Radboud University

Advanced Network Security

Lecture 11: Demystifying 5G

Harald Vranken, Katharina Kohls

May 17th, 2021

Open University Nijmegen
Radboud University Nijmegen

Recap

(1) Clarifying Imp4Gt
- Encryption oracle: Inject arbitrary packets in uplink direction
- Depends on the Ping reflection

(2) ReVoLTE
- Exploiting keystream reuse in VoLTE calls
- Record target call
- Place subsequent call, recover keystream, decrypt

(3) Required Background
- ROHC and Codecs
- VoLTE AKA and SRTP
- IMS and data bearers
- Keystream generation

This Lecture

4G versus 5G

- 4G is deployed and used by millions...
- 5G is in a transition state
- We can measure and test what happens in 4G...
- and for 5G it's sometimes not even specified.

This Lecture

Interactive Lecture!

- Introduction to 5G and some basics
- Selected topics
- *Investigate blind spots*

The 5G Wonderland

Technical Background

5G Improvements

The 5G Wonderland

Buzzword Bingo!

Buzzword Bingo

Massive IoT

Edge Computing

Ultra-reliable low-latency communication (URLLC)

Artificial Intelligence

Fifth Mobile Generation

5G enables a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices.[1]




[1] https://www.qualcomm.com/5g/what-is-5g

Qualcomm about 5G

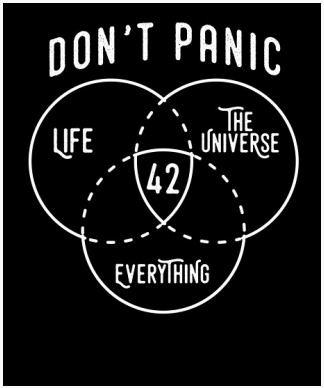
5G is designed to deliver peak data rates up to 20 Gbps . . . the Qualcomm® Snapdragon™ X65 is designed to achieve up to 10 Gbps in downlink peak data rates.

But 5G is about more than just how fast it is. In addition to higher peak data rates, 5G is designed to provide much more network capacity by expanding into new spectrum, such as mmWave.

5G can also deliver much lower latency for a more immediate response and can provide an overall more uniform user experience so that the data rates stay consistently high—even when users are moving around.[2]

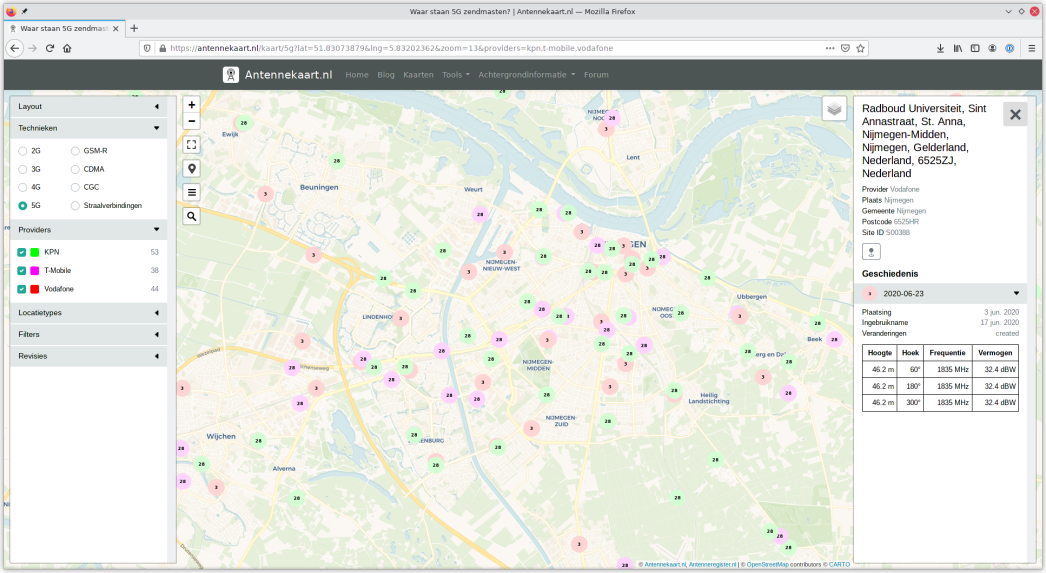
[2] https://www.qualcomm.com/5g/what-is-5g

The answer to everything



What are possible use cases for 5G?

The answer to everything...
where can I get it?



https://antennekaart.nl

Technical Background

Network Components

UE

eNodeB

EPC

gNodeB

5GC

Component	4G	5G	Icon
Phone	UE	UE	
Base Station	eNodeB	gNodeB	
Core Network	EPC	5GC	
Internet	IP Network	IP Network	

5G Deployment

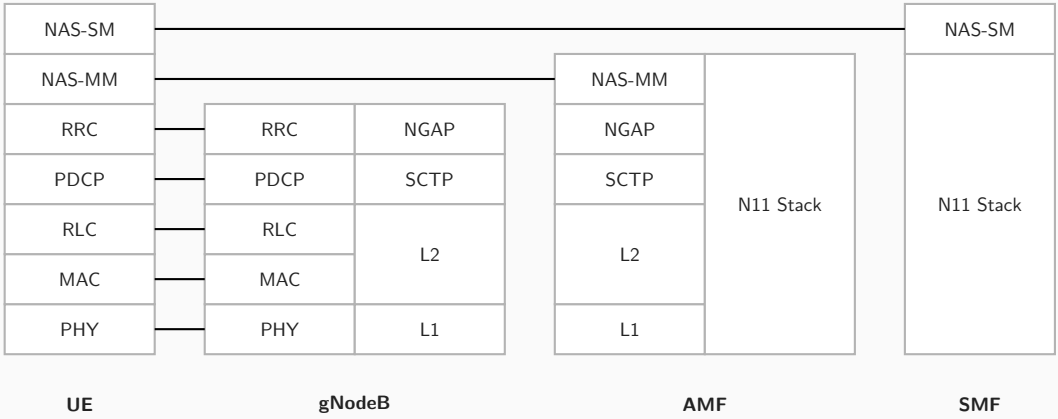
5G Non-Standalone (5G NSA)

