

5G-ENSURE

Security Architecture

Alireza Ranjbar, Ericsson

Ghada Arfaoui, Orange

ETSI security week, 16th June 2017



5G Security Architecture - Overview

- ❑ A security architecture provides a high level overview of
 - ❑ involved entities,
 - ❑ its interactions and,
 - ❑ the trust relationships between them.

➡ Enhance security, privacy and resilience.
- ❑ Main idea: Extend 3GPP security architectures of 3G/4G to capture new technologies, use cases, trust models and features of 5G networks.



Limitations in 4G Architecture (TS 33.401)

Two main concepts: **Domain** and **Stratum**.

Like to build on proven concepts but...

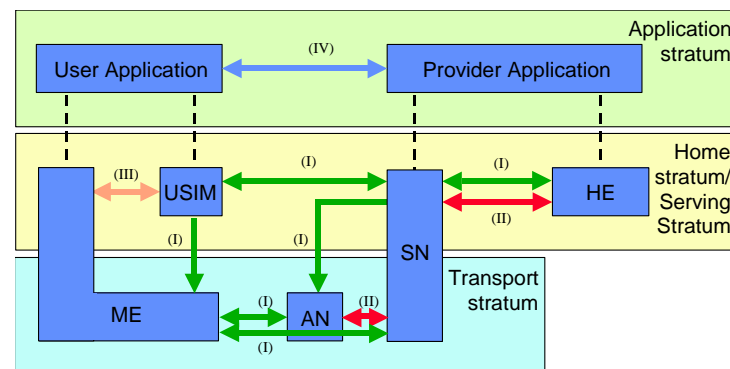
Trust relations are not reflected

Relevant 5G use cases and business models are not captured.

Technical issues:

Management aspect is omitted.

Service delivery models (i.e., Virtualization and Network slicing concepts) are not visible.



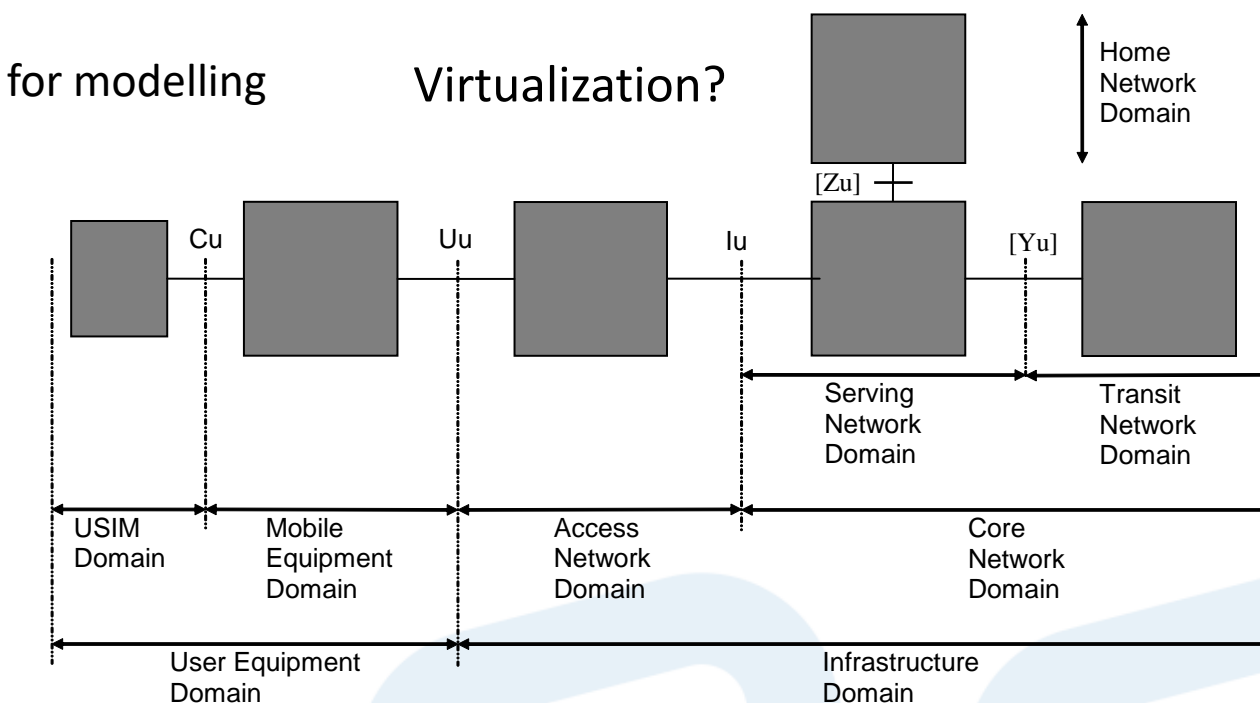
Domains (TS 23.101)

