5G Security

Communications Security

Security means preventing unauthorized access to
- messages
- communications infrastructure resources

while still providing the communications service between intended parties

Privacy means protecting a user's
- identity
- location
- personal data

A **threat** is a method to breach security or privacy
- denial of service (DoS) to the user
- theft of service by an unauthorized user
- access/modification to information by an unauthorized user
- control of restricted resources by an unauthorized user
- physical damage to resources

Trust is the degree to which we believe
that an entity will behave according to policy and not exploit threats

Security history

In the beginning the model was *trust everyone*

In the 1990s the model changed to *soft on the inside, hard on the outside*
trust employees and colleagues but not outsiders
which led to development of access policies, firewalls, etc.

Today standard operation procedures dictate

- *trust no-one*
- constantly monitor everything
- pro-actively search for vulnerabilities

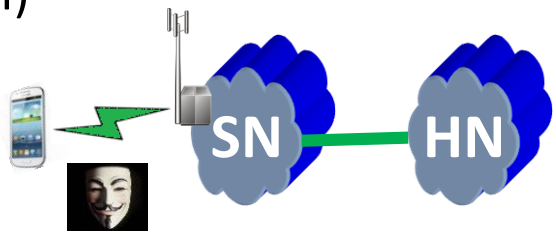
and utilizing multiple layers of protection (in case any one fails)

Trust through the generations 2G/3G

In **2G** trust is *required* (and attained using a SIM)

- of the UE by the network(s)

in order to avoid the threat of *theft of service*



However, it is *assumed* that

- the UE trusts the network
- the threat of eavesdropping on the air interface is acknowledged
  but assumed that simplistic encryption is enough to handle this issue

Trust is *assumed*

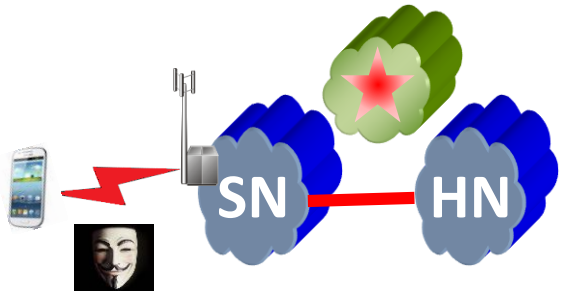
- inside any mobile network
- between **S**erving **N**etwork and **H**ome **N**etwork (or any other mobile network)

In **3G** it is no longer assumed that the UE can trust the network
(due to the possibility of fake base stations)
and the encryption of the air interface was strengthened (but still botched)

Trust through the generations 4G

In **4G** there are more actors

- UEs
- serving network
- home network
- transport networks (e.g., in the RAN)
- other networks (3GPP and non-3GPP)



and the assumptions are

- UEs and networks have mutual *lack of trust*
- user *privacy* must be respected
  must prevent not just eavesdropping but tracking too
- between networks there may be trust (at least to some degree)
  different mobile networks need to authenticate each other
- the air interface must be encrypted well

5G trust issues

Since 5G is designed to enable critical applications, such as

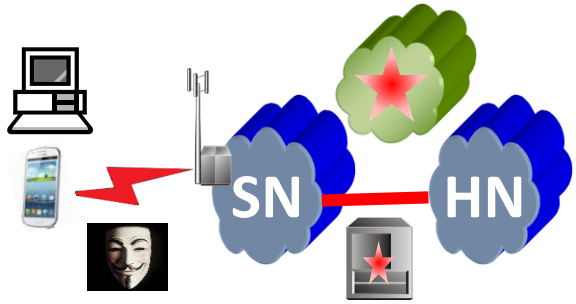
- critical infrastructure (electric, water, transportation, traffic control)
- emergency response
- smart cities
- autonomous cars

the threats are more significant than theft of service and eavesdropping

Furthermore the trust model involves many entities

- UE
- new host types (laptops, IoT, vehicles)
- home network
- serving network
- new transport mechanisms
- cloud service providers
- third-party application function providers
- private network operators
- direct peer-to-peer connections (e.g., for V2V)

and a priori no entity trusts any other entity



Countermeasures

What can we do to combat threats ?