- 5G Network supported by existing 4G RAN and EPC
- Dual Connectivity: UE simultaneously connected to LTE cell and 5G NR cell
- Best option for early deployment
- Quick creation of 5G coverage

5G Standalone (5G SA)

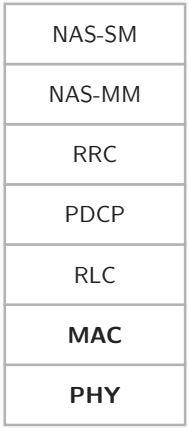
- 5G network without support from 4G RAN infrastructure
- 5G NR coverage
- Simplification and improved efficiency compared to NSA operation
- Final target architecture

Protocol Stack: Control Plane



https://www.metaswitch.com/knowledge-center/reference/what-is-the-5g-access-and-mobility-management-function-amf
https://www.metaswitch.com/knowledge-center/reference/what-is-the-5g-session-management-function-smf

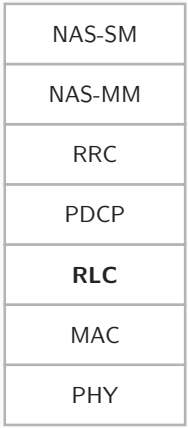
Protocol Stack: PHY, MAC



PHY, MAC

- **Physical Layer (PHY)**
  - Receive and send signals
  - Multiplexing
- **Medium Access Control (MAC)**
  - Scheduling
  - RNTI
  - Error correction
  - Retransmissions

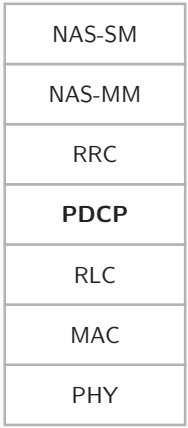
Protocol Stack: Radio Link Control (RLC)



Radio Link Control (RLC)

- Transfer upper layer data units in three different modes
  (1) Acknowledged Mode
  (2) Unacknowledged Mode
  (3) Transparent Mode

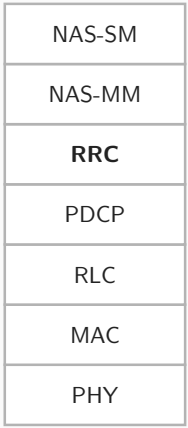
Protocol Stack: Packet Data Convergence Protocol (PDCP)



Packet Data Convergence Protocol (PDCP)

- Robust Header Compression (ROHC)
- Separation of user plane (IP) and control plane (RRC)
- Encryption of control and user plane
- Integrity protection of control plane

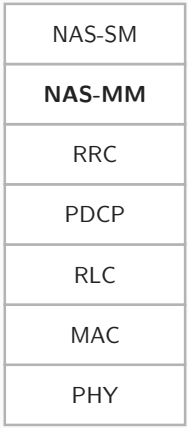
Protocol Stack: Radio Resource Control (RRC)



Radio Resource Control (RRC)

- Establish and release RRC connection
- Assign Radio Network Temporary Identity (RNTI)
- Establish data bearers
- Measurement configuration, reporting

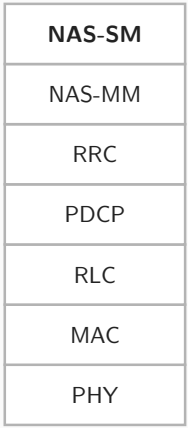
Protocol Stack: NAS Mobility Management (NAS-MM)



NAS Mobility Management (NAS-MM)

- Mobility management (paging)
- Identity management
- Authentication

Protocol Stack: NAS Session Management (NAS-SM)



NAS Session Management (NAS-SM)

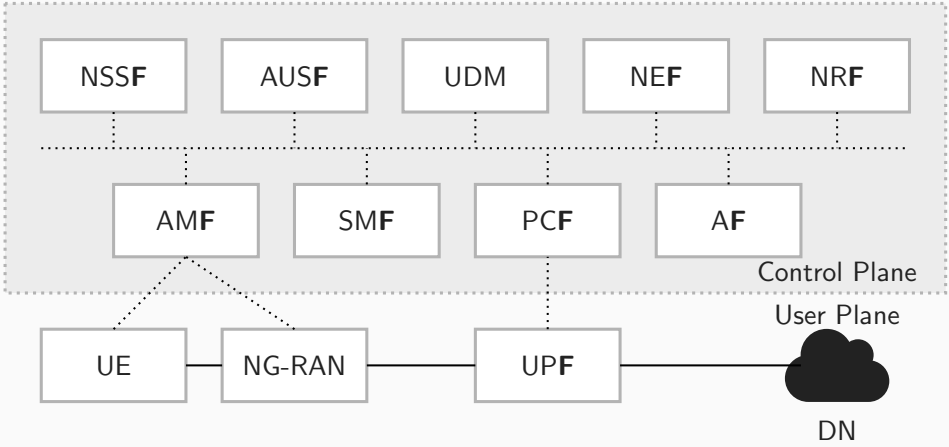
- Establish and manage communication links
- Assign IP address
- Quality of Service