Domain: The highest-level group of physical entities. Reference points are defined between domains.

Better starting point for modelling trust!

But some gaps....

Slicing?



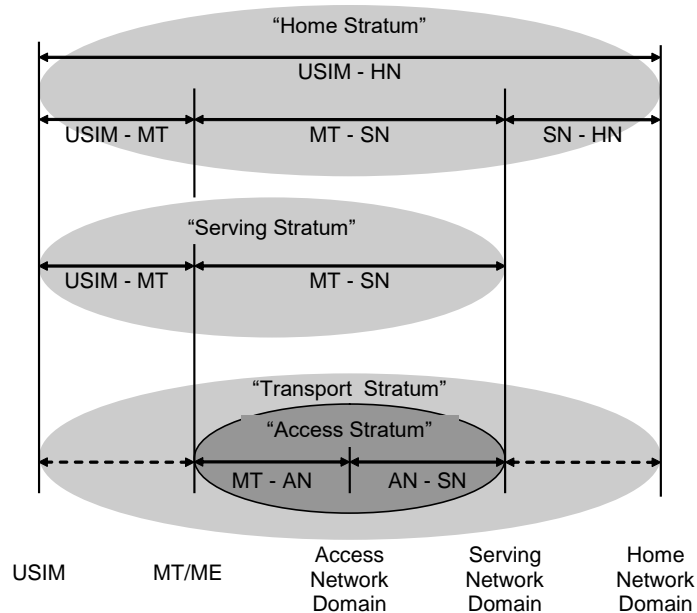
Management?

In 5G, may have several Infrastructure domains from different providers,

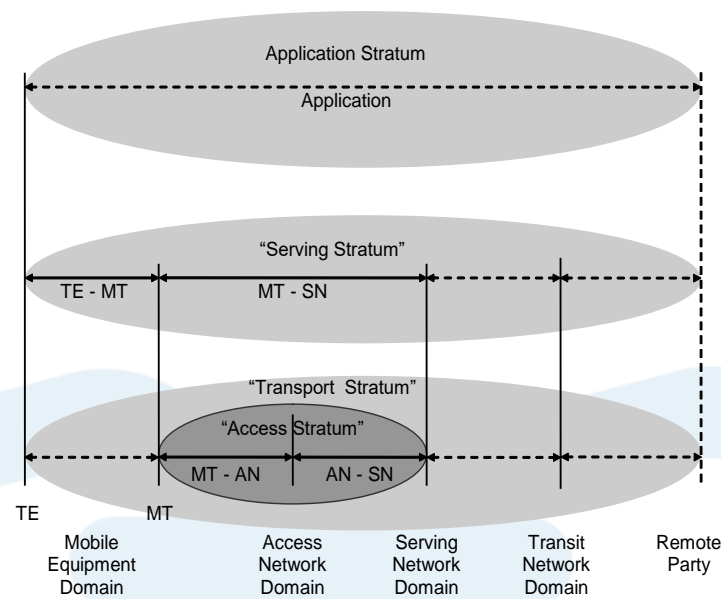


Stratum (TS23.101)

A **stratum** is a grouping of protocols related to one aspect of the services provided by one or several domains.