- Physical security – preventing access to communications devices and links
- Emission security – preventing interception and jamming
- Privacy enforcement – protecting user's identity and blocking impersonation
- Authorization – preventing unauthorized access to resources
- Source authentication – confirming the source of a message
- Integrity – preventing tampering with messages
- Confidentiality – preventing eavesdropping
- DoS blocking – preventing Denial of Service
- Topology hiding – thwarting traffic analysis
- Anti-hacking – preventing injection of computer malware

Cellular security mechanism history

2G GSM already contained some basic security functions

- encryption of the radio interface to prevent eavesdropping
  different algorithms were allowed (A5/1, A5/2, A5/3), but all were broken
- tamper resistant SIM card for subscriber authentication
  to prevent theft of service
- use of random temporary identifiers to thwart subscriber tracking

3G introduced several improvements

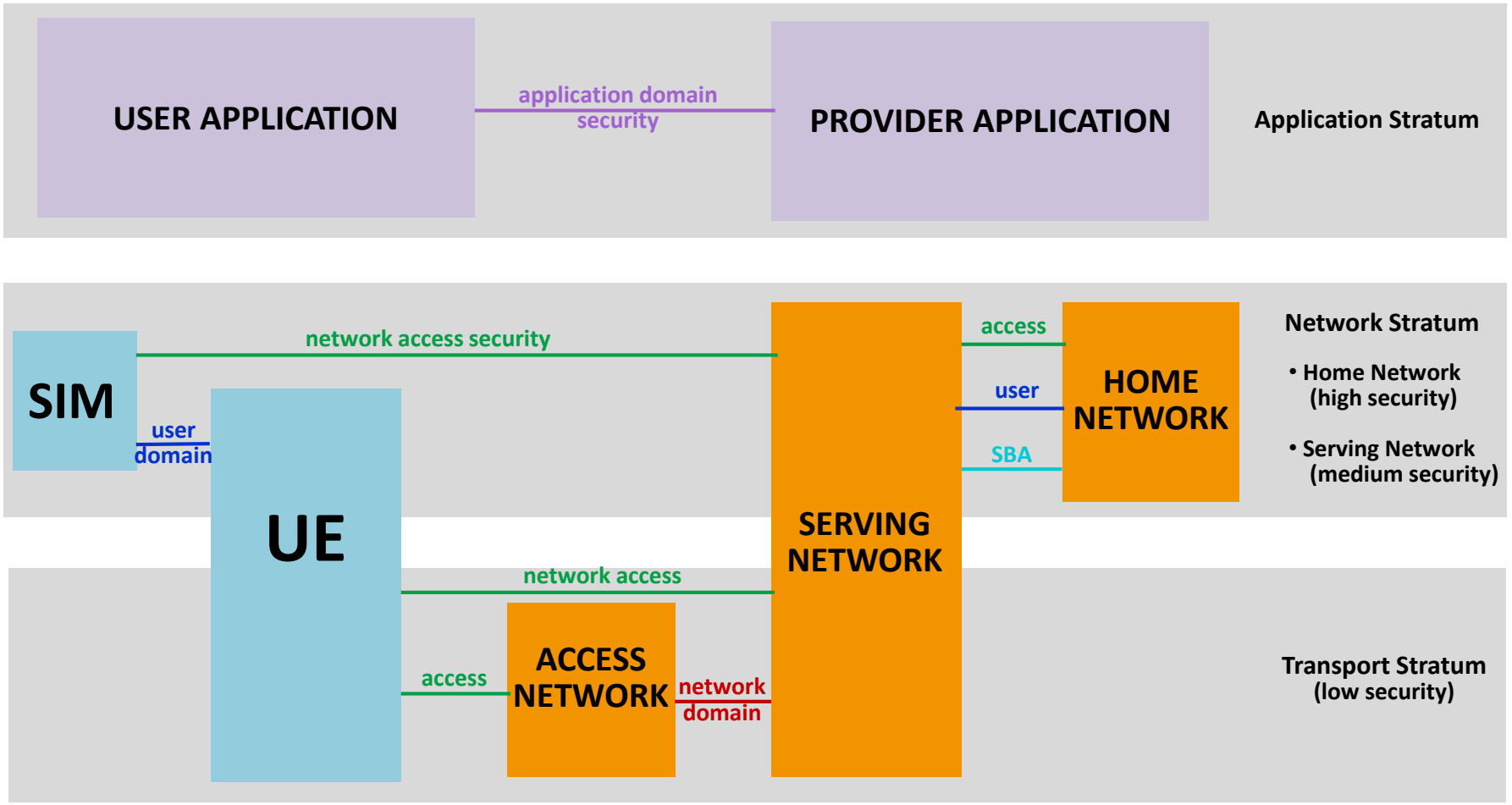
- mutual authentication to avoid fake base stations
- improved encryption algorithms (Kasumi)