5G Improvements

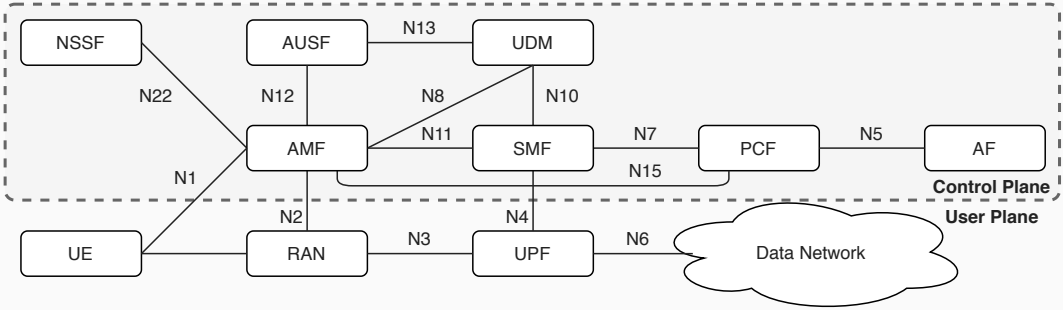
5G Improvements

Service-Based Architecture	Unified Access-agnostic Authentication	5GC-EPS Interworking Security	RAN Security DU-CU Split
User Plane Integrity Protection	Primary Authentication	Visibility Configurability	Interconnection Security SEPP
Enhanced Subscriber Privacy	Increased Home Control	Secondary Authencication	Initial NAS Message Protection

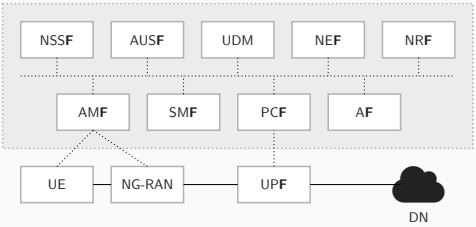
Service-Based Architecture



Reference Point Architecture



Service-Based Architecture



Service-Based Architecture

- REST/HTTPS-based interfaces
- Third party applications in the core network
- Cloud-based deployment
- New core network vendors

What are possible challenges of the service-based architecture?

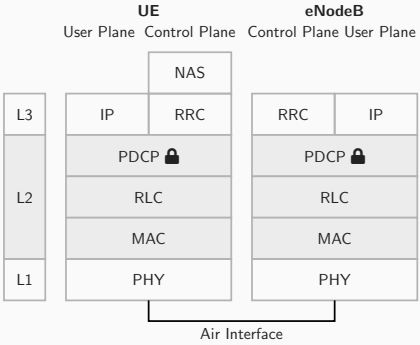
- Correct implementation
- Trust between entities

5G Improvements

Service-Based Architecture	Unified Access-agnostic Authentication	5GC-EPS Interworking Security	RAN Security DU-CU Split
User Plane Integrity Protection	Primary Authentication	Visibility Configurability	Interconnection Security SEPP
Enhanced Subscriber Privacy	Increased Home Control	Secondary Authencication	Initial NAS Message Protection

4G: Plaintext Modification

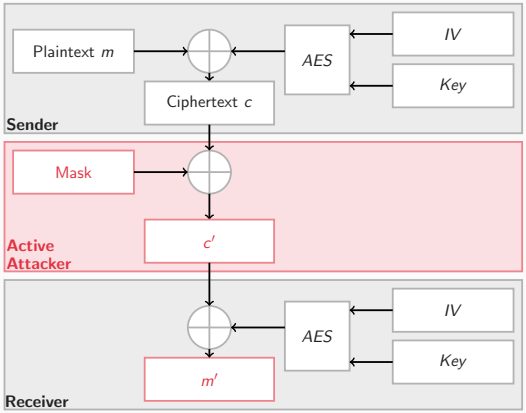
Feature	Control Plane	User Plane
Encryption	✔	✔
Integrity Protection	✔	✘



There is no integrity protection for user plane traffic!

4G: Plaintext Modification

- PDCP encrypts IP packet
- Stream cipher: AES in counter mode
- XOR manipulation mask m
- Deterministic manipulation
- Manipulation remains undetected



User Plane Integrity Protection

Mandatory Integrity Protection

- 4G: No integrity protection for user plane data
- User data redirection (L8), Full Impersonation (L9)
- 5G: Mandatory to support
- Optional to use by operator

What are challenges of mandatory integrity protection?

- Overhead
- Deployment

5G Improvements

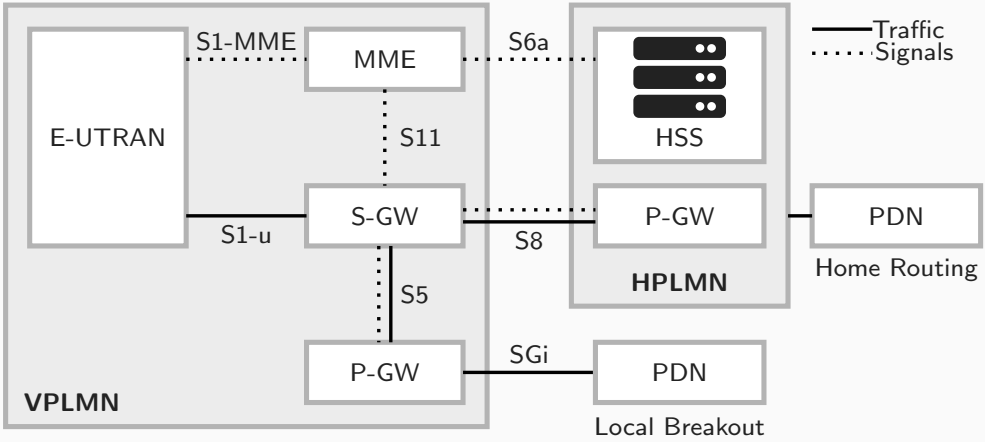
Service-Based Architecture	Unified Access-agnostic Authentication	5GC-EPS Interworking Security	RAN Security DU-CU Split
User Plane Integrity Protection	Primary Authentication	Visibility Configurability	Interconnection Security SEPP
Enhanced Subscriber Privacy	Increased Home Control	Secondary Authencication	Initial NAS Message Protection

Interconnection

What does “Interconnection” mean?

