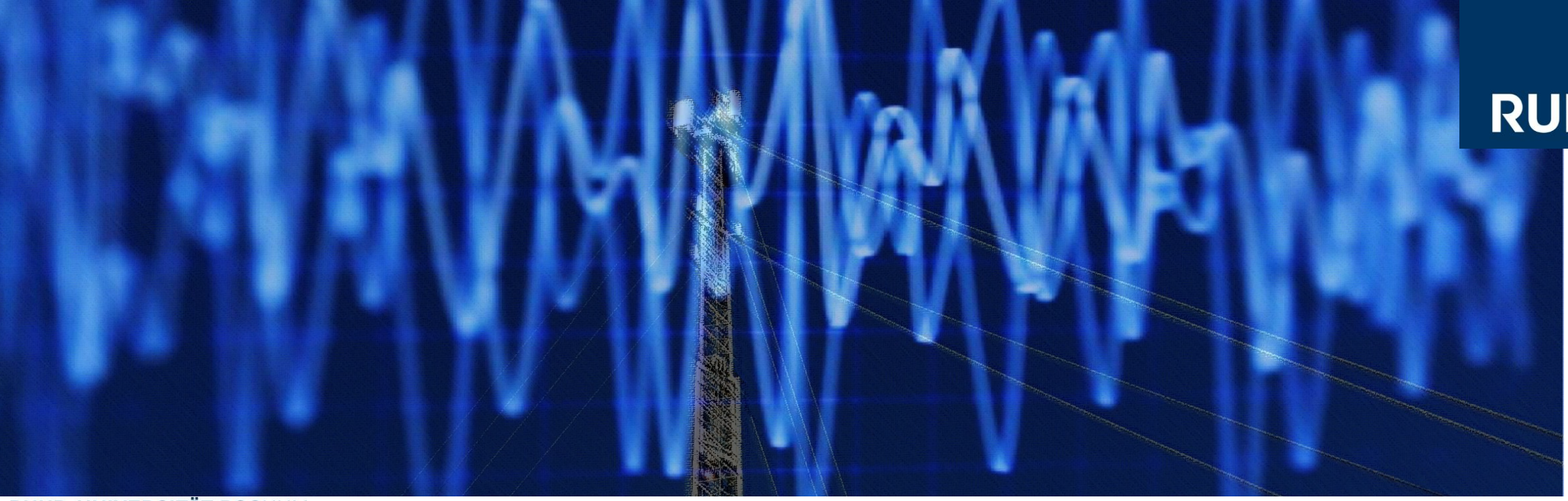


RUB

RUHR-UNIVERSITÄT BOCHUM

Putting LTE Security Functions to the Test:
A Framework to Evaluate Implementation Correctness

David Rupprecht
Ruhr-University Bochum

Kai Jansen
Ruhr-University Bochum

Christina Pöpper
NYU Abu Dhabi

hgi
Horst Görtz Institute for IT-Security

UbiCrypt
Cryptography in Ubiquitous Computing

More than **8 billion** mobile subscribers estimated for 2019 [1]

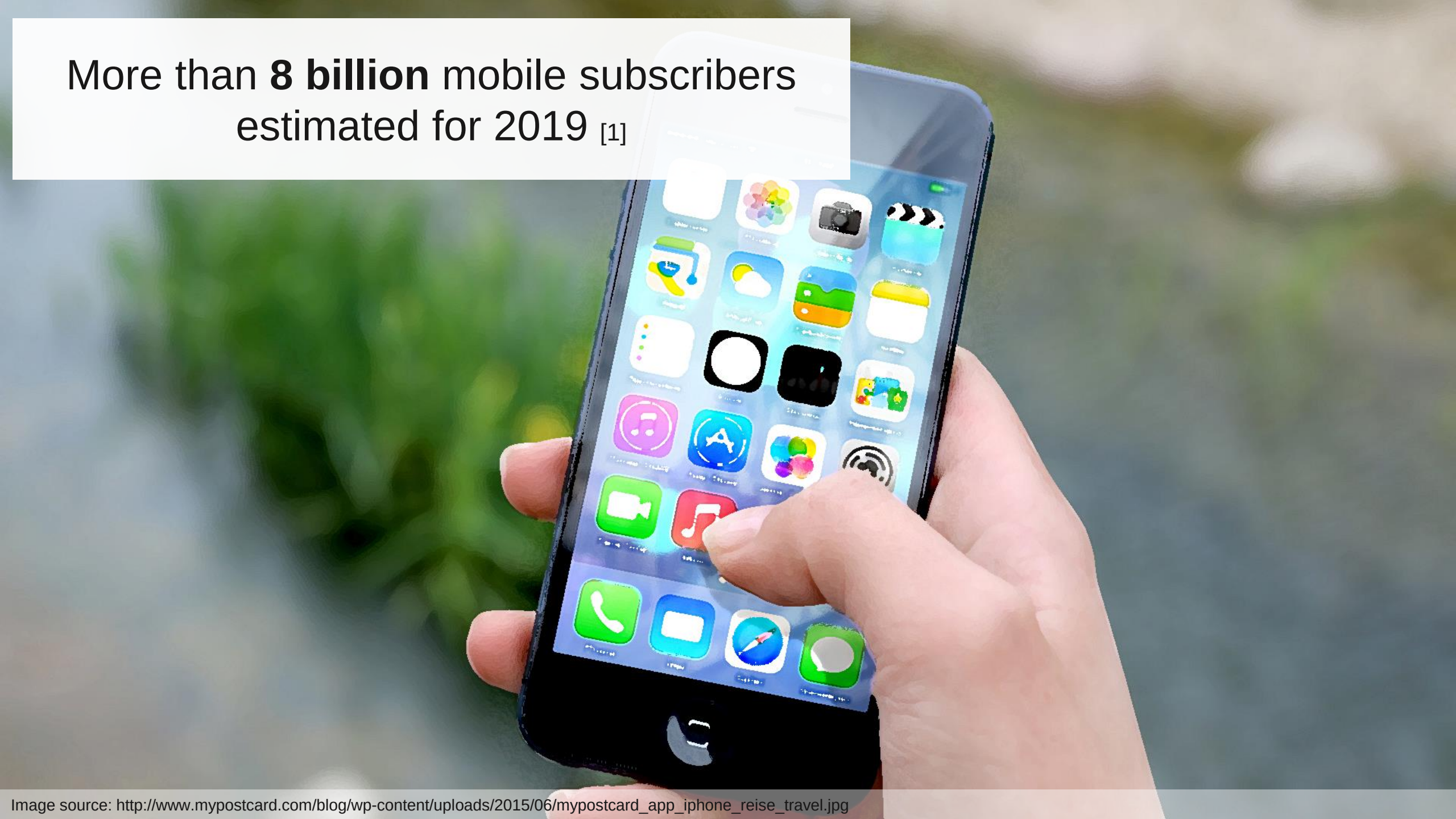


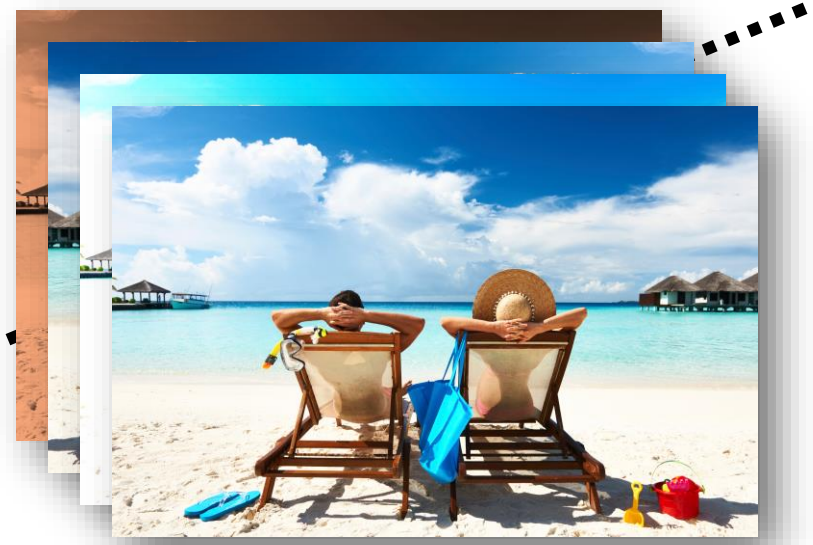
Image source: http://www.mypostcard.com/blog/wp-content/uploads/2015/06/mypostcard_app_iphone_reise_travel.jpg



Image source: http://www.blogcdn.com/slideshows/images/slides/279/787/9/S2797879/slug/l/vacation-1.jpg





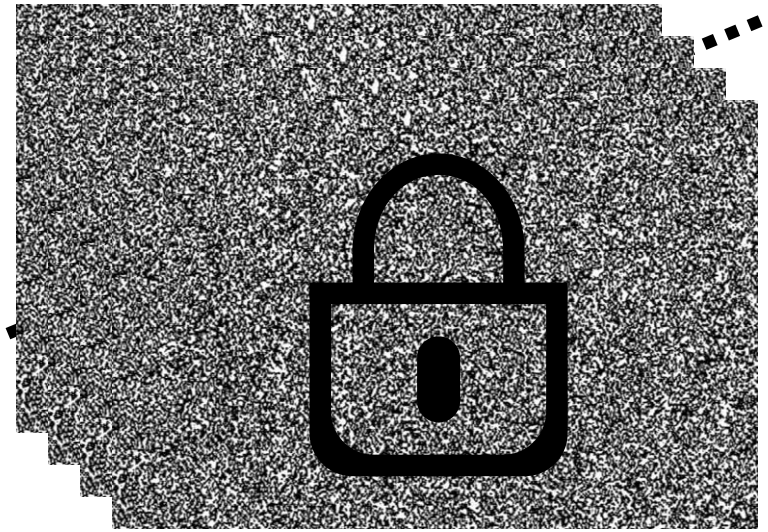




Eavesdropping of unencrypted data









LTE provides
mutual **authentication**
and **encryption**



Implementation flaw:

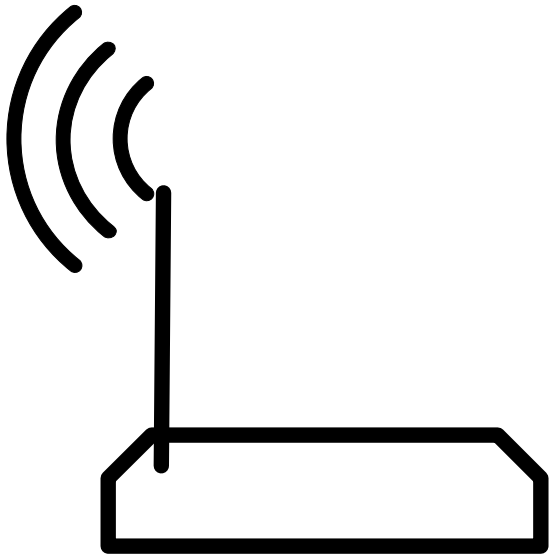
Undermine LTE security

Putting LTE Security Functions to the Test

Implementation flaws in LTE devices → Eavesdropping on private information → Testing security functions of devices