4G was similar to 3G except

- **A**uthentication and **K**ey **A**greement protocol
- IMEI is only sent over secure channels
- use of state-of-the-art AES encryption (but SNOW-3G and ZUC allowed)
- **SE**curity **G**ateways create IPsec tunnels to protect backhaul

5G security architecture

5G defines 3 hierarchical *strata* and 5 *security domains*



Strata

Transport stratum

- includes PHY of air interface, transport network in RAN, UPF of core
- low security sensitivity (enables non-trusted vendors to provide RAN)
- only utilizes temporary identifiers and keys

Network stratum - *Serving* Network

- includes serving network's AMF, NRF, NEF, SEPP
- relatively high security sensitivity
- utilizes mid-level derived keys (such as AMF keys)

Network stratum - *Home* Network

- includes UE's SIM, home network's AUSF and UDM
- high security sensitivity
- utilizes SUPIs, user root keys, and high-level keys

Application stratum

- includes MEC, AF, 3d party functionalities, mobile payment
- responsibility of application service providers
- separated from mobile networks
- utilizes end-to-end security

Security domains

Network access security

- enables UE to authenticate and securely access services
  - mutual authentication, integrity protection, encryption
- protects against attacks on the air interface and from RAN to serving core

Network domain security

- protects RAN to core (IPsec) and serving-core to home-core (TLS, PRINS)
- protects control and user planes

User domain security

- secures end-user access to UE (passwords, PIN codes, etc)
- SIM access

Application domain security

- enable user applications to exchange messages with provider applications
- mechanisms provided by application providers and transparent to mobile

SBA domain security

- enable NFs in the SBA to securely communicate (TLS)
- features include NF registration, discovery, and authorization (OAuth)

SIM

Since 2G, the anchor of user identity
has been the **U**niversal **S**ubscriber **I**dentity **M**odule

Being a physical device it presents some degree of trust
like a physical key (but both can be stolen)

which is 1 reason for resistance to the ideas of eSIM and software-SIM

Today the *SIM* is part of the **U**niversal **I**ntegrated **C**ircuit **C**ard smart card
which consists of ROM, RAM, and a CPU, and contains

- USIM application (used in AS and NAS)
- **I**ntegrated **C**ircuit **C**ard **ID** (19 digit E.118 identifier written on SIM)
- **I**nternational **M**obile **S**ubscriber **I**dentity
- 2 PIN codes for protection
- 128-bit long-term pre-shared authentication key (also in HSS)
- file storage (e.g., for phone book)
- **I**P-Multimedia **S**ervices **I**dentity **M**odule application (used for SIP, VoLTE)

IMSI

International **M**obile **S**ubscriber **I**dentity uniquely identifies every UE