- Roaming
- You connect to the local network
- Your credentials are in the home network
- Both networks must connect

Roaming Architecture in 4G

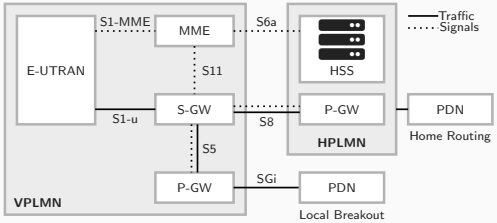


HPLMN and VPLMN

Home versus visiting network

- The HPLMN is the home network.
  - This is where your SIM card is from.
  - Key components like the HSS are always at home.
- The VPLMN is the visiting network.
  - This is where you currently are.
  - In case you are in your SIM'c home country, $HPLMN = VPLMN$

Home Routing and Local Breakout



Local Breakout versus Home Routing

- There are two modes of operation
- **Local Breakout**
  - You use the infrastructure of the VPLMN
  - The HPLMN is only involved in the AKA
- **Home Routing**
  - The S-GW routes your traffic to the home network.
  - You use a P-GW in the HPLMN

Interconnection Security SEPP

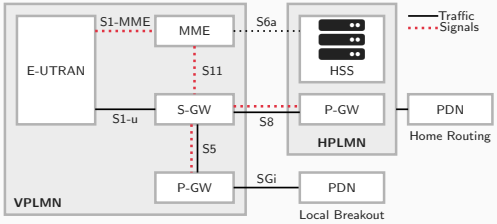
Before 5G

- SS7 network (70s) based on trust
- Many attacks on user tracking, eavesdropping

5G Standalone

- Security Edge Protection Proxy (SEPP)
- HTTPS and PRotocol for N32 INterconnect Security (PRINS)

Control Traffic



Interconnection Security

- SS7, Diameter, SEPP, PRINS...
- Only for control traffic!
- **Problem: SS7 remains as fallback!**
- *What happens to user plane roaming traffic?*

Investigate

Questions

- We know about the control plane, but what happens to user plane traffic?
- What transport protocols are used for the user plane traffic?

Hints

- Read the specification: EPS Roaming Guidelines Version 22.0
  `IR.88-v22.0_lecture_11.pdf`
- Focus on LTE, that's OK for now
- If you find GTP you're on the right track!

What happens to user plane traffic?

- Local breakout (using the VPLMN's local gateway) or home routed
- Home routed traffic is sent over the N9 interface which uses the GPRS tunneling protocol (GTP). GTP uses UDP.
- Same as LTE and before, home routed traffic sent via SEPP

How does the SEPP stack differ from the SS7 stack?

- HTTP/2 and JSON, using TLS
- SS7 uses its own stack

5G Improvements

Service-Based Architecture	Unified Access-agnostic Authentication	5GC-EPS Interworking Security	RAN Security DU-CU Split
User Plane Integrity Protection	Primary Authentication	Visibility Configurability	Interconnection Security SEPP
Enhanced Subscriber Privacy	Increased Home Control	Secondary Authencication	Initial NAS Message Protection

Enhanced Subscriber Privacy

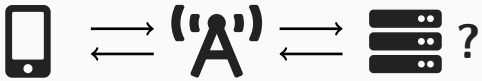
Permanent and Temporary

- Unique identifier on the SIM card
- Because AKA uses a shared symmetric key, it can only happen after user identification
- Sending the IMSI/SUPI in plaintext means a user can be identified and tracked ☹
- **To avoid this, temporary identifiers are used!**

	4G	5G
Permanent	IMSI	SUPI
Temporary	TMSI	GUTI

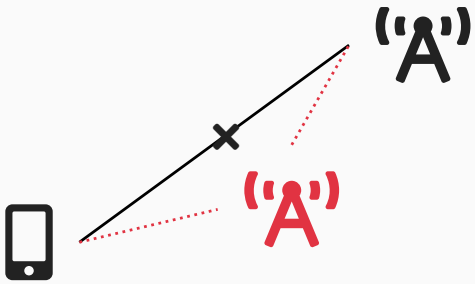
It's not always possible to use the temporary identifiers.

When does a temporary identifier not work?



Contacting the Network

- Temporary identifiers need to be assigned
- When the user visits for the first time, there is no TMSI/GUTI for the user
- Special case: IMSI/SUPI cannot be derived from the TMSI/GUTI



Man-in-the-Middle

(1) UE connects to legitimate eNodeB

(2) Attacker places a fake base station

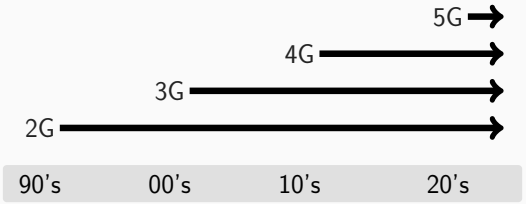
(3) Stronger signal makes user connect to fake bts

(4) **Attacker can force the user to share permanent identifiers!**

IMSI Catcher Protection in 5G

Backward Compatibility

- 2G/3G/4G are vulnerable to IMSI catchers
- Main reason: Backward compatibility
- 5G solves the problem at the cost of backward compatibility



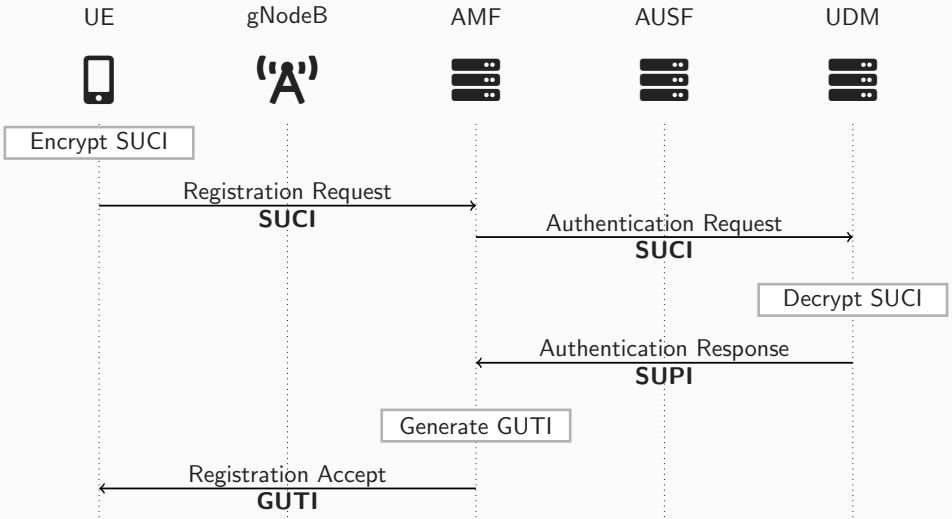
How do they do it?

