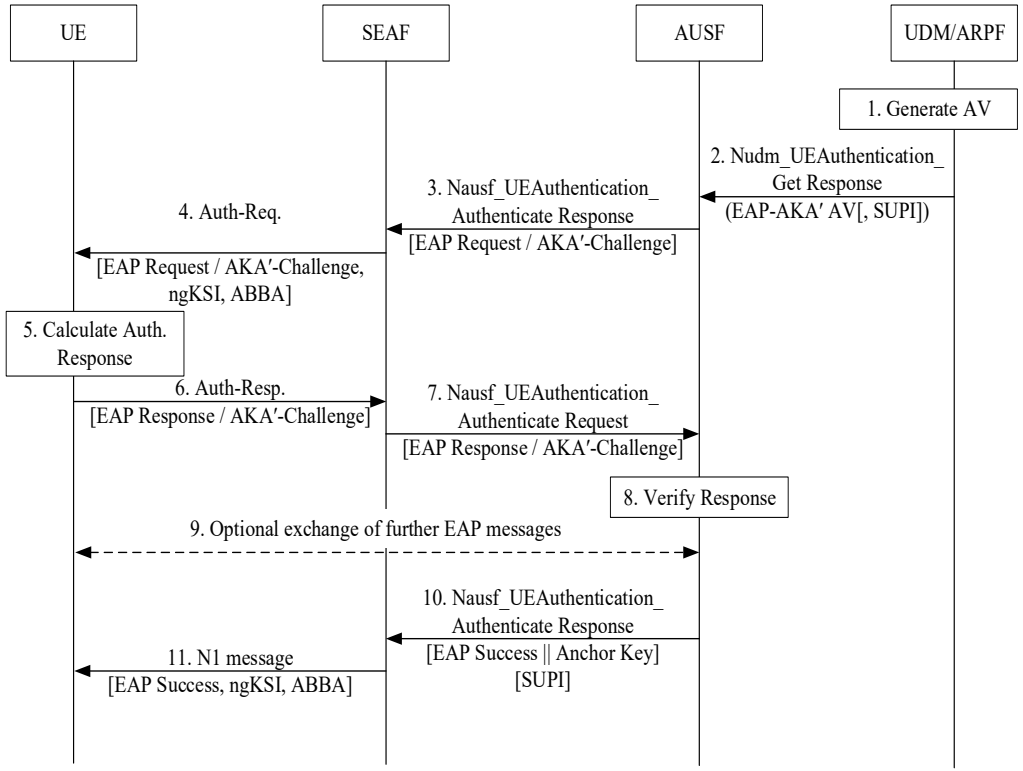
- Application layer
  - IMS AKA
  - GIBA (GPRS IMS bundled authentication)
  - GBA (available since 2007)
  - AKMA
  - MEC EEC client authentication (anything TLS)



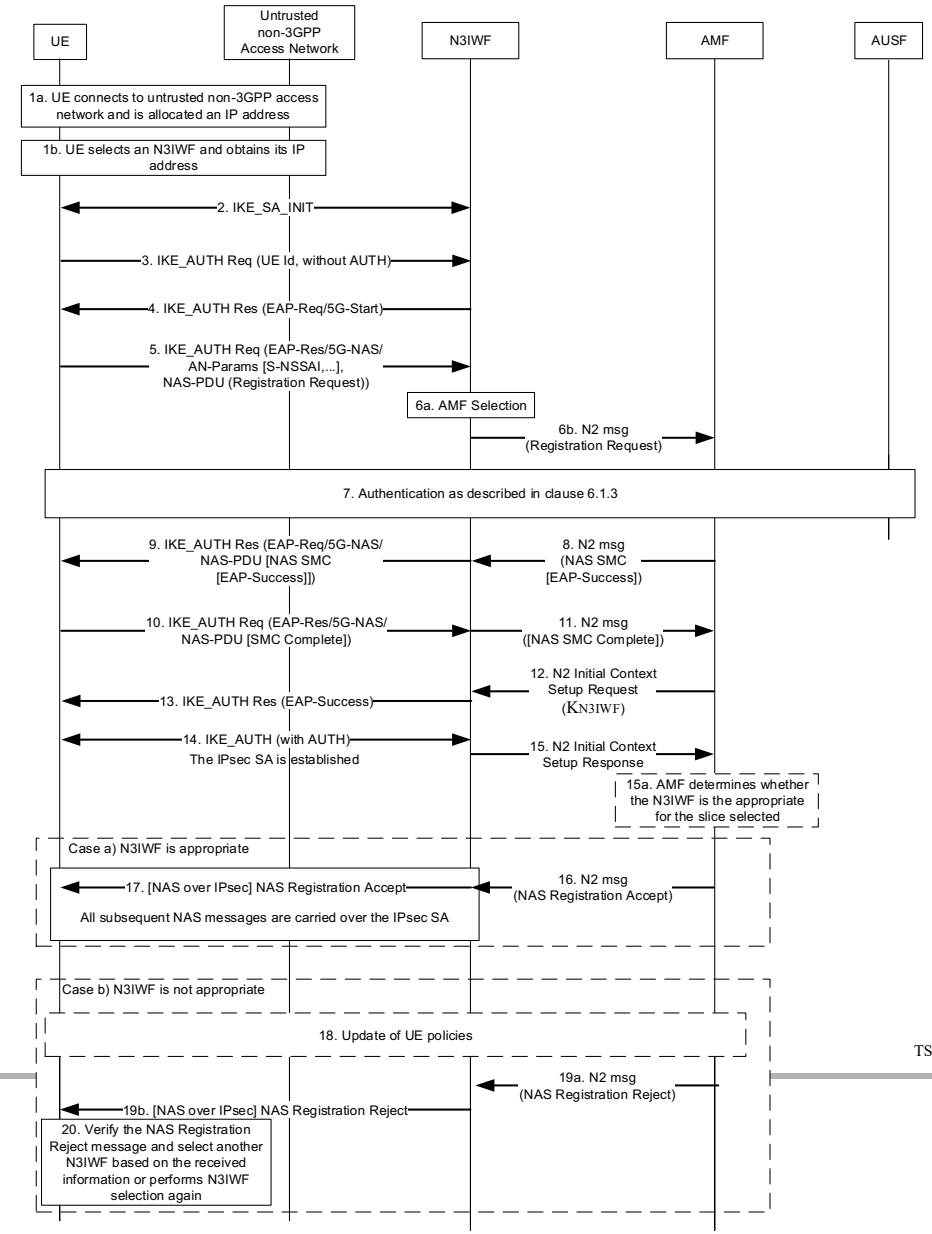
https://xkcd.com/927/

Complexity
Example: Access security

- 3GPP 5G access



- Non-3GPP access



TS 33.501

Incentives for standardization

- Global
  - Interoperability
  - Economy of scale
  - Competition more granular

- On individual level
  - IPR
  - KPI
    - „Leadership“
    - Accepted contributions

→ New solutions favoured → Complexity

So what could to be done for 6G?

- Lower complexity
- Clear requirements
- Re-use solutions and protocols
  - Lower complexity
- Clean interface to network services
  - Lower complexity
- Decouple verticals
  - Lower complexity
- Adapt incentives in standards
  - Lower complexity

→ Lower Complexity

Hochschule
München
University of
Applied Sciences

Questions?