It is defined by ITU E.212 as up-to-15 digit number composed of:

- **H**ome **N**etwork **I**dentity (or PLMN ID)
  - **M**obile **C**ountry **C**ode (3 digits) e.g., Israel=425
  - **M**obile **N**etwork **C**ode (2-3 digits) e.g., Partner=01 Cellcom=02 Golan=08
- **M**obile **S**ubscription **I**dentification **N**umber (up to 10 digits)

The IMSI (and not the *phone number*) is

- stored in the **S**ubscriber **I**dentity **M**odule (along with the authentication key)
- sent by the UE as its identifier to the network
- indexes subscriber information in the HLR/HSS
- is locally copied into the VLR

To prevent *IMSI catching* the IMSI is sent

only when a unregistered UE registers to a cell (called *IMSI attach*)

From then on, including during paging and handoff

an arbitrary **T**emporary **M**obile **S**ubscriber **I**dentity (2G/3G) or

Globally **U**nique **T**emporary **I**dentifier (4G)

is used instead (and are frequently changed to prevent tracking)

4G EPS-AKA

In LTE, the mutual authentication and initial key exchange
between the UE's USIM and the MME uses
the **E**volved **P**acket **S**ystem **A**uthentication and **K**ey **A**greement protocol
with the MME acting as **A**ccess **S**ecurity **M**anagement **E**ntity

- UE completes RRC procedure with eNB
  and sends *attach request* to **S**erving **N**etwork MME with its IMSI
- MME sends IMSI and SN to HSS and requests **A**uthentication **V**ector
- based on IMSI and SN
  HSS generates AV={RAND, XRES, $AUTN_{HSS}$, K_{ASME}} and sends to MME
- ME stores AV, and forwards {RAND,$AUTN_{HSS}$} to UE
- UE computes {RES, $AUTN_{UE}$, K_{ASME}}
- UE compares $AUTN_{HSS}$ to $AUTN_{UE}$ for network authentication
- UE sends RES to MME
- MME compares RES with XRES for UE authentication
- if all succeeds, the key K_{ASME} (never transferred between UE and MME)
  is now shared between UE and MME

4G privacy vulnerabilities

There are several privacy vulnerabilities 4G

- AKA requires the UE to sends its IMSI *in the clear* over the air interface to the MME (see next slide)
- once registered the UE-MME messaging uses the GUTI to hide the UE's identity, but:
  - GUTIs are not changed frequently enough
  - GUTI allocation is often predictable
- the home network provides AVs to the serving network but is not part of the authentication decision

5G remedies these vulnerabilities by supporting 3 new authentication methods

- 5G-AKA
- EAP-AKA' (with Perfect Forward Security)
- EAP-TLS

IMSI catching

IMSI catching is a man-in-the-middle attack to collect IMSIs
(there are even miniature *wearable* IMSI catchers used by police)

Since IMSIs are only rarely transmitted
the probability of passively catching one is very low

An IMSI catcher (AKA a *StingRay*) masquerades as a base station
and causes the UE to register and send its IMSI

The principle was patented in 2003 by Rhode and Schwartz for GSM
but the patent was invalidated in 2012 (no *inventive step*)

Simple IMSI catching enables tracking, and perhaps impersonating, users

In a full MitM attack, the attacker

- convinces the UE that it is the preferred BS (has strongest pilot signal)
- captures the UE's IMSI
- negotiates null encryption
- intercepts all user traffic
- passes user traffic to and from a true base-station

Hiding the IMSI

5G enhances user *privacy* as compared to previous generations

- user identity cloaking
- user location confidentiality
- user activity masking

by *never* sending an IMSI in plaintext

5G defines

- **SU**bscription **P**ermanent **I**dentifier
  (IMSI or *email address* user@network for non-3GPP)
  which is never sent over the air interface
- **SU**bscription **C**oncealed **I**dentifier (pronounced Suchi ☺)
  which is freshly cryptographically generated by the UE
  before being sent *once* over the air interface