Subscription Concealed Identifier (SUCI)

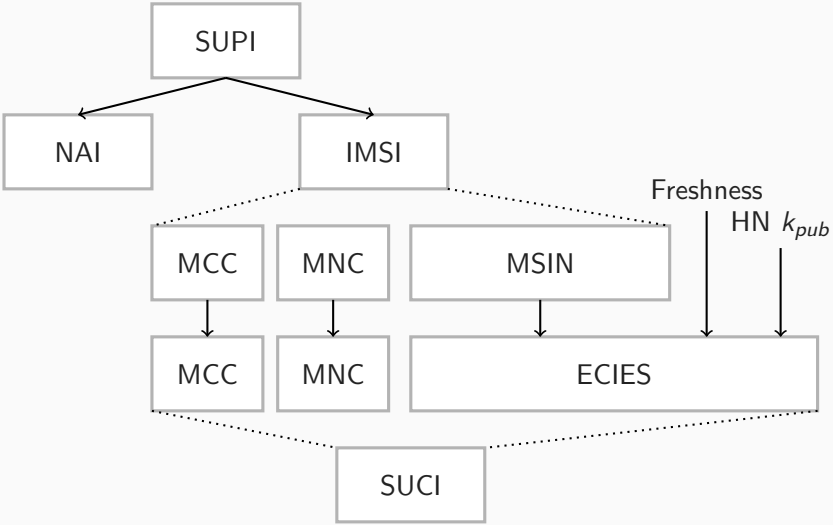
- Whenever the SUPI is needed, a concealed version is sent instead
- Elliptic Curve Integrated Encryption Scheme (ECIES) [3]
- The SUCI is sent instead of the plaintext permanent SUPI

[3] ECIES combines a Key Encapsulation Mechanism with a Data Encapsulation Mechanism. It derives a bulk encryption key and MAC key from a common secret. It's a hybrid scheme that uses an asymmetric approach to send a symmetric key.

5G Identity Exchange



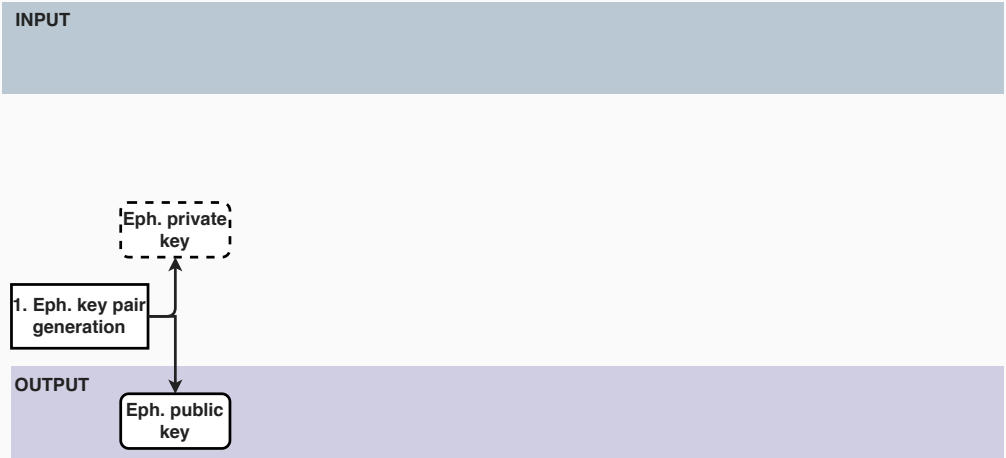
From SUPI to SUCI



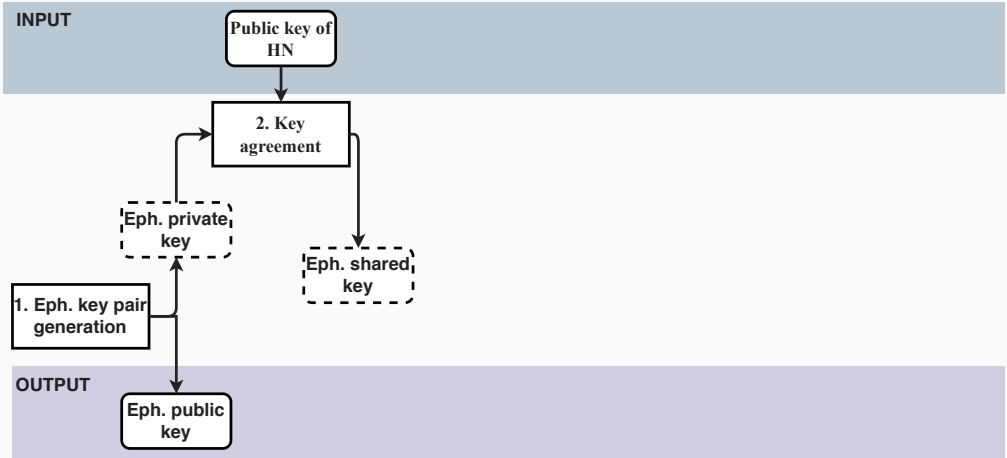
From SUPI to SUCI

- The SUPI consists of
  - IMSI: Standard case we know from 4G; unique personal number
  - NAI: New 5G setting, personal address like `user@homerealm.example.net`
- IMSI has MCC and MNC as "preamble", example KPN Telecom B.V.:
  - `MCC 204`
  - `MNC 69`
- MSIN is a personal, permanent, unique number
- Needs protection, gets encrypted using a fresh input and a public key