Management?

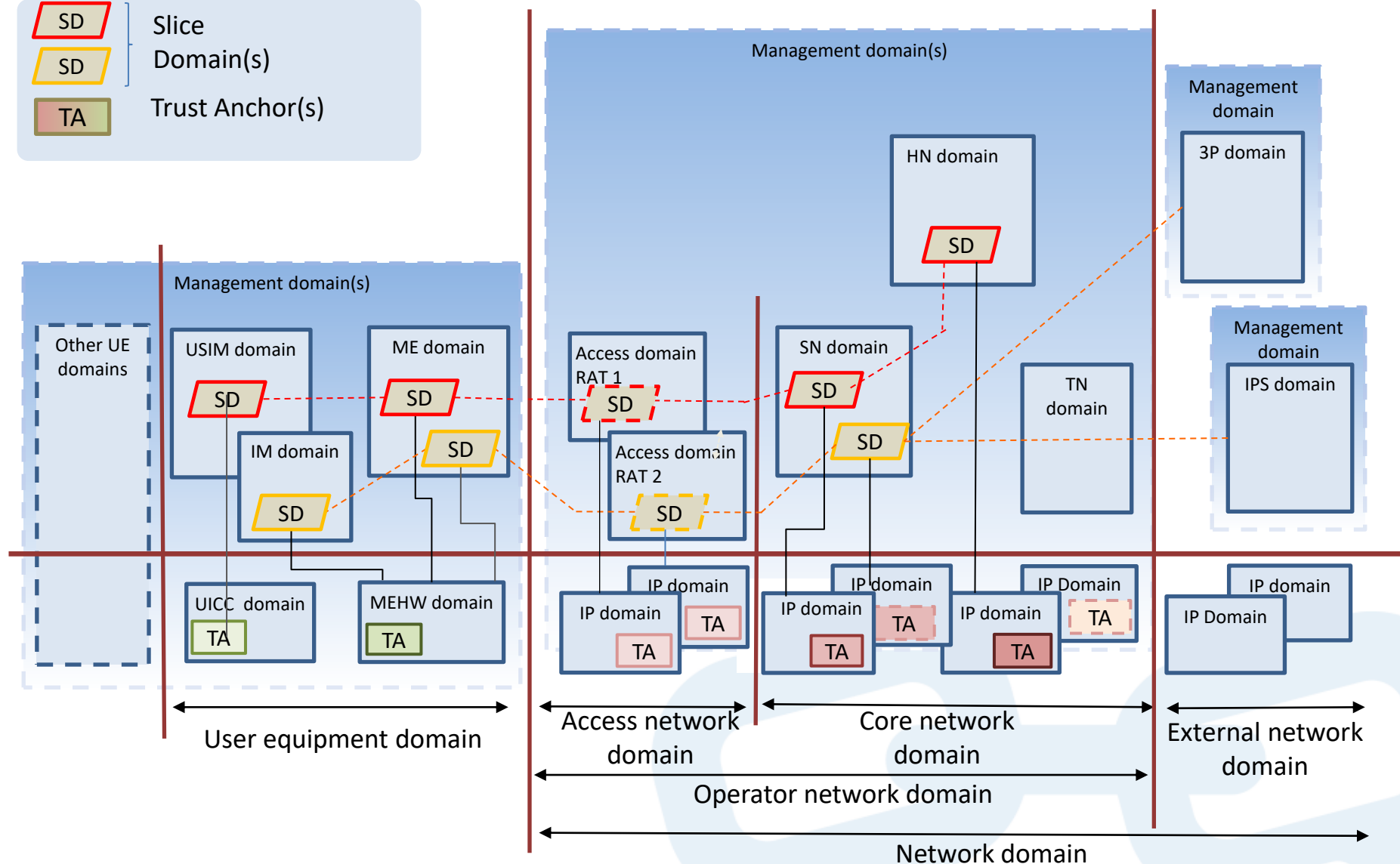


5G domains and strata - Definitions

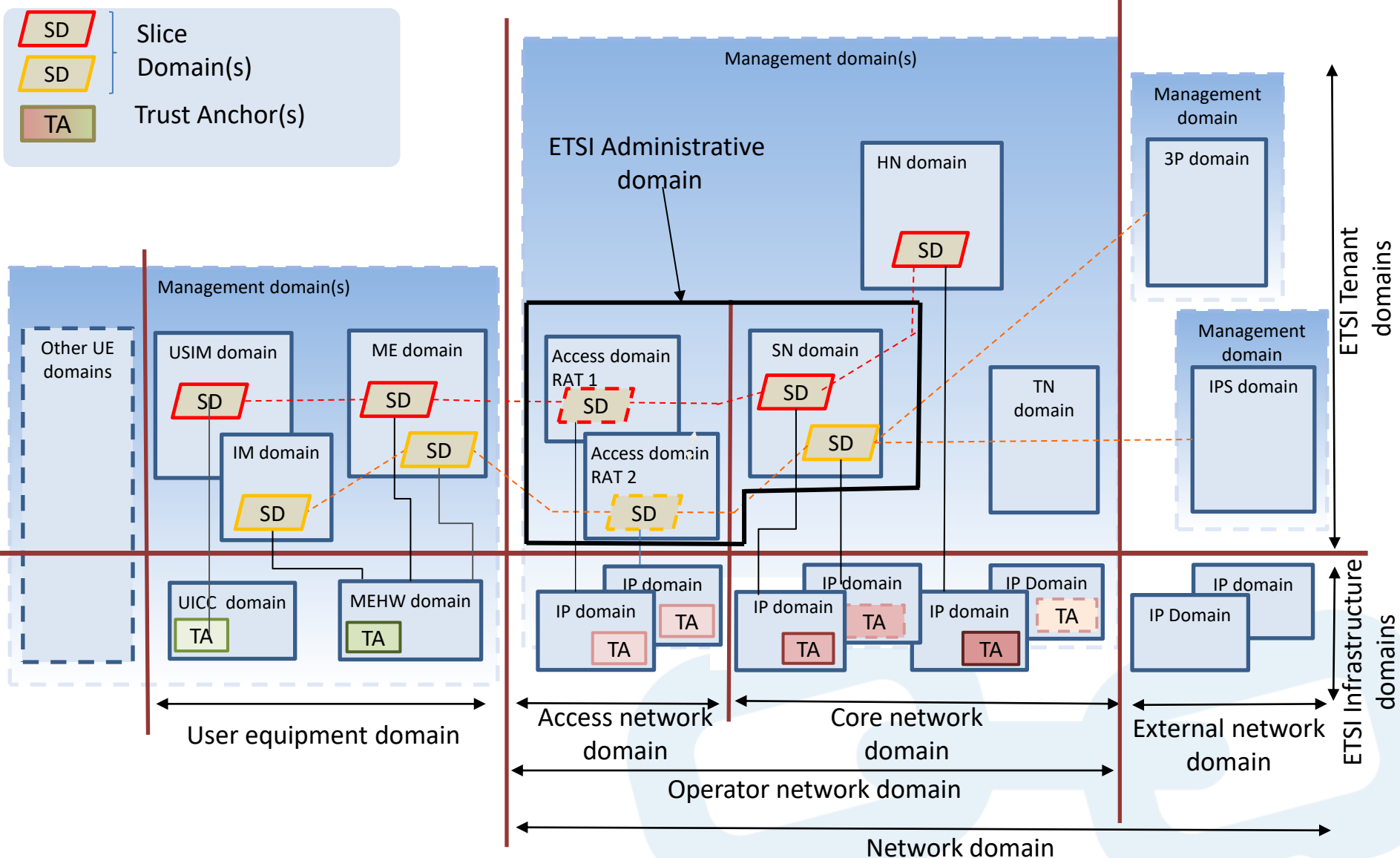
- ❏ A **domain** is a grouping of network entities according to **physical or logical** aspects that are relevant for 5G networks.
- ❏ A **Compound domain** is a collection of other domains, grouped together according to some 5G relevant aspect, e.g. ownership, joint administration.”
- ❏ A **stratum** is a grouping of **protocols, data, and functions** related to one aspect of the services provided by one or several domains.