The technique is called the **E**lliptic **C**urve **I**ntegrated **E**ncryption **S**cheme

The UE (using elliptical curve crypto) generates the SUCI
by encrypting its SUPI and a sequence number (incremented to prevent repetition)
using the public key of its home network

5G ECIES

To simplify we'll assume the non-roaming case (UE in home network)

- UE encrypts SUPI (MSIN, not MCC/MNC) and SQN creating SUCI
- UE sends *registration request* with SUCI to AMF
- AMF sends *authentication request* with SUCI to AUSF
- AUSF+UDM decrypt SUCI to SUPI
- AUSF sends *authentication response* with SUPI to AMF
- AMF generates GUTI and remembers GUTI-SUPI mapping
- AMF sends *registration accept* to UE
- UE sends second *registration request* with GUTI to AMF
  commencing 5G's version of AKA (slightly more complicated than 4G's)

Several other related mechanisms are provided by 5G as well

- in 4G IMSI-based paging (used when UE is *idle*) leaked IMSI information
  5G uses only one-time temporary identifiers
- 5G introduces a **SE**curity **A**nchor **F**unction to facilitate re-authentication
  when moving between different RANs w/o full AKA
  thus reducing load on the home network AUSF+UDM

Additional 5G authentication features

Long term identifiers are never transmitted in the clear

When roaming, it is the home network's AUSF
that performs UE authentication

The **SE**curity **A**nchor **F**unction in a serving network can act as middleman
during the authentication process
and can reject the authentication from the UE
but never accept the authentication

In addition to 5G-AKA, **E**xtensible **A**uthentication **P**rotocol can be used, and

- there are 2 variants – EAP-AKA' and EAP-TLS (for private networks and IoT)
- the UE acts as an EAP supplicant
- the AUSF acts as an EAP server
- the SEAF acts as an EAP pass-through authenticator

When authentication is over untrusted non-3GPP access networks
the Non-3GPP Interworking Function (N3IWF) is used
to allow the UE to access the 5G core over IPsec tunnels.

Compartmentalization

We have mentioned the use of multiple layers of security

Another general principle of modern security is *compartmentalization*
that is, isolating different parts of a system
so that breaches in one area do not affect other areas

5G utilizes compartmentalization in many aspects

- the 3 strata (transport, network, application) are isolated
- the RAN and core are clearly demarcated
- different core networks are isolated (SEPP)
- different keys are used after handoff
- network slices have separate security functions

Security in the SBA

There are various threats to the SBA which must be handled, e.g.,

- eavesdropping on sensitive N-interface messages
- crashing NF by sending malformed messages
- overwhelming NF by flooding
- obtaining unauthorized access to services
- modifying N-interface messages on the fly
- malicious changes to NF configuration

We have seen that the SBA-based 5GC uses the following protocols:

- **J**ava**S**cript **O**bject **N**otation (for encoding information)
- http/2 (for interaction, RESTful CRUD operations)
- TCP (for reliability and load balancing) [rather than SCTP as in 4G]

and so 3GPP mandates use of

- TLS 1.3 (RFC 8446)
  - to authenticate parties using public key crypto
  - to provide integrity of all connections
  - to encrypt messages
- OAuth2.0 (RFC 6749)
  - to provide delegated authorization via tokens without divulging keys

TLS

Transport **L**ayer **S**ecurity is an updated version of **S**ecure **S**ockets **L**ayer
originally developed by Netscape for its browser
but now used for browsing (https), email, chat, VoIP, etc.