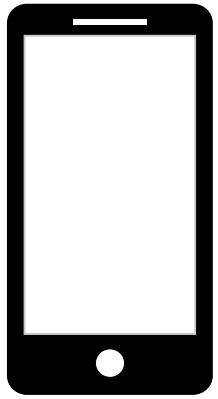


LTE Architecture

Communication Establishment and Security Algorithms

LTE Architecture

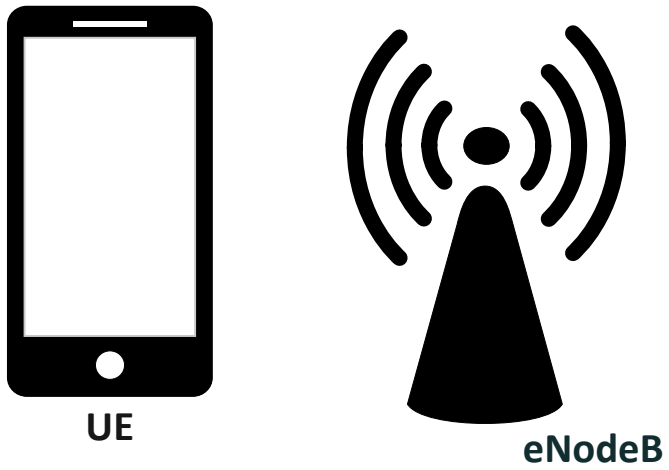
User Equipment



UE

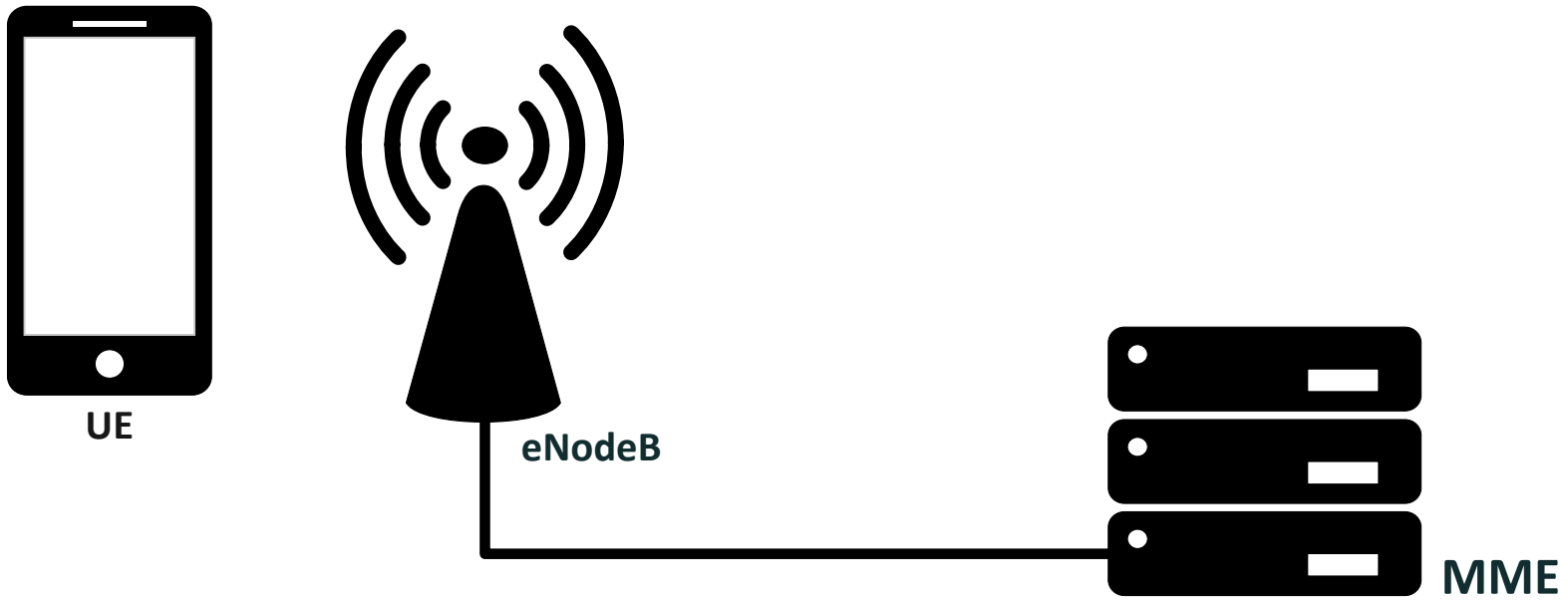
LTE Architecture

Evolved Node B

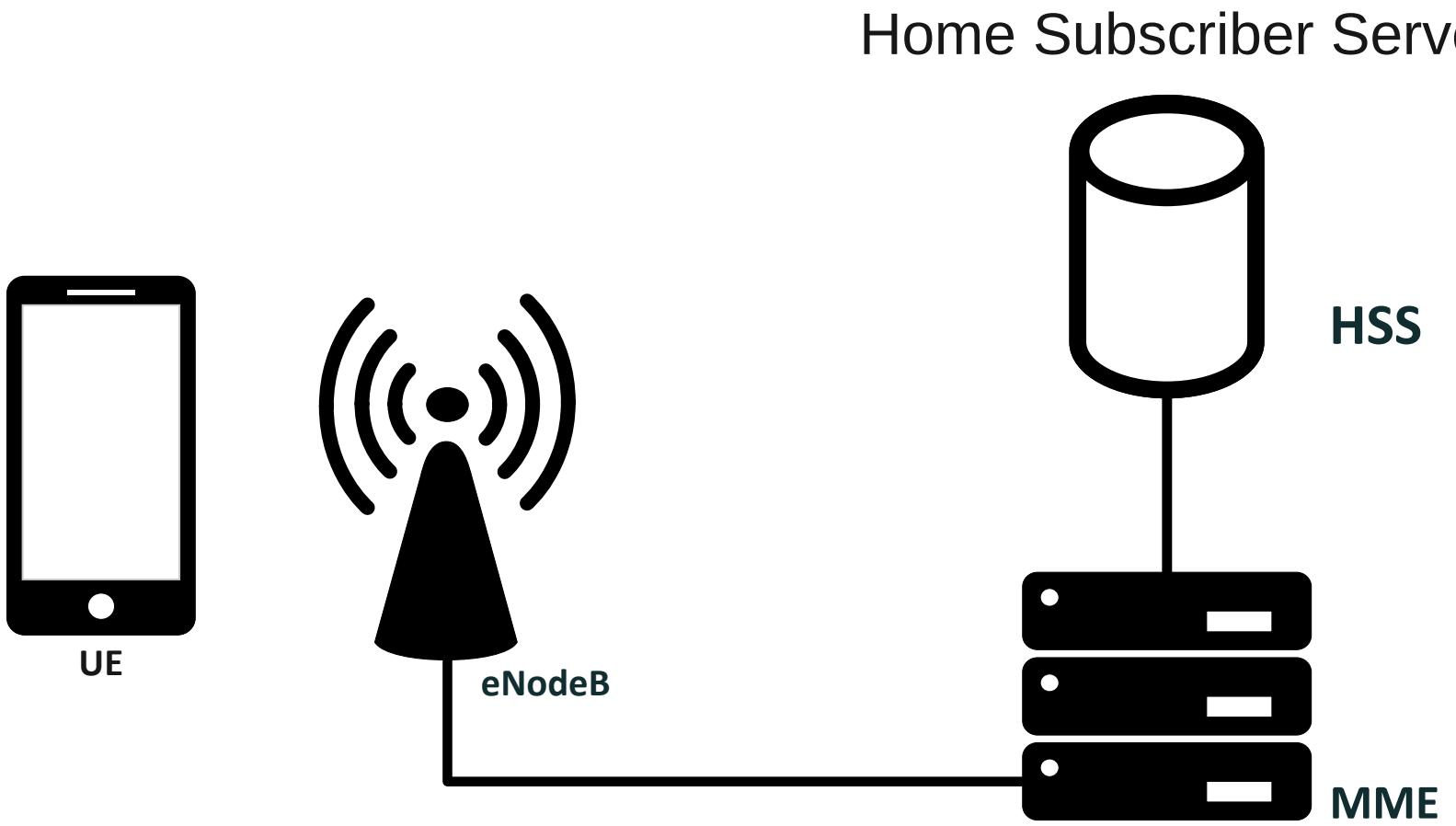


LTE Architecture

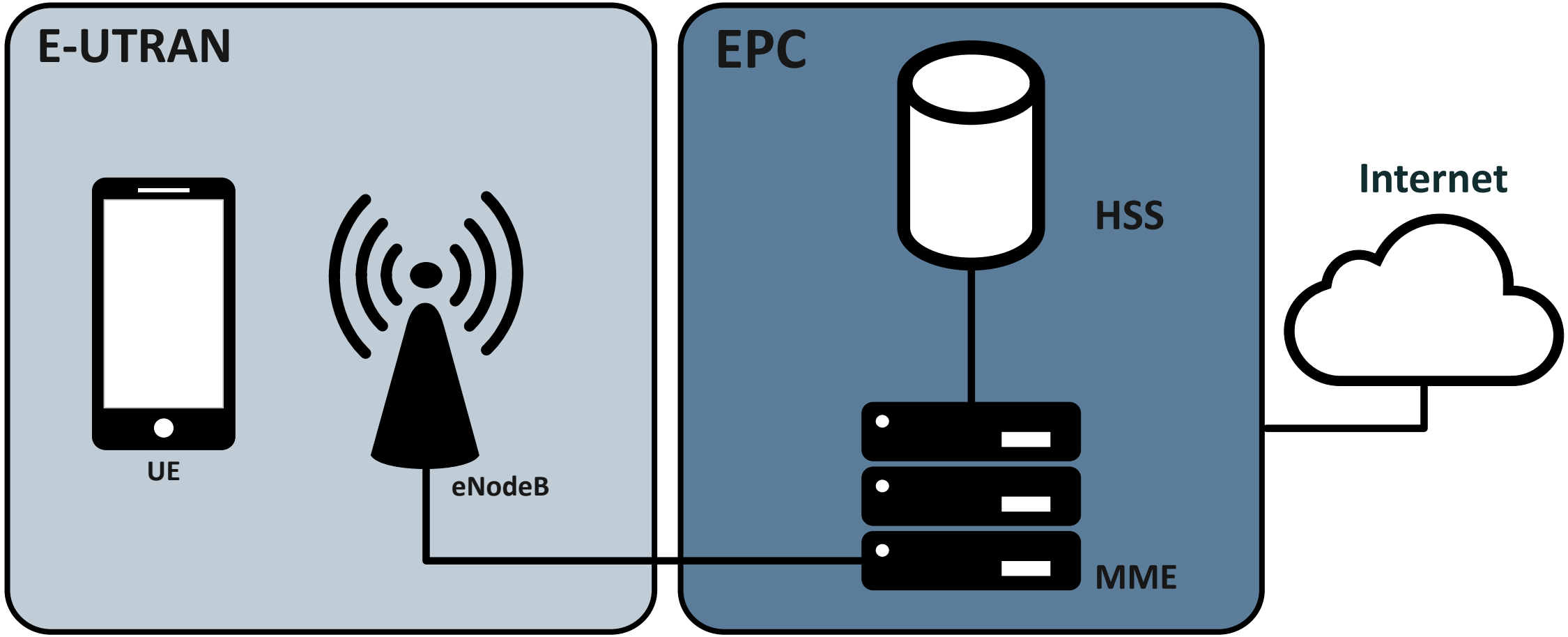
Mobility Management Entity



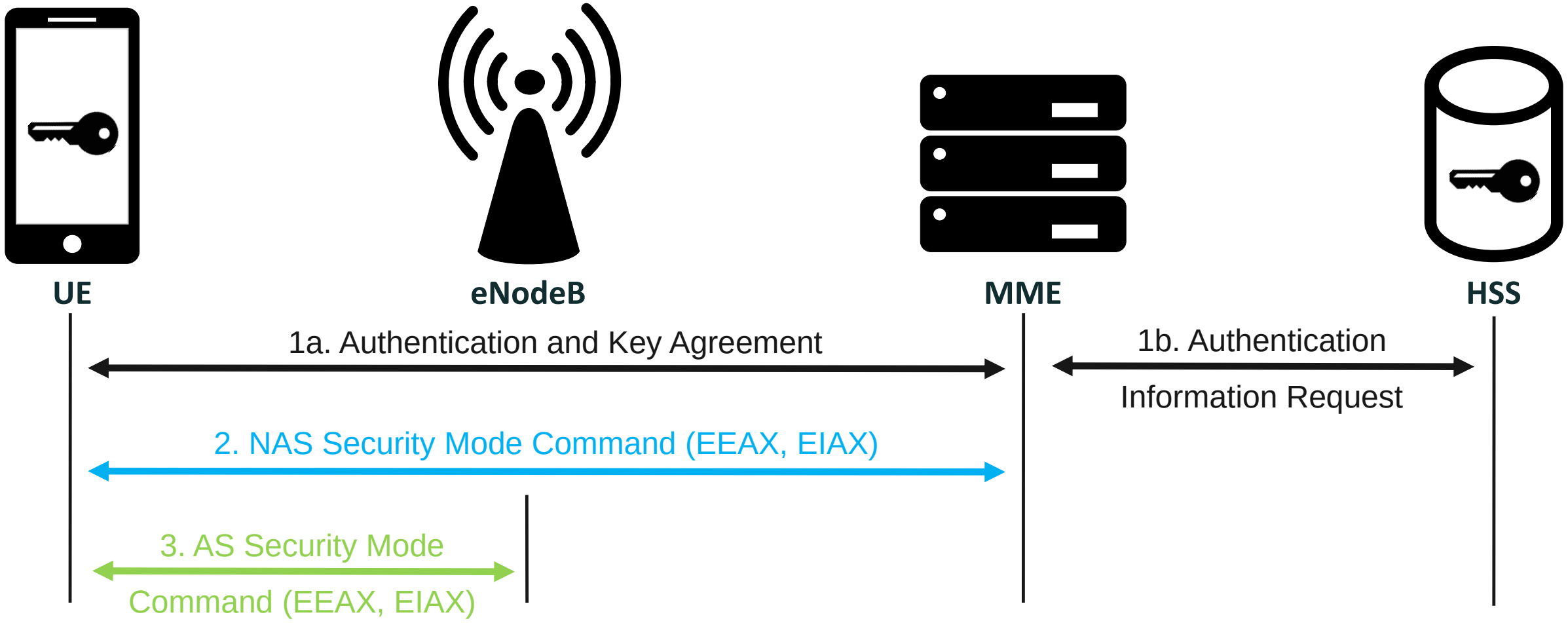