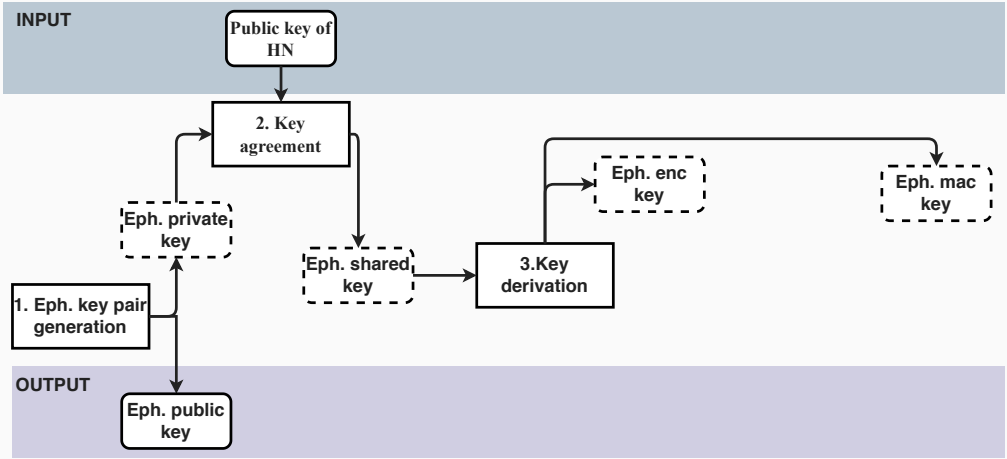
From SUPI to SUCI – Encryption — Step 1



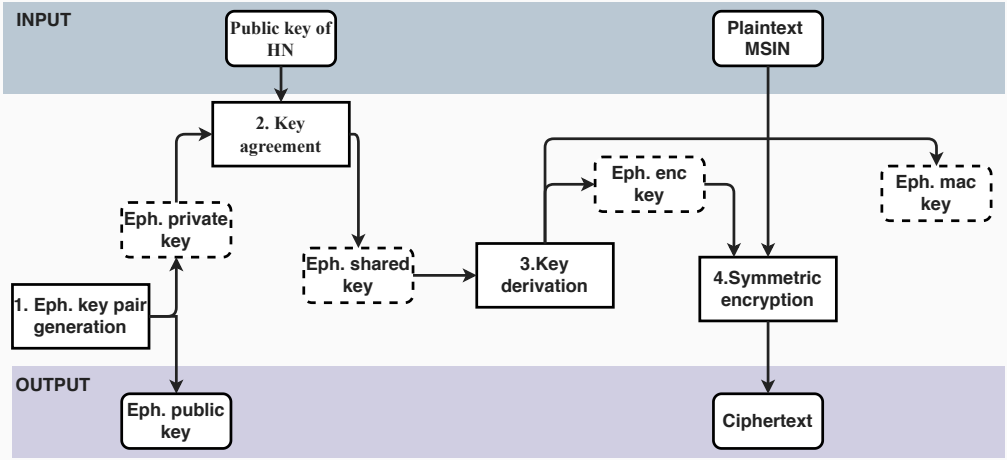
From SUPI to SUCI – Encryption — Step 2



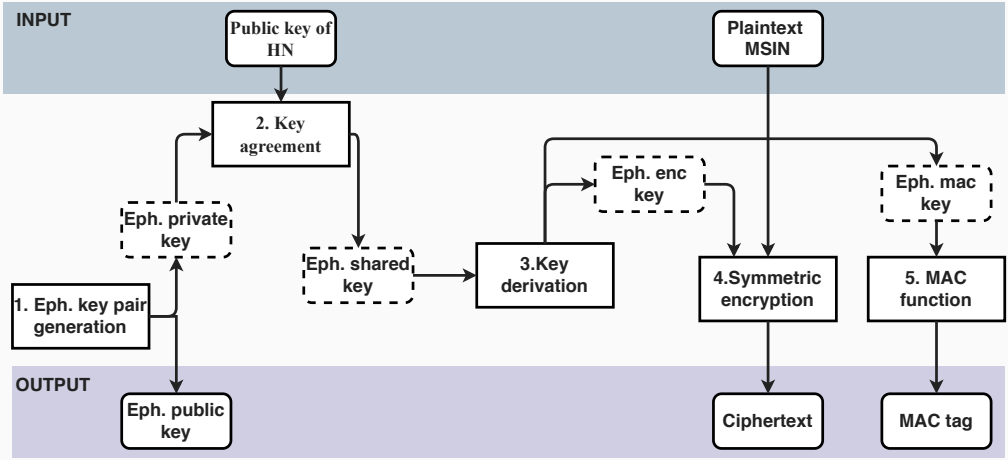
From SUPI to SUCI – Encryption — Step 3



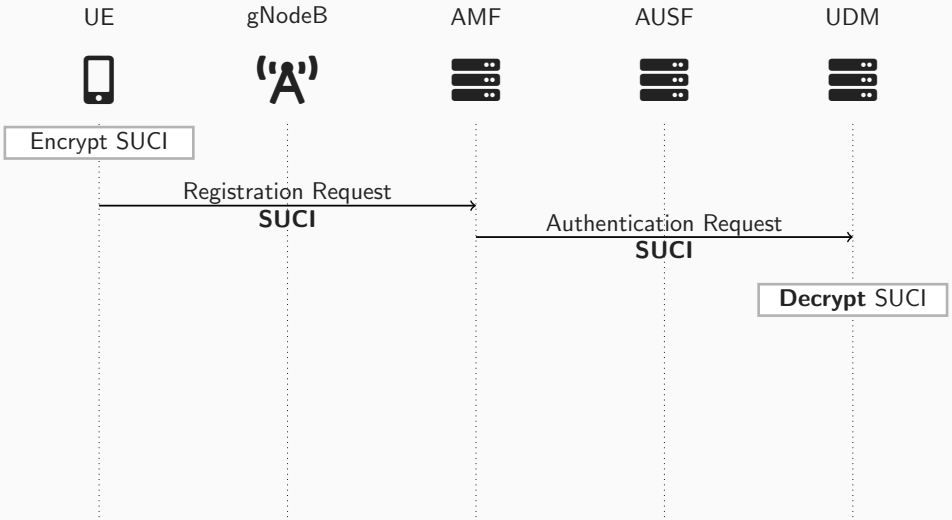
From SUPI to SUCI – Encryption — Step 4



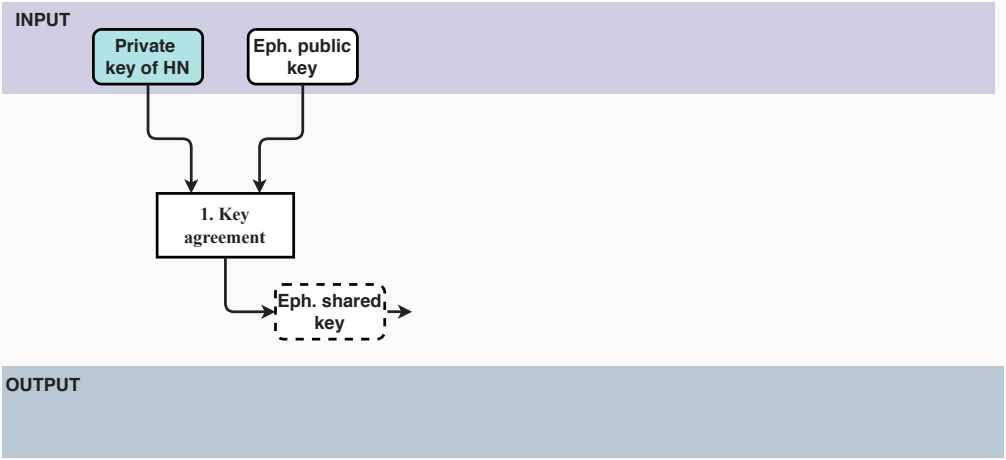
From SUPI to SUCI – Encryption — Step 5



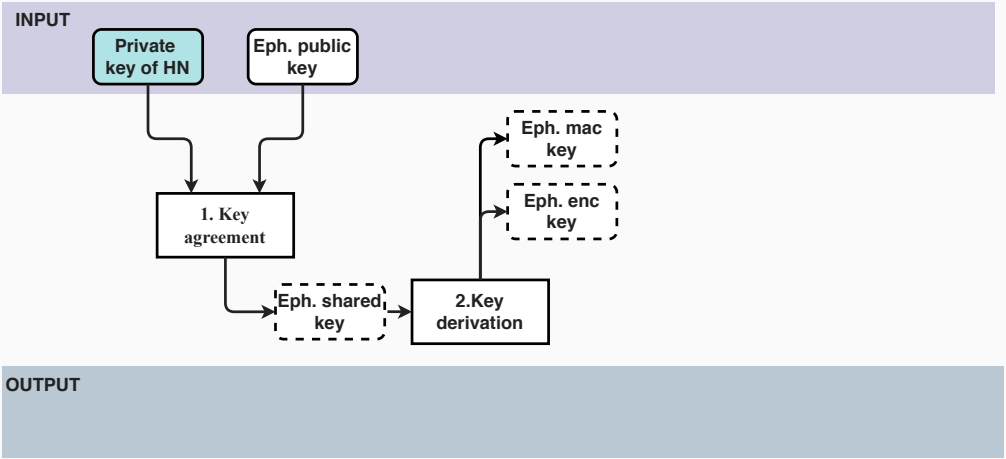
5G Identity Exchange



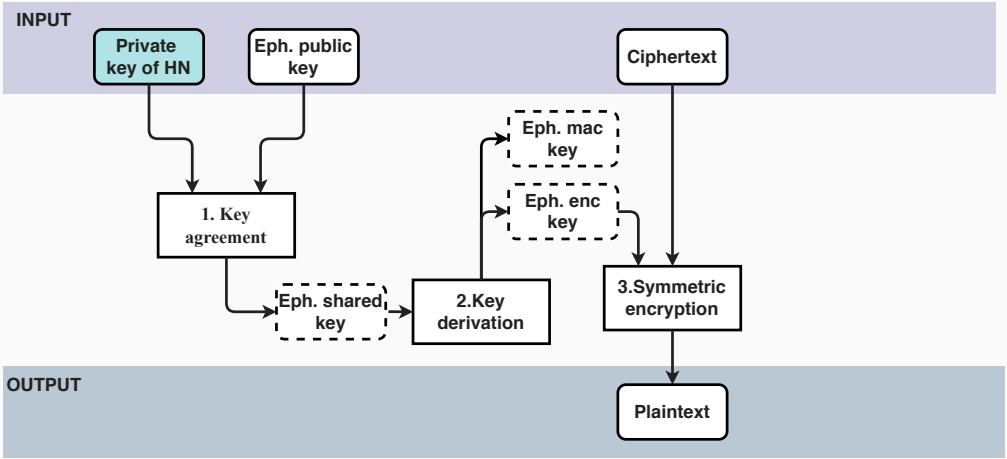
From SUCI to SUPI – Decryption — Step 1



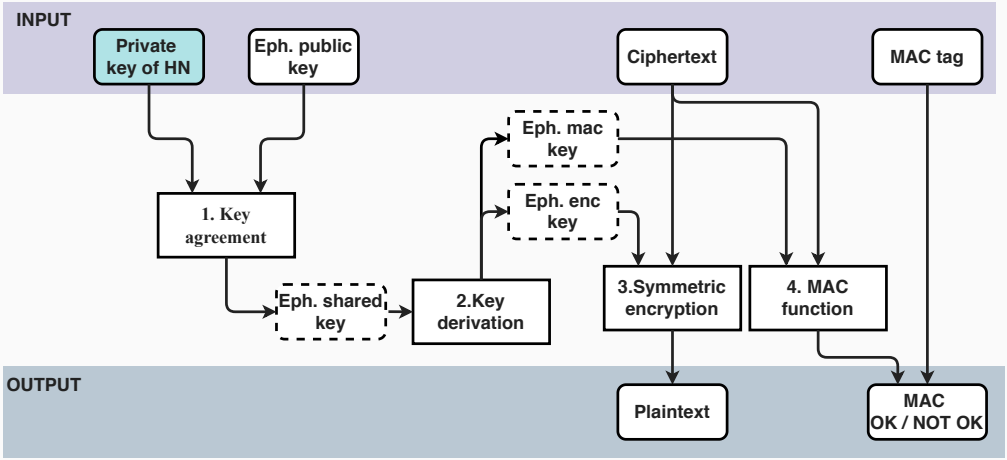
From SUCI to SUPI – Decryption — Step 2



From SUCI to SUPI – Decryption — Step 3



From SUCI to SUPI – Decryption — Step 4



Trace Analysis

`registration_request_suci.pcapng`

SUCI Decryption

SUPI Encryption

Packet 1

SUPI Encryption

Packet 2

CryptoMobile Example

What we will do:

- Install the CryptoMobile lib
- Prepare the keys
- Load the SUCIs from the PCAPs
- Recover the IMSIs from them

Demo: CryptoMobile

Example (Linux Machine)

```
git clone https://github.com/P1sec/CryptoMobile.git
cd CryptoMobile
python setup.py install
```

Demo: CryptoMobile

```
from CryptoMobile.EC import *
from CryptoMobile.ECIES import *
import binascii
# Setting up home network UDM environment
ec = X25519(binascii.unhexlify(
  'c53c22208b61860b06c62e5406a7b330c2b577aa5558981510d128247d38bd1d'))
hn_privkey = ec.get_privkey()
hn_pubkey = ec.get_pubkey()
binascii.hexlify(hn_pubkey)