4G security was based on IPsec and DIAMETER
5G's uses https based on TLS

Unlike IPsec, TLS provides a *client-server* model of security
and assumes *reliable* transport
and so is situated between TCP and an application

TLS has 2 sub-layers :

- TLS *handshake*
  - set-up negotiation (algorithms, generating keys, etc.)
  - (optional) authorization using public key cryptography and certificates
- TLS *record*
  - integrity using HMAC
  - encryption using symmetric key cryptography

5G requires authorization and uses authenticated encryption algorithms

OAuth

OAuth is a mechanism for secure access delegation
i.e., a way for resource owners to grant 3rd parties
restricted access to resources (servers, accounts, information)
without sharing their credentials

If you have ever accessed a website using your Google/Facebook account
you have used Oauth!

OAuth began in 2006 at Twitter, but the effort was joined by Google, etc.

The inspiration behind Oauth is the *valet key*
Some luxury cars come with a special key to give to valets or garages
and only allows driving a short distance
but not opening the trunk or glove compartment, etc.

Similarly, Oauth allows limited access to specific resources
using tokens that the user can later revoke

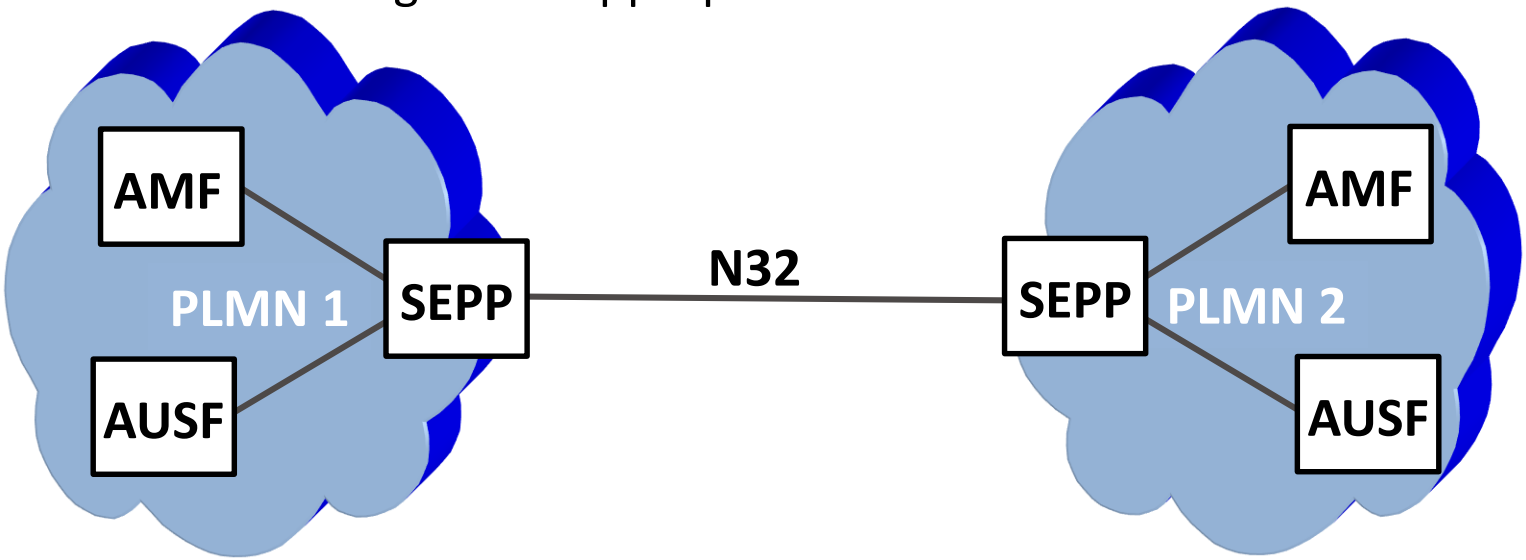
SEPP

Security issues arose in previous generations when communications bridged several mobile networks (e.g., when *roaming*)

To solve such problems 5G introduced a perimeter security function called **S**ecurity **E**dge **P**rotection **P**roxy and a new N32 interface

The SEPP sits at the perimeter of the 5GC and

- protects all outgoing messages before sending to a 2nd PLMN over N32
- receives and verifies all incoming messages on N32 interface before forwarding to the appropriate NF