LTE Architecture



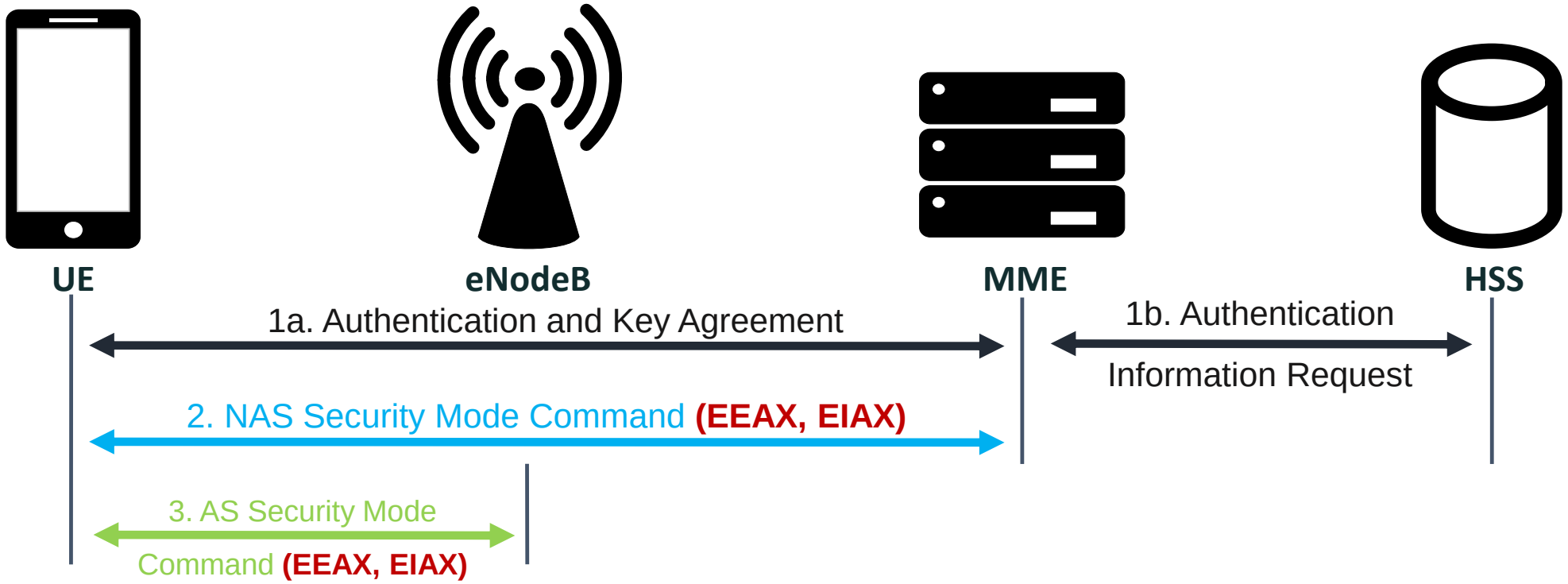
LTE Architecture



Security Procedures

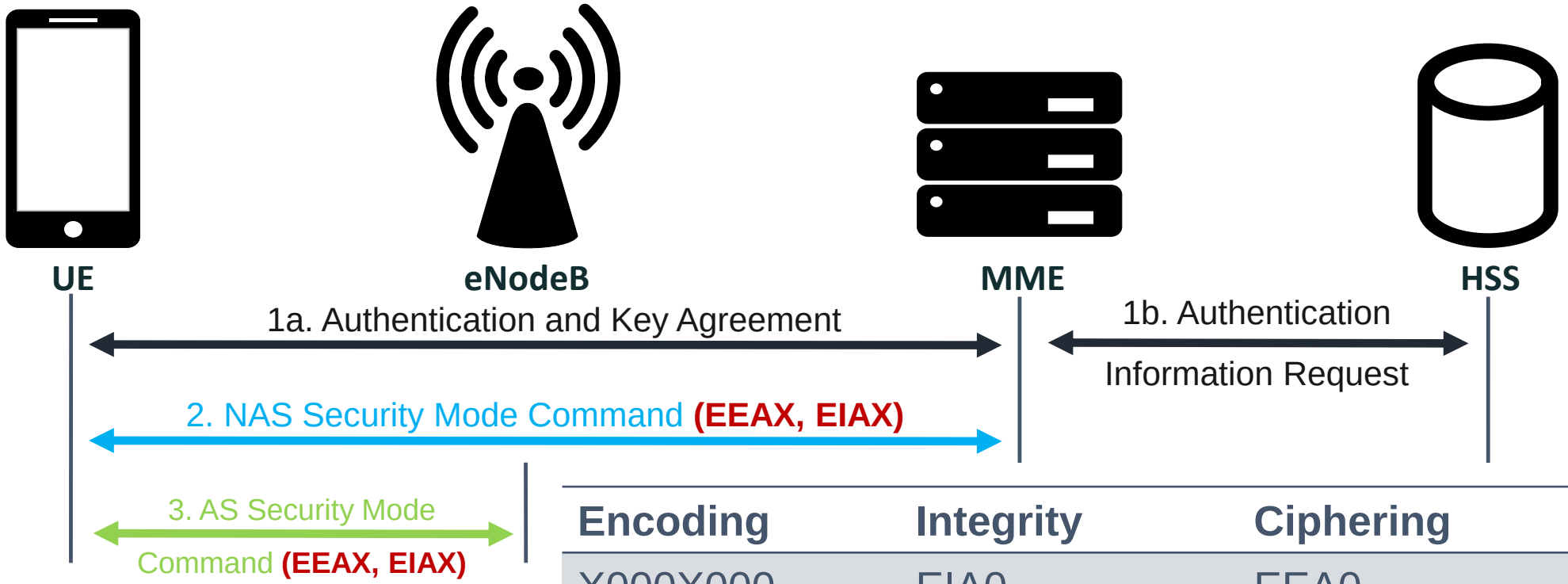


Security Algorithms



Security algorithms are selected by the provider

Security Algorithms



Security algorithms are selected by the provider

Encoding	Integrity	Ciphering	Algorithm
X000X000	EIA0	EEA0	NULL
X001X001	128-EIA1	128-EEA1	SNOW3G
X010X010	128-EIA2	128-EEA2	AES
X011X011	128-EIA3	128-EEA3	ZUC

