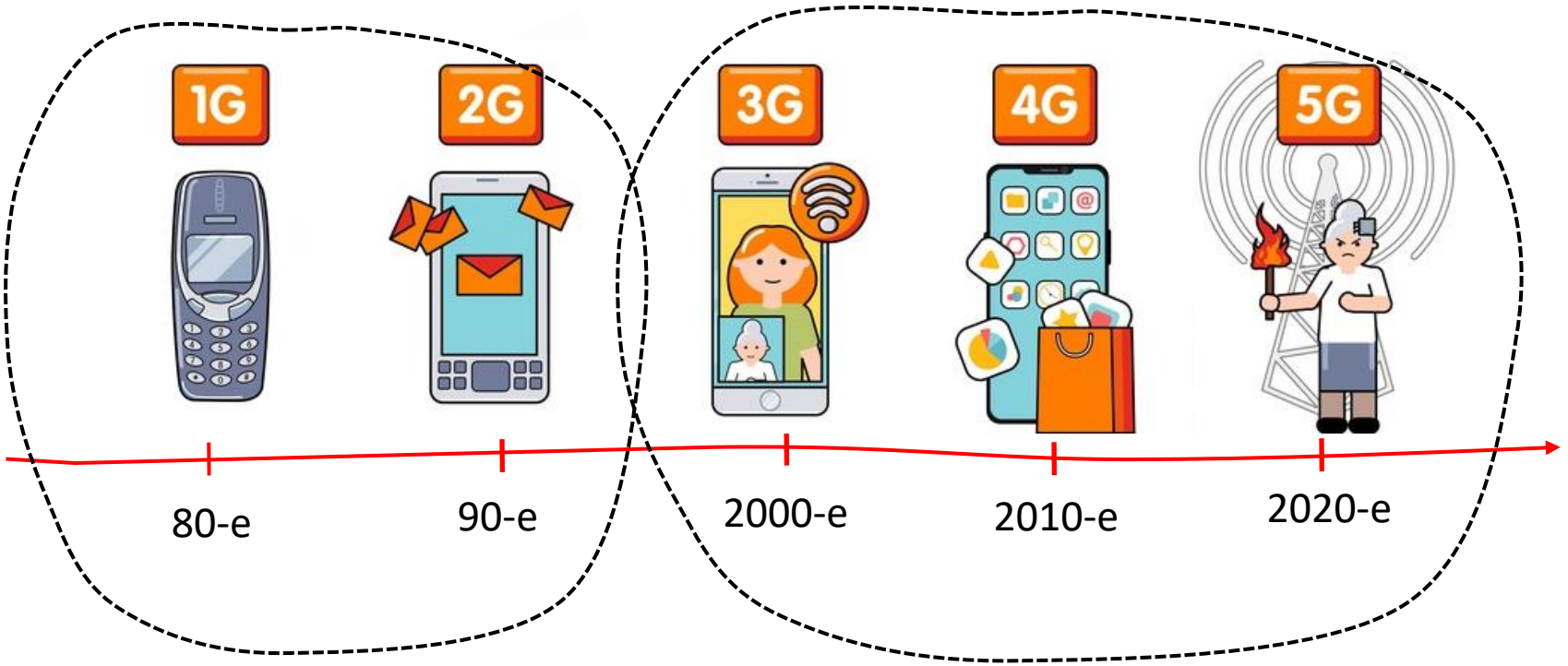
КРИПТОНИТ

О разработке отечественных аналогов криптографических алгоритмов и протоколов в сетях связи 5G/IMT-2020