SEPP protocols

The SEPP provides end-to-end protection
for application layer control plane messages
between NFs belonging to different core networks
from being exposed or manipulated by other parties

A consumer in one network can safely access a producer in another
so that we have a cSEPP and a pSEPP

The SEPP hides internal topology information from 3rd parties
and performs rate limiting to prevent DoS

Since the 5GC is based on RESTful interfaces using http and JSON
the SEPP protocols are based on

- https, which is http over **T**ransport **L**ayer **S**ecurity (RFC 8446, ex-SSL)
- use of *telescopic FQDNs*

If there are interconnect providers between the SEPPs, then we also need

- *PRINS* - PRotocol for N32 INterconnect Security (application layer security)
  - JSON Web Encryption (JWE, RFC 7516) between SEPPs
  - JSON Web Signatures (JWS, RFC 7515) by interconnect provider to sign changes

Telescopic FQDNs

The **F**ully **Q**ualified **D**omain **N**ame of a particular 5GC is
5gc.mncXXX.mccXXX.3gppnetwork.org

and for a NF in this core, for example the NRF:
nrf.5gc.mncXXX.mccXXX.3gppnetwork.org

For example, the NRF of Partner's 5GC here in Israel will be
nrf.5gc.mnc001.mcc425.3gppnetwork.org
but these URLs can be much more complex

REST API calls are between such URLs

SEPPs obfuscate the internals of their cores by using *telescopic FQDNs*
consisting of a label as first element and SEPP's domain as trailer

For example, if access to some NF is requested from some core
nf.xxx.xxx.5gc.mnc001.mcc425.3gppnetwork.org
is replaced by the pSEPP with
label.5gc.mnc001.mcc425.3gppnetwork.org
where label is generated by the pSEPP which remembers the mapping

NESAS

Network **E**quipment **S**ecurity **A**ssurance **S**cheme
has been jointly defined by GSMA and 3GPP
for security evaluation of mobile network equipment

It offers a single process approach to security audits
thus saving time and expense for both vendors and operators

NESAS assesses the security of

- a vendor's products (in ISO 17025 accredited security test labs)
  - conformance to 3GPP security standards
- its R&D lifecycle (via GSMA selected security auditors)
  - security by design
  - version control, source code review, vulnerability remedy process
  - security documentation, point of contact

and provides uniform equipment certification and security documentation

The Huawei question

The *elephant in the room* is the trustworthiness of Chinese vendors

The US forbids use of Huawei equipment by tier 1 domestic operators
and is threatening sanctions on the rest of the world to follow suit
and also requiring chip vendors to obtain licenses before selling to Huawei

China believes this is part of an international trade war
and has nothing to do with true security issues
and Huawei denies involvement in espionage on behalf of the Chinese state

The problem is that Huawei is

- number 1 telecom supplier in the world
- number 2 phone manufacturer in the world
- a major player in 5G and in some areas *the* technology leader

while the US no longer has any major mobile equipment vendor

The UK (which today is heavily Huawei dependent)
is phasing out Huawei's involvement in national networks
and limiting it to the 5G RAN segment and to no more than 35% of it
under threat of sanctions from the US intelligence community

EU 5G security toolbox

After studying the issue of foreign vendors
the EU member states have agreed on a toolbox of mitigating measures
to address security risks related to 5G rollout :

- Strengthening the role of national authorities
  to restrict supply, deployment and operation of 5G network equipment
- Performing audits on operators
- Assessing the risk profile of suppliers to identify **H**igh **R**isk **V**endors
  including vendors with a strong link to the government of a 3rd country
- Controlling the use of Managed Service Providers (MSPs)
- Ensuring the diversity of suppliers
  to avoid major dependency on a single supplier
- Strengthening resilience at the national level
- Identifying key assets and fostering diverse/sustainable 5G ecosystem
- Maintaining diversity and EU capacities in future network technologies