Security Algorithms



Null Algorithms: **No Security**

X000X000	EIA0	EEA0	NULL
X001X001	128-EIA1	128-EEA1	SNOW3G
X010X010	128-EIA2	128-EEA2	AES
X011X011	128-EIA3	128-EEA3	ZUC

Security algorithms are selected by the provider

NULL Algorithms





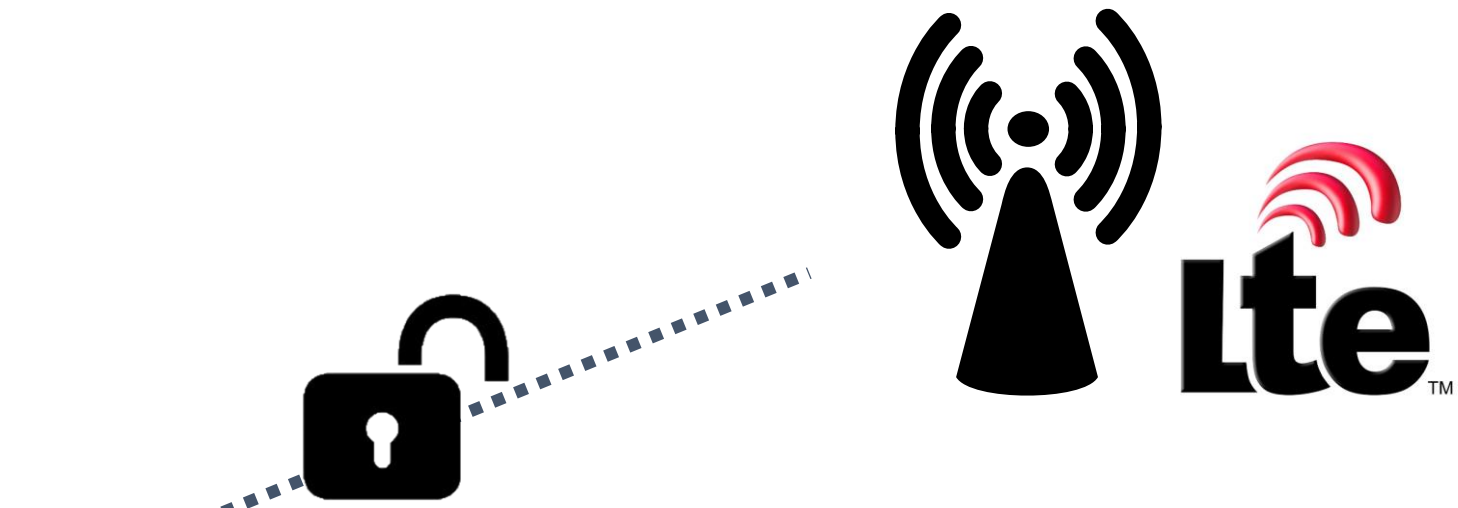
Null Integrity:
Emergency calls even
when no key is available

Encoding	Integrity	Ciphering	Algorithm
X000X000	EIA0	EEA0	NULL

Image source: https://www.percona.com/sites/default/files/icons/emergency.png

NULL Algorithms





Null Encryption:

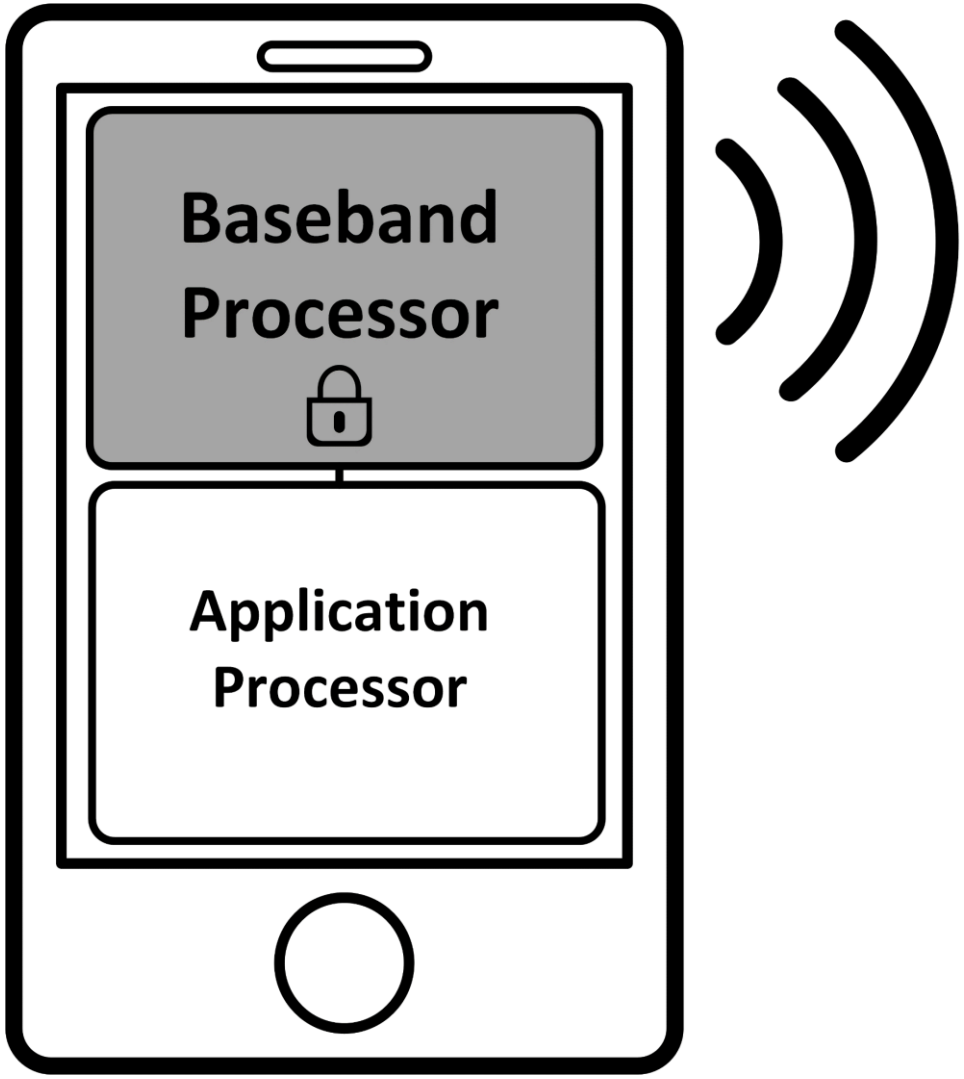
1. Ciphering indicator
2. SIM card flag
3. User interface

Encoding	Integrity	Ciphering	Algorithm
X000X000	EIA0	EEA0	NULL

Framework

Design and Tests

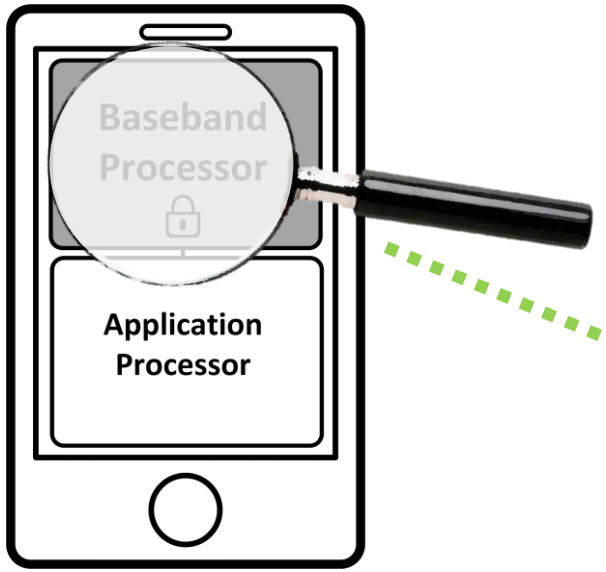
Baseband



Security functions are implemented on the Baseband

- Processor for communication:
  Qualcomm, HiSilicon, Mediatek, Samsung
- (Proprietary) Baseband is always exposed