Грибоедова Екатерина

Руководитель направления стандартизации,
Лаборатория криптографии

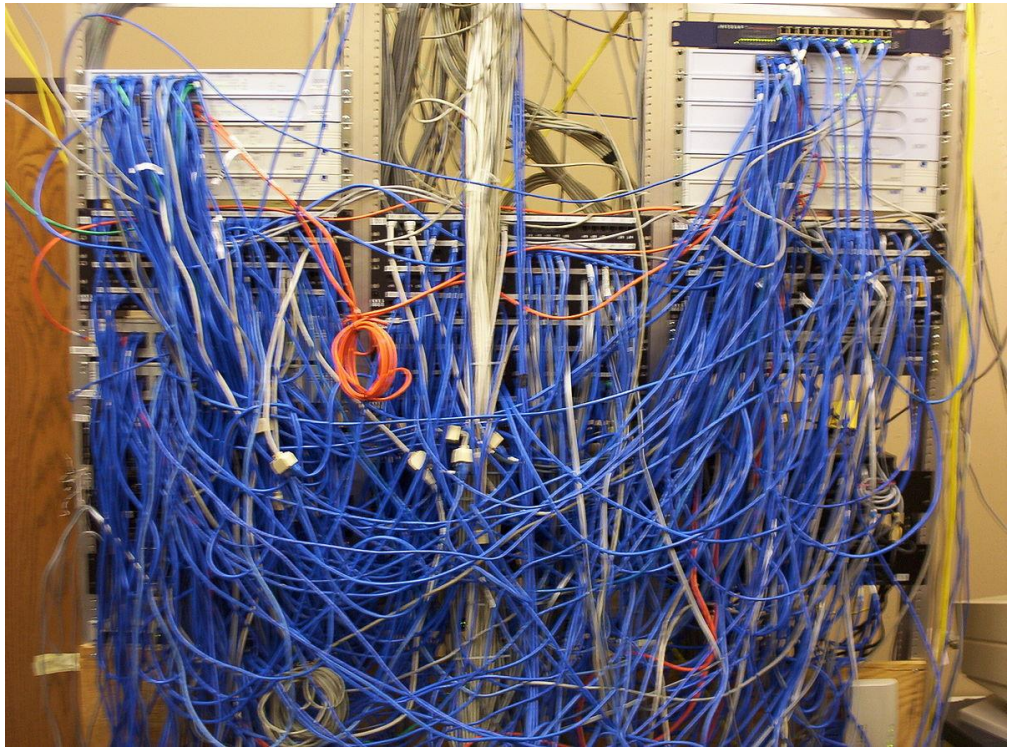
Поколения сотовой связи

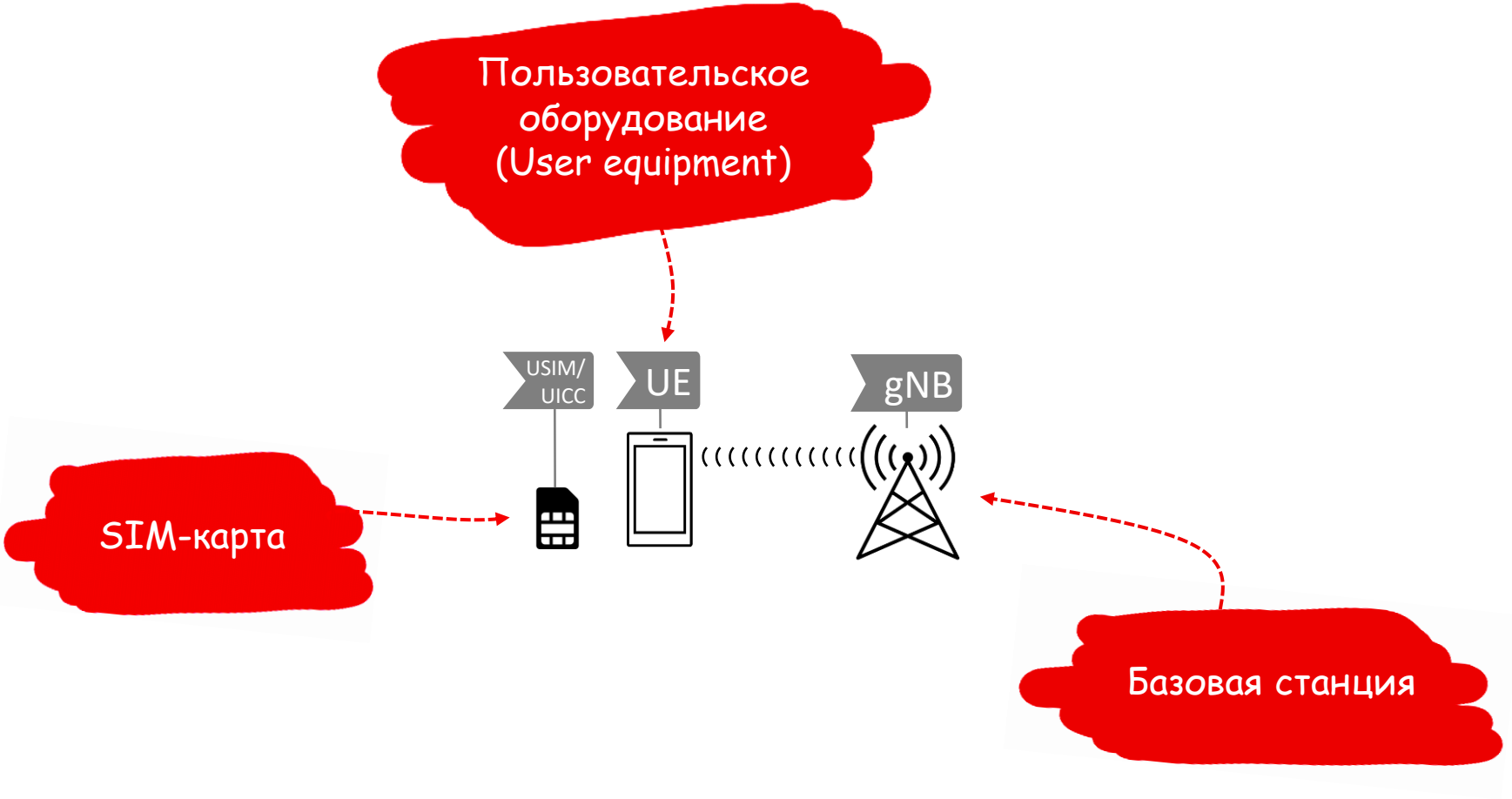


Локальные стандартизирующие организации