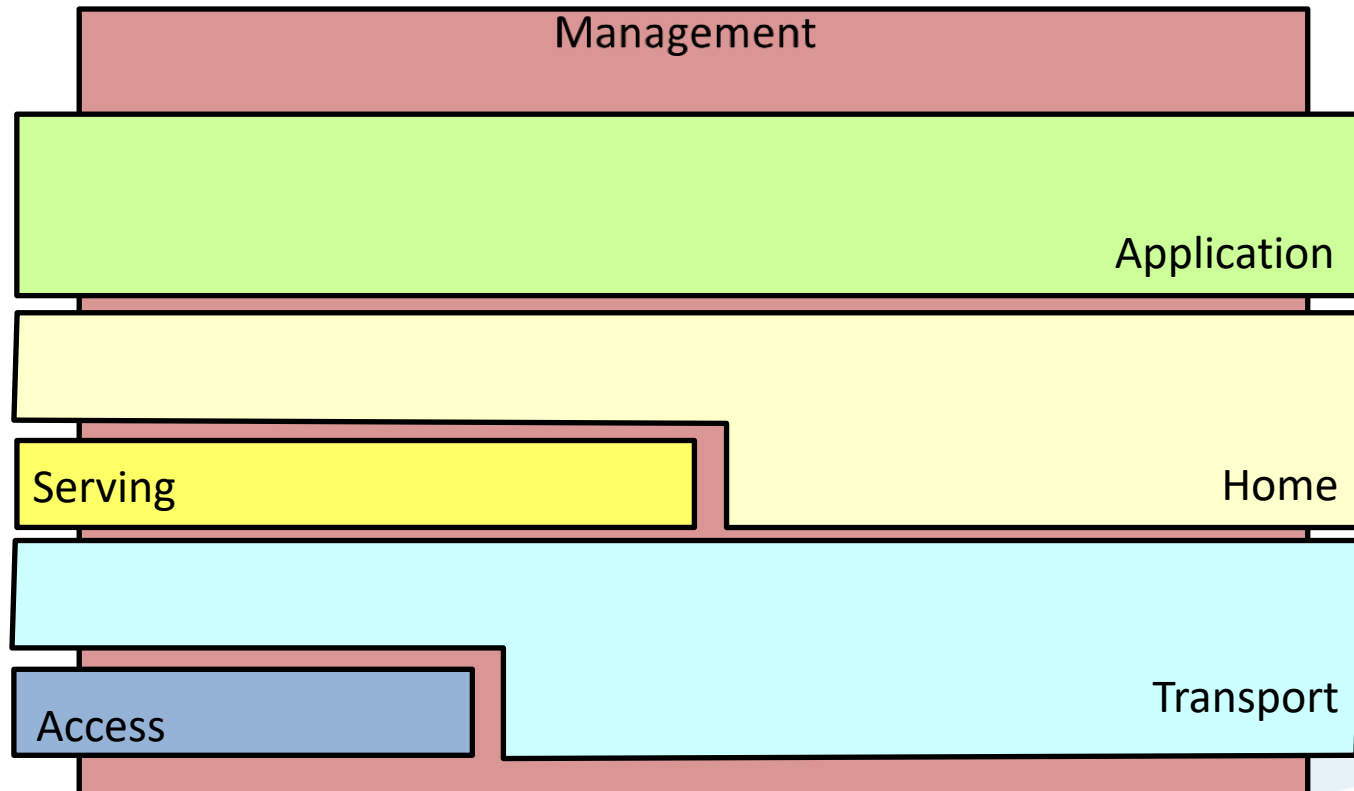
5G (Security) Domains



5G Security Domains – ETSI

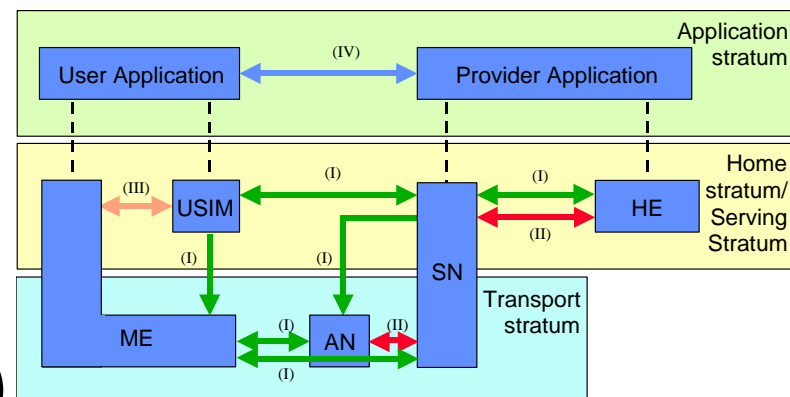


5G Strata




Security Feature Groups (TS 33.401)

- ❑ TS 33.401 defines
 - ❑ Network access security (I)
 - ❑ Network domain security (II)
 - ❑ User domain security (III)
 - ❑ Application domain security (IV)
 - ❑ Visibility and configurability of security (V)



- ❑ These are unclearly motivated/defined
 - ❑ E.g. “user domain” basically just comprises the PIN access code to the UICC
- ❑ Replace by *Security Realms, Security Control Classes*

Security Realms

 A **Security Realm (SR)** captures security needs of one or more strata or domain(s).

Security Realm	Note
Access Network Security	Corresponds closely to “Network Access Security” Feature Group of 33.401
Application Security	Corresponds closely to “Application Security” Feature Group of 33.401
UE Security	Very loosely related to “User Security” SFG of 33.401
Network Security	Corresponds somewhat to “Network Security” Feature Group of 33.401
Management Security	No counterpart in 33.401
Infrastructure & Virtualization Security	No counterpart in 33.401



Security Control Classes

- ❑ A **Security Control Class (SCC)** is a collection of security functions (including safeguards and countermeasures) to avoid, detect, counteract, or minimize security risks to 5G networks, in particular, risks to a network's physical and logical infrastructure, its services, the user equipment, signalling, and data.
- ❑ An extension of the well-known CIA-triad
 - ❑ Confidentiality
 - ❑ Integrity
 - ❑ Availability
- ❑ Used in many contexts ISO 27001, IETF, NIST, SANS, CSA
- ❑ We define 10 Security Control Classes.



SR & SCC Matrix

Security Realms	Security Control Classes									
	ID & Access Mgmt	AuthN	Non-repudiation	Confid.	Integrity	Availability	Privacy	Audit	Trust & Assurance	Compliance
Access Network Security										
Application Security				T R						
UE Security										
Network Security										
Management Security										
Infra.& Virtualiz. Security										

Intend to map threats **T** into this matrix (i.e. “threat to confidentiality in App. Realm”)
For each threat, a corresponding requirement **R** should be in place.



Summary

- Our high-level security architecture
 - re-uses well-known concepts, extending to 5G security landscape
 - is described in terms of
 - Domains & Strata*
 - Security Realms & Security Control Classes*
 - Allows to map our trust model and enablers.
- For more info, see our Deliverable D2.4,
http://5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.4-SecurityArchitectureDraft.pdf





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.