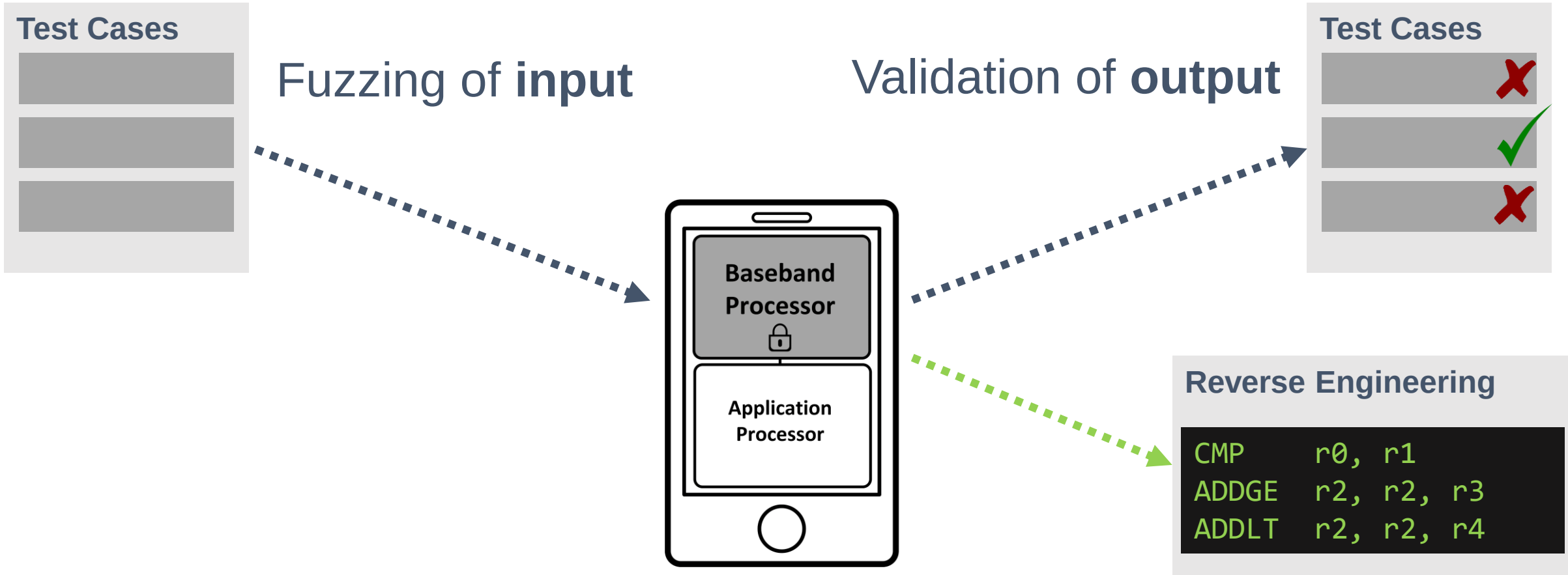
Approach



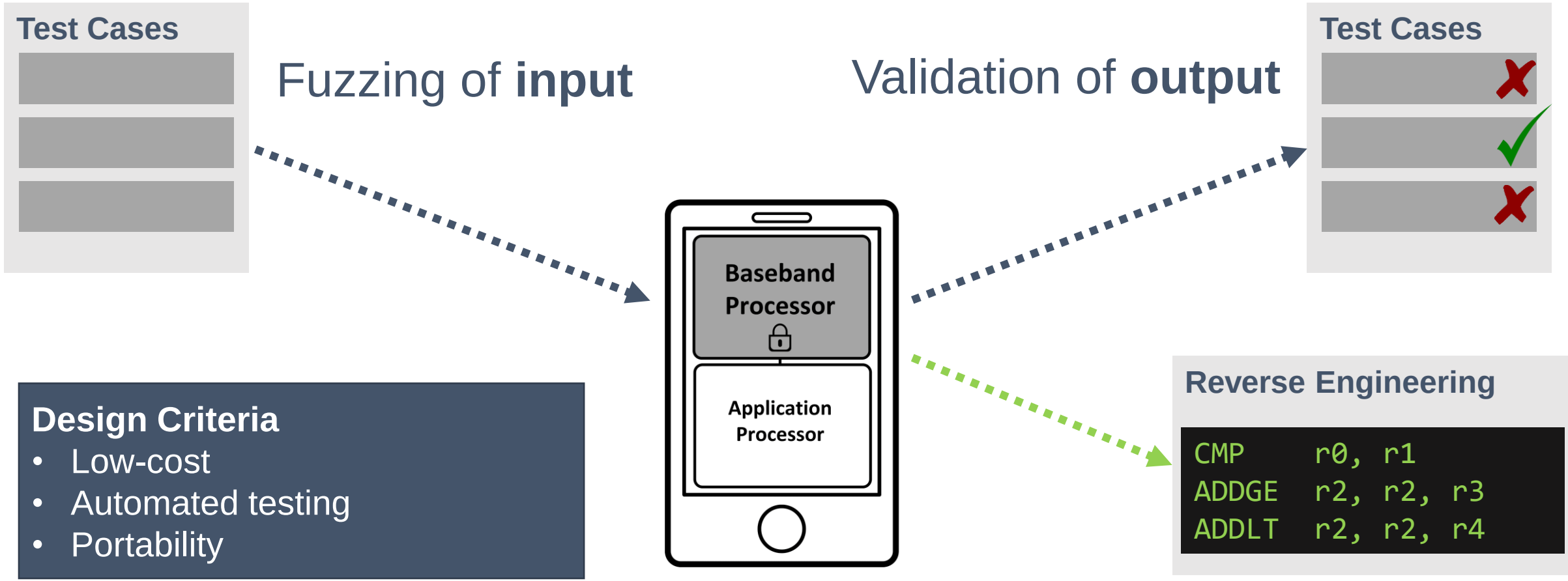
Reverse Engineering

```
CMP     r0, r1
ADDGE   r2, r2, r3
ADDLT   r2, r2, r4
```

Approach


Test Cases
Fuzzing of **input**
Validation of **output**
Test Cases
Baseband Processor
Application Processor
Reverse Engineering
CMP r0, r1
ADDGE r2, r2, r3
ADDLT r2, r2, r4

Approach



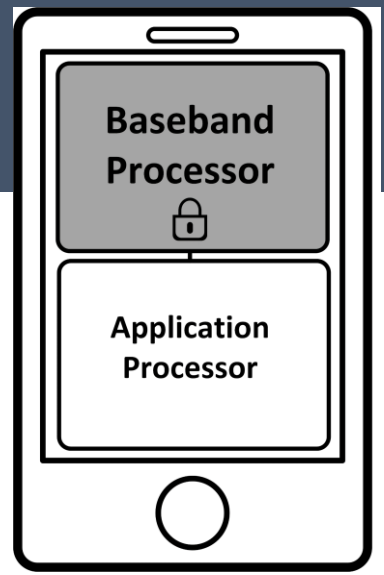
Design Criteria
- Low-cost
- Automated testing
- Portability

Approach

Fuzzing (our choice)

Test Cases

Fuzzing of **input**



Validation of **output**

Test Cases

Design Criteria
- Low-cost
- Automated testing
- Portability

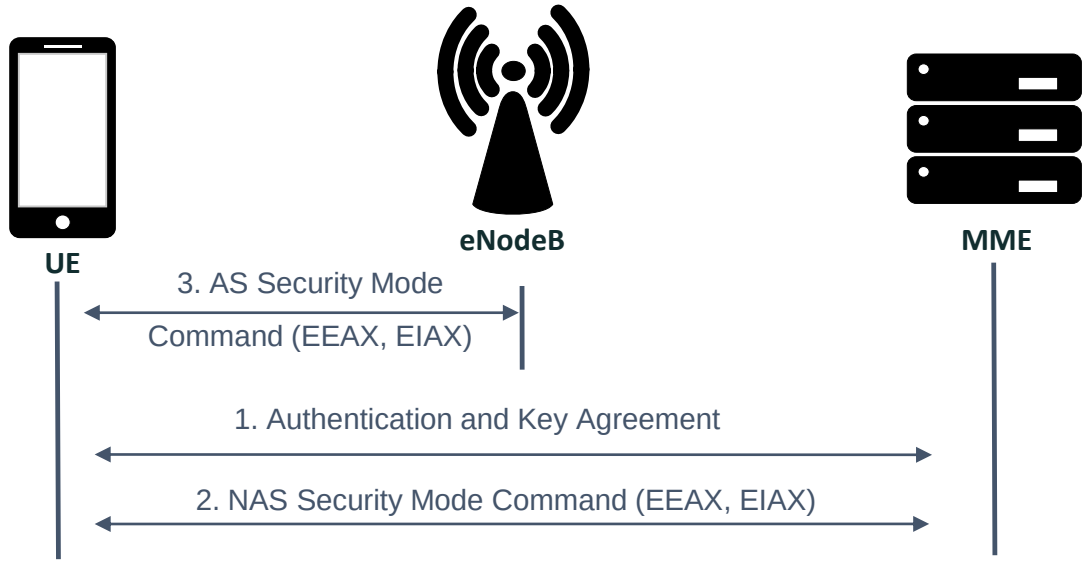
Reverse Engineering

```
CMP     r0, r1
ADDGE   r2, r2, r3
ADDLT   r2, r2, r4
```

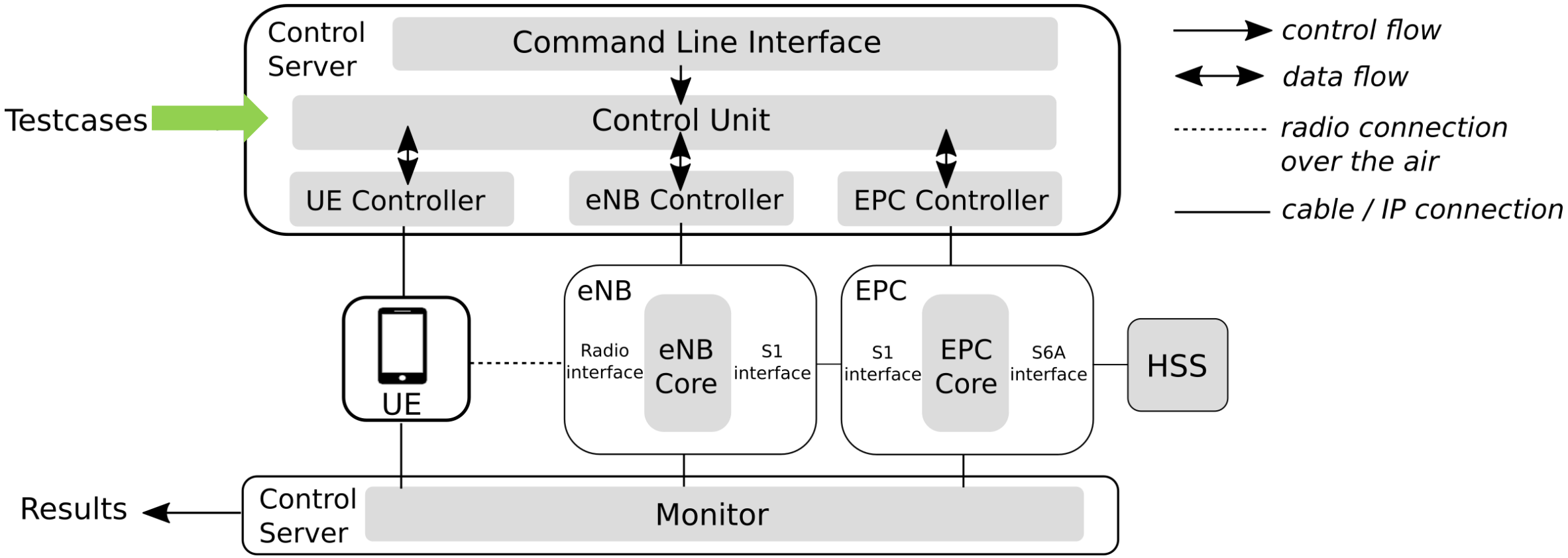
Tests

- Undefined Values
- Sequence of Messages
- Ciphering Indicator with Null Encryption

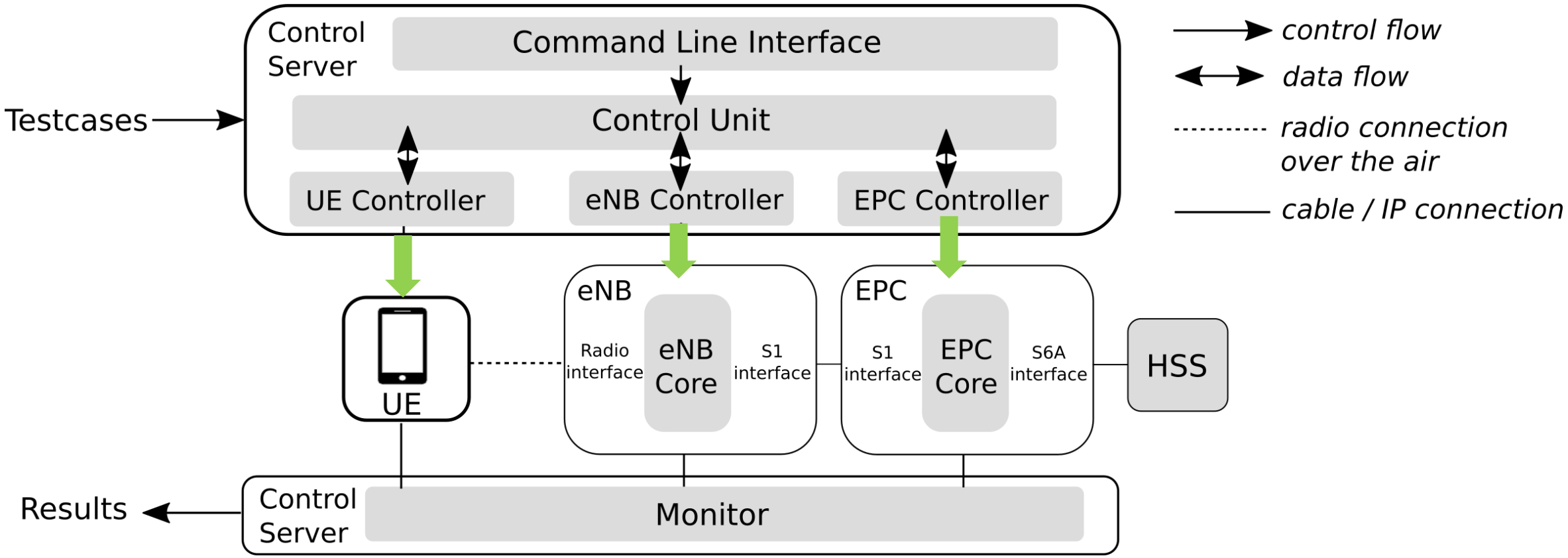
Encoding	Integrity	Ciphering	Algorithm
X000X000	EIA0	EEA0	NULL
X011X011	128-EIA3	128-EEA3	ZUC
X100X100	EIA4	EEA4	Not specified
…	…	…	…