b'5a8d38864820197c3394b92613b20b91633cbd897119273bf8e4a6f4eec0a650'
hn = ECIES_HN(hn_privkey, profile='A')
```

Demo: CryptoMobile

```
# Decrypting incoming SUCI A from PCAP
ue_pubkey = binascii.unhexlify(
  '7b27b315a3423f7ca10fdb77028798f86b1f58fa876cc864514a8f882d33c404')
ue_ciphertext =  binascii.unhexlify('31a0371c')
ue_mac = binascii.unhexlify('7bdd02efd7162ba2')
hn_msin = hn.unprotect(ue_pubkey, ue_ciphertext, ue_mac)
binascii.hexlify(hn_msin)

> b'00000100'
# IMSI is 2089300000100 MCC and MNC in cleartext PCAP

# Decrypting incoming SUCI B from PCAP
ue_pubkey = binascii.unhexlify(
  'b34b34516dafed6973956d4cdd548d1e5d568bba76f29a9a0c17e62c28349239')
ue_ciphertext =  binascii.unhexlify('2f1fd3e7')
ue_mac = binascii.unhexlify('e158a42f076118da')
hn_msin = hn.unprotect(ue_pubkey, ue_ciphertext, ue_mac)
binascii.hexlify(hn_msin)
> b'00000101'
# IMSI is 2089300000101 MCC and MNC in cleartext PCAP
```

Summary

Introduction to 5G

- The 5G wonderland
  - 20Gbps, ultra low latency
  - New use cases, new network concepts
- Improvements
  - Service-based architecture
  - User plane integrity protection
  - Interconnection security
  - Enhanced subscriber privacy
- Digging through the specification
- Decrypting SUCIs

Acronyms

5G NR	5G New Radio
5G NSA	5G Non-Standalone
5G SA	5G Standalone
5GC	5G Core
AF	Application Function
AMF	Access and Mobility Management Function
AKA	Authentication and Key Agreement
AUSF	Authentication Server Function
eNodeB	Evolved NodeB
ECIES	Elliptic Curve Integrated Encryption Scheme
EEA	EPS Encryption Algorithm
EPC	Evolved Packet Core
E-UTRAN	Evolved Universal Terrestrial Radio Access
gNodeB	gNodeB
GUTI	Global Unique Temporary Identifier
HPLMN	Home PLMN
HSS	Home Subscriber Service
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
MAC	Medium Access Control
MCC	Mobile Country Code
MME	Mobility Management Entity
MNC	Mobile Network Code
MSIN	Mobile Station Identification Number
NAI	Network Access Identifier
NAS	Non-Access Stratum
NAS-MM	NAS Mobility Management
NAS-SM	NAS Session Management
NEF	Network Exposure Function
NGAP	NG Application Protocol
NRF	Network Respository Function
NSSF	Network Slice Selection Function
P-GW	PDN Gateway
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PHY	Physical Layer
PRINS	PRotocol for N32 INterconnect Security
RAN	Radio Access Network
RA-RNTI	Random Access RNTI
RLC	Radio Link Control
RNTI	Radio Network Temporary Identity
ROHC	Robust Header Compression
RRC	Radio Resource Control
RTP	Real-Time Transport Protocol
SCTP	Stream Control Transmission Protocol
SMF	Session Management Function
S-GW	Serving Gateway
SEPP	Security Edge Protection Proxy
SIP	Session Initiation Protocol
SMF	Session Management Function
SRTP	Secure Real-Time Transport Protocol
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SS7	Signalling System 7
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UDM	Unified Data Management
UPF	User Plane Function
VPLMN	Visiting PLMN