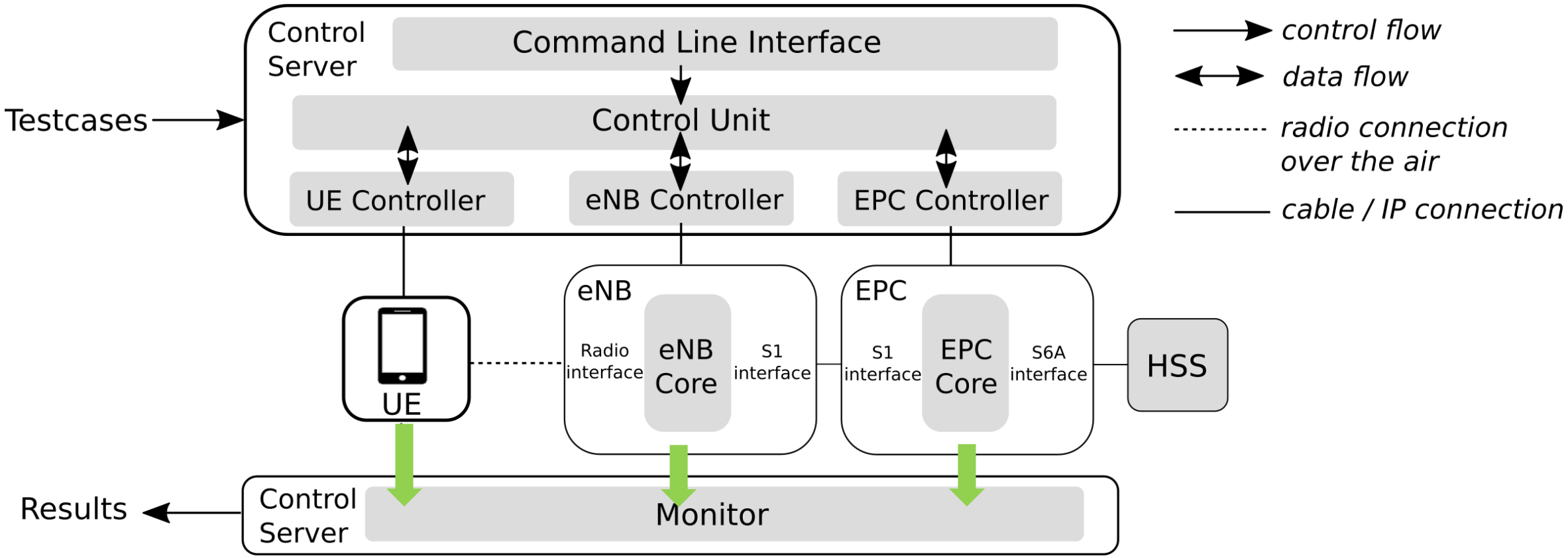
Framework Architecture



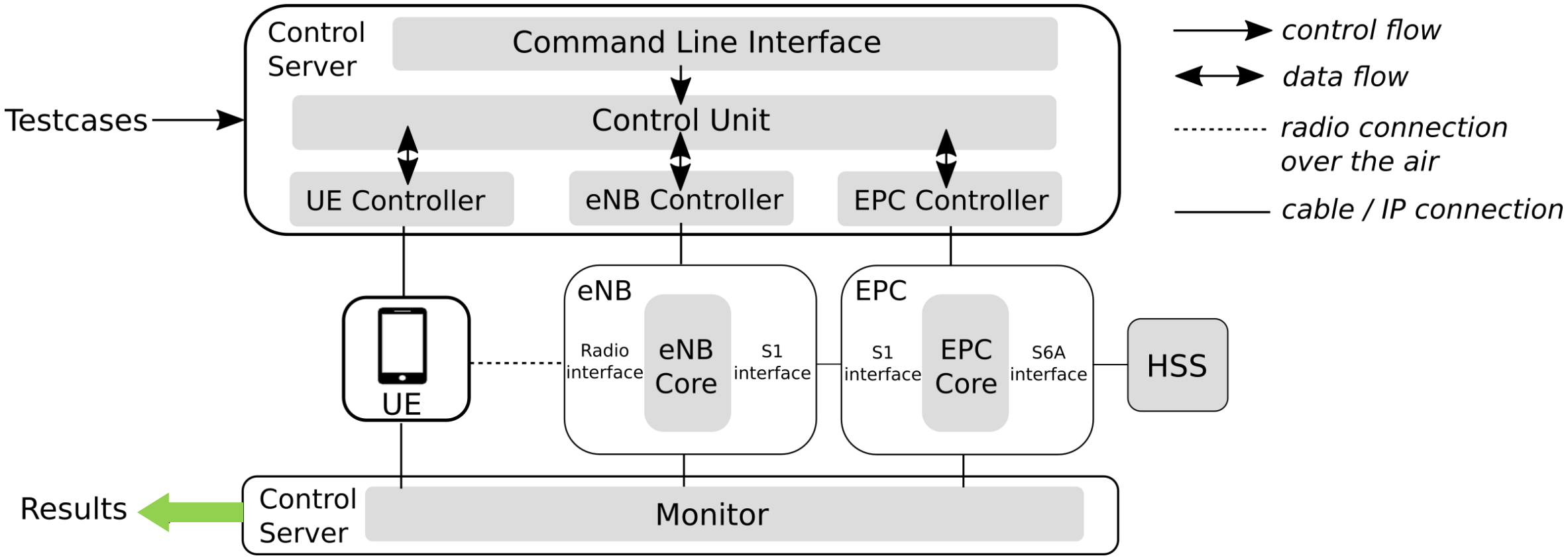
Framework Architecture

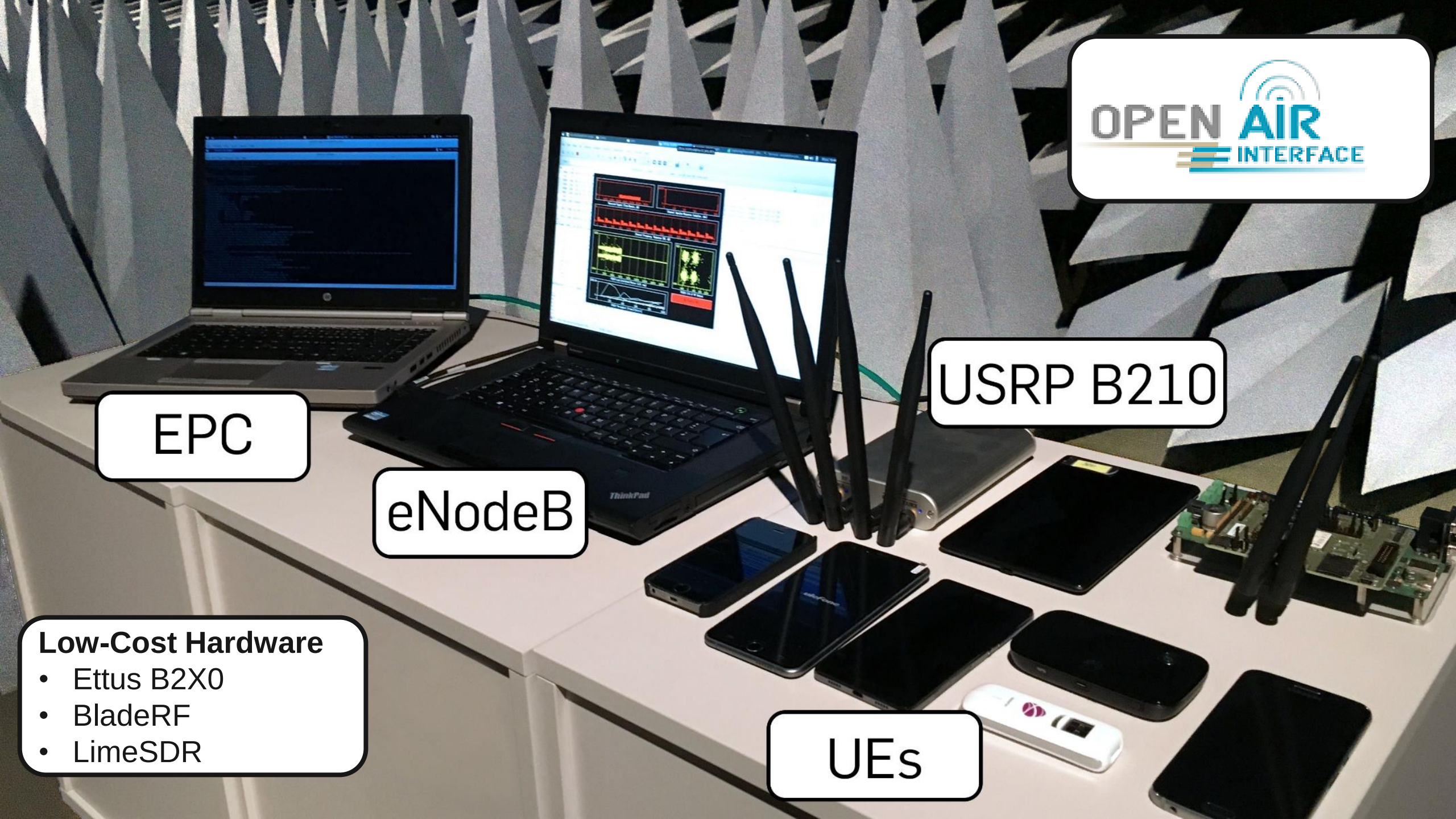


Framework Architecture



Framework Architecture




OPEN AIR INTERFACE
EPC
eNodeB
USRP B210
UEs
Low-Cost Hardware
• Ettus B2X0
• BladeRF
• LimeSDR

Evaluation

Analysis Results

Results

None of the devices show the Ciphering Indicator











	Huawei E3276 USB Dongle	Huawei E5776 Wi-Fi AP	Huawei P8 Lite	Telit EVK2 LE910	Google Nexus 5	Google Nexus 7	Apple iPhone 5s	Apple iPhone 6s	Samsung Galaxy S4	Ulefone Be Touch 2
User Data Encryption	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Network Authentication	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓

Results

Null Integrity Algorithm:
Normal data connections







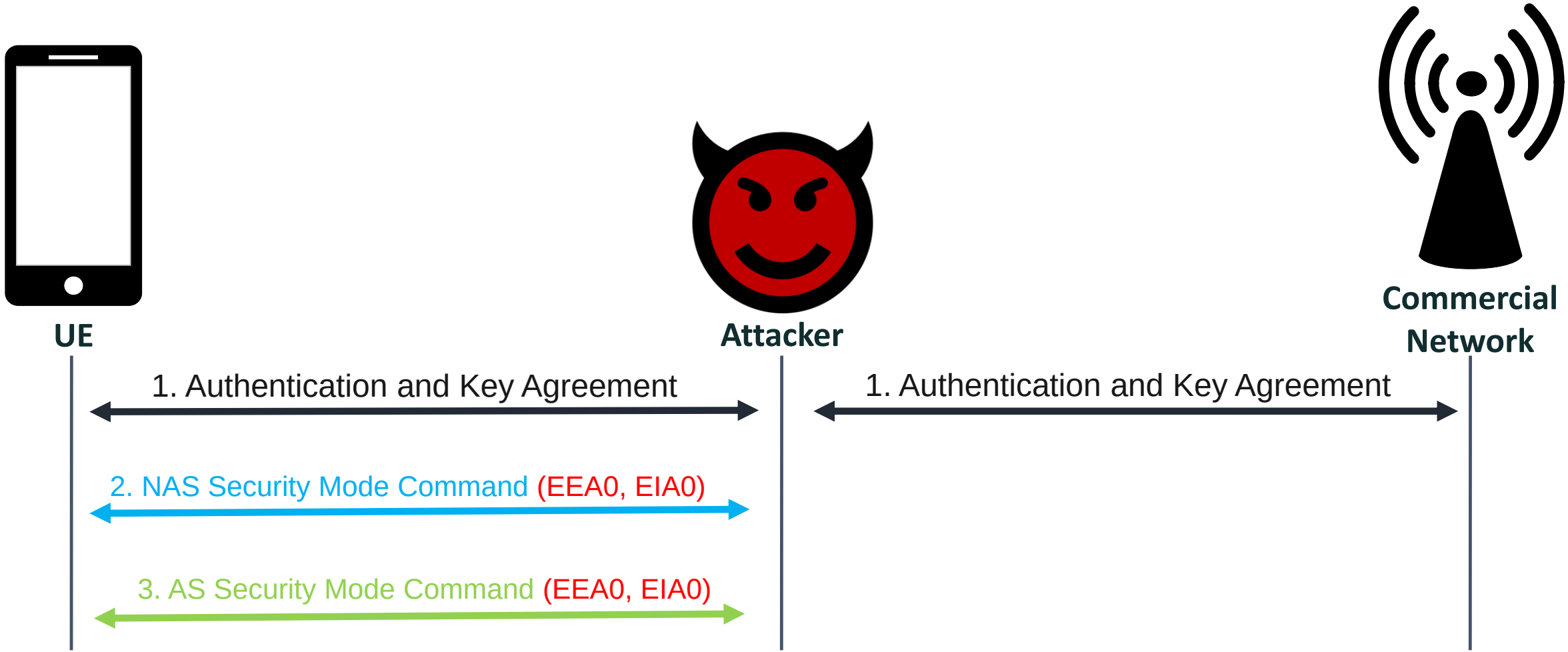






	Huawei E3276 USB Dongle	Huawei E5776 Wi-Fi AP	Huawei P8 Lite	Telit EVK2 LE910	Google Nexus 5	Google Nexus 7	Apple iPhone 5s	Apple iPhone 6s	Samsung Galaxy S4	Ulefone Be Touch 2
User Data Encryption	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Network Authentication	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓

Results


UE
Attacker
Commercial Network
1. Authentication and Key Agreement
1. Authentication and Key Agreement
2. NAS Security Mode Command (EEA0, EIA0)
3. AS Security Mode Command (EEA0, EIA0)

Conclusion

Conclusion

Implementation Flaws can Undermine the LTE Security

- No Ciphering Indicator
- Authentication procedure



Conclusion

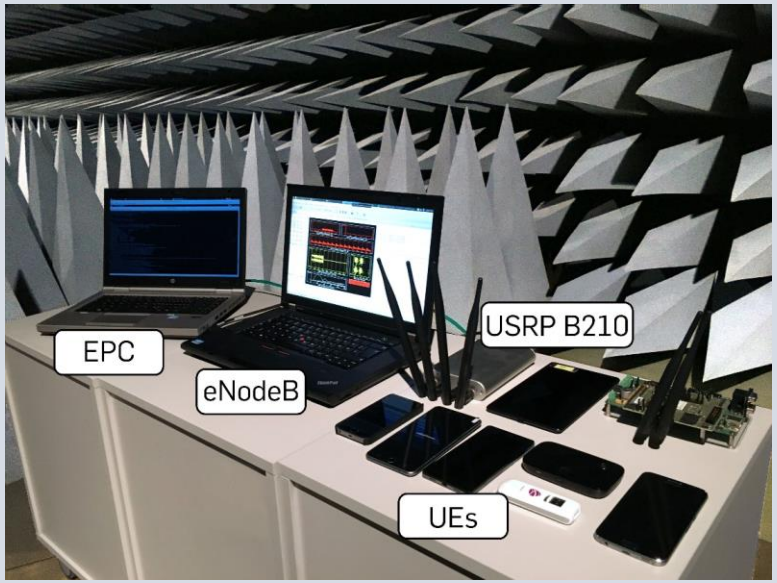
Implementation Flaws can Undermine the LTE Security

- No Ciphering Indicator
- Authentication procedure



LTE Security Testing Framework

- Low-cost
- Software Defined Radio
- Automated testing
- Logical implementation flaws



Conclusion

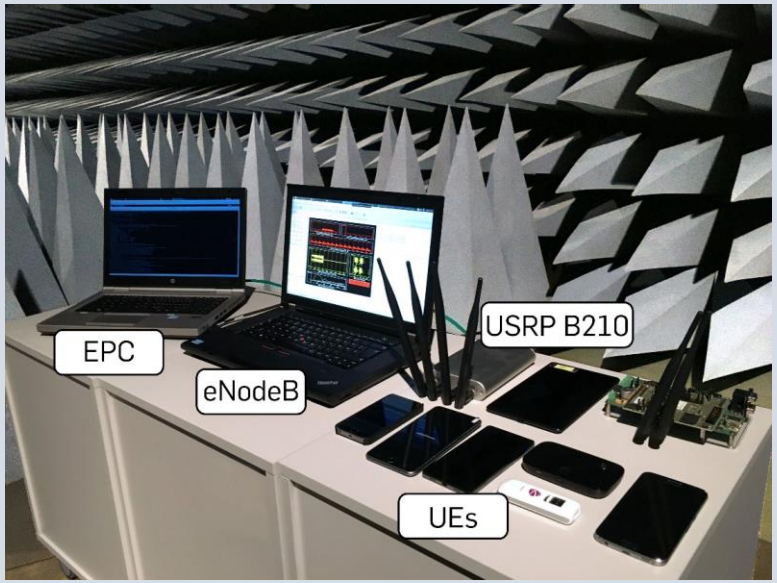
Implementation Flaws can Undermine the LTE Security

- No Ciphering Indicator
- Authentication procedure



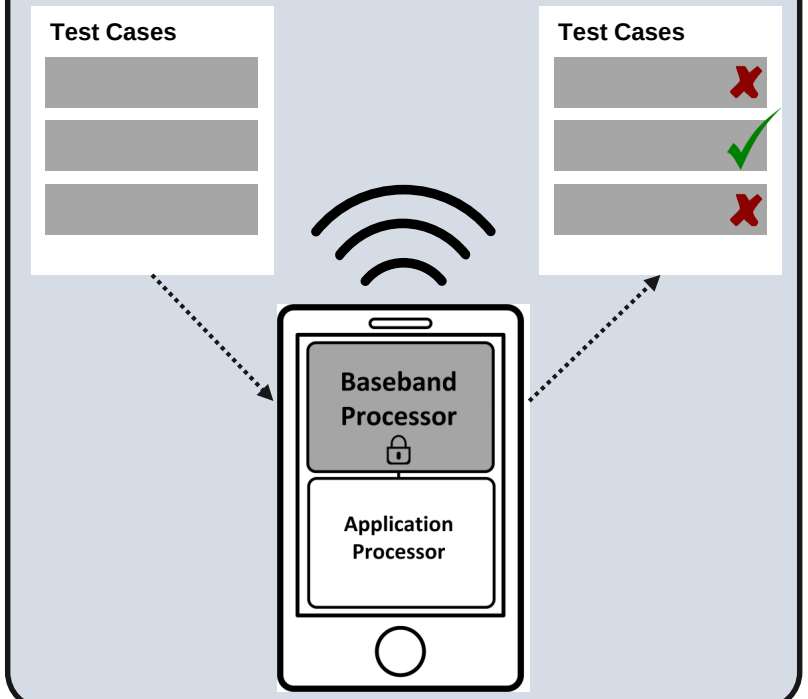
LTE Security Testing Framework

- Low-cost
- Software Defined Radio
- Automated testing
- Logical implementation flaws



Standard Test of Security Functions

- Standard Radio Testing
- Standard Security Testing



Thank You! Questions?

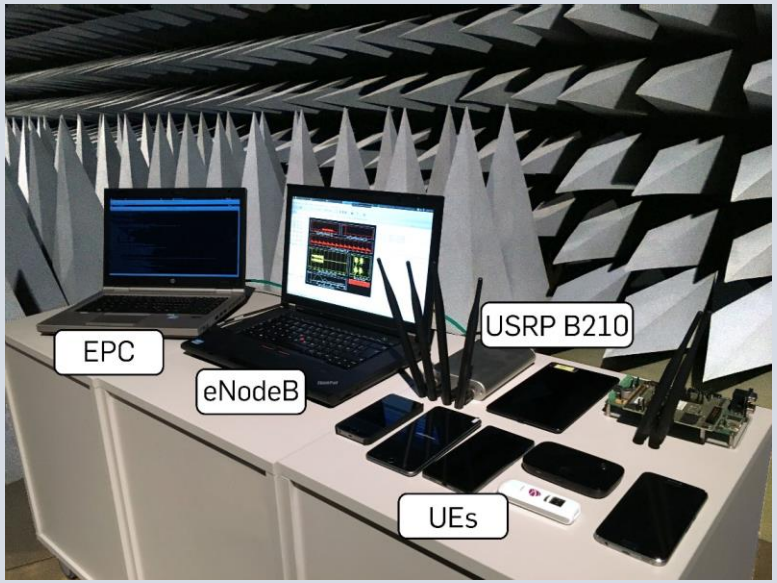
Implementation Flaws can Undermine the LTE Security

- No Ciphering Indicator
- Authentication procedure



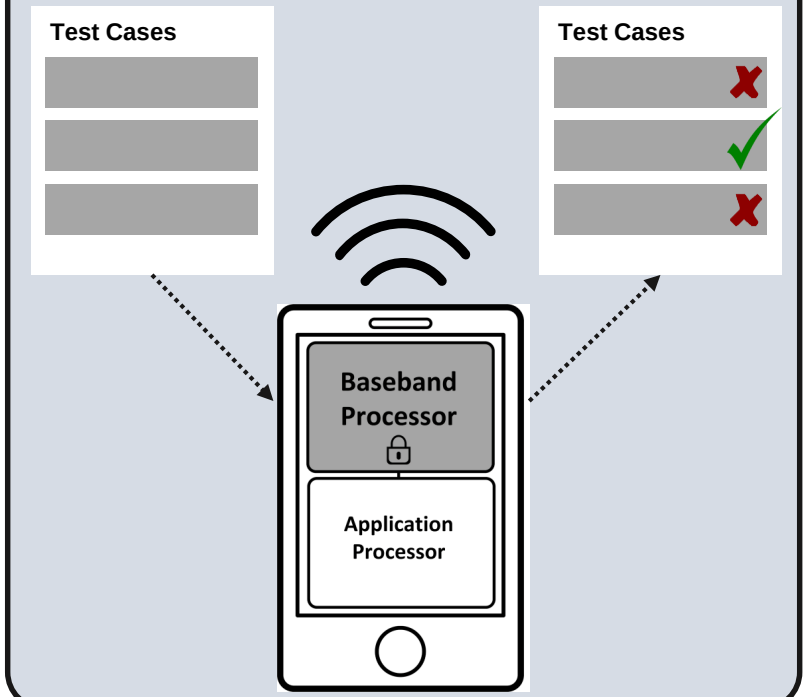
LTE Security Testing Framework

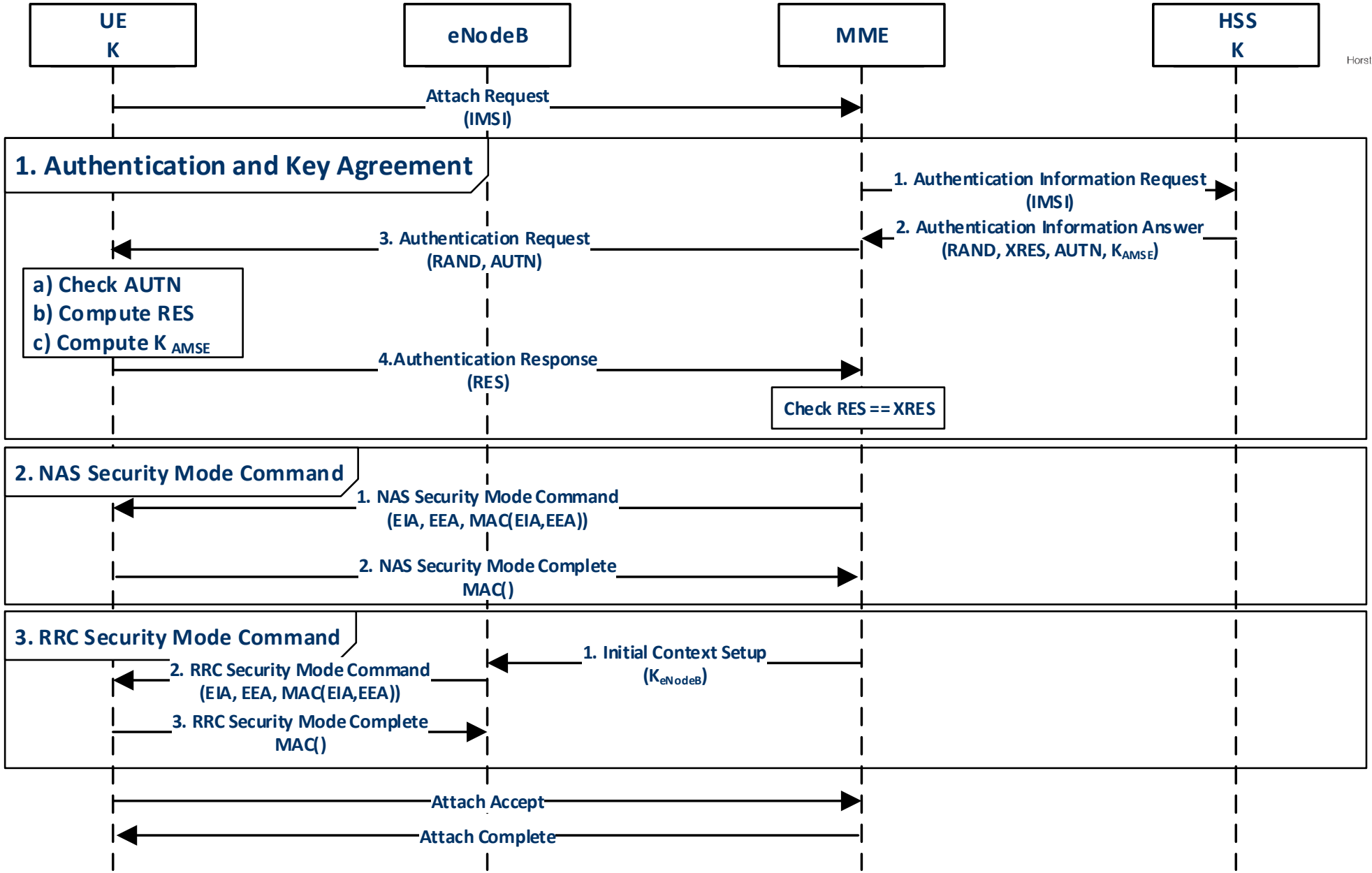
- Low-cost
- Software Defined Radio
- Automated testing
- Logical implementation flaws



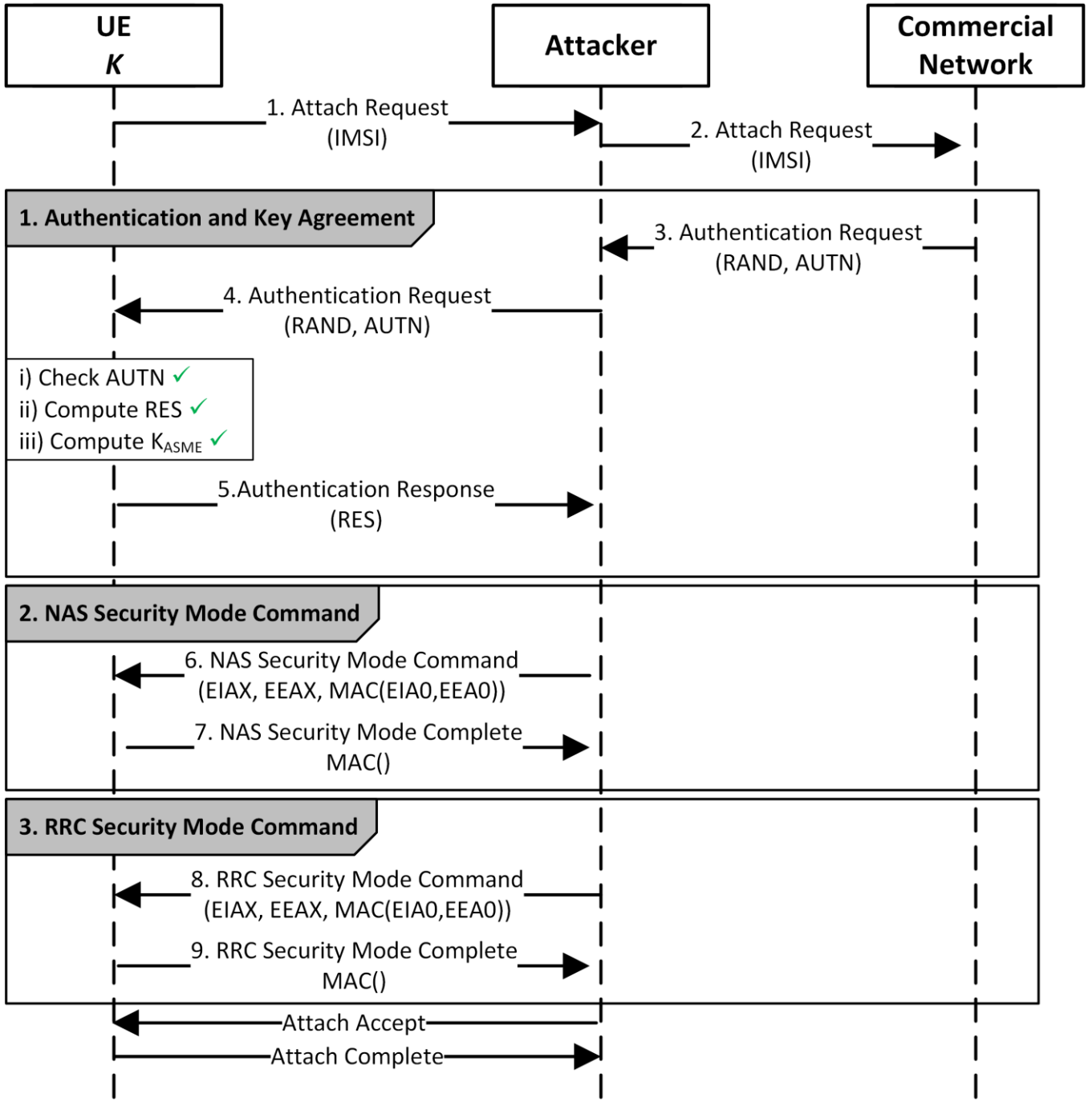
Standard Test of Security Functions

- Standard Radio Testing
- Standard Security Testing




UE
K
eNodeB
MME
HSS
K
Attach Request
(IMSI)
1. Authentication and Key Agreement
1. Authentication Information Request
(IMSI)
2. Authentication Information Answer
(RAND, XRES, AUTN, K_AMSE)
3. Authentication Request
(RAND, AUTN)
a) Check AUTN
b) Compute RES
c) Compute K AMSE
4.Authentication Response
(RES)
Check RES == XRES
2. NAS Security Mode Command
1. NAS Security Mode Command
(EIA, EEA, MAC(EIA,EEA))
2. NAS Security Mode Complete
MAC()
3. RRC Security Mode Command
1. Initial Context Setup
(K_eNodeB)
2. RRC Security Mode Command
(EIA, EEA, MAC(EIA,EEA))
3. RRC Security Mode Complete
MAC()
Attach Accept
Attach Complete

Backup


UE
K
Attacker
Commercial Network
1. Attach Request
(IMSI)
2. Attach Request
(IMSI)
1. Authentication and Key Agreement
3. Authentication Request
(RAND, AUTN)
4. Authentication Request
(RAND, AUTN)
i) Check AUTN ✓
ii) Compute RES ✓
iii) Compute K_ASME ✓
5.Authentication Response
(RES)
2. NAS Security Mode Command
6. NAS Security Mode Command
(EIAX, EEAX, MAC(EIA0,EEA0))
7. NAS Security Mode Complete
MAC()
3. RRC Security Mode Command
8. RRC Security Mode Command
(EIAX, EEAX, MAC(EIA0,EEA0))
9. RRC Security Mode Complete
MAC()
Attach Accept
Attach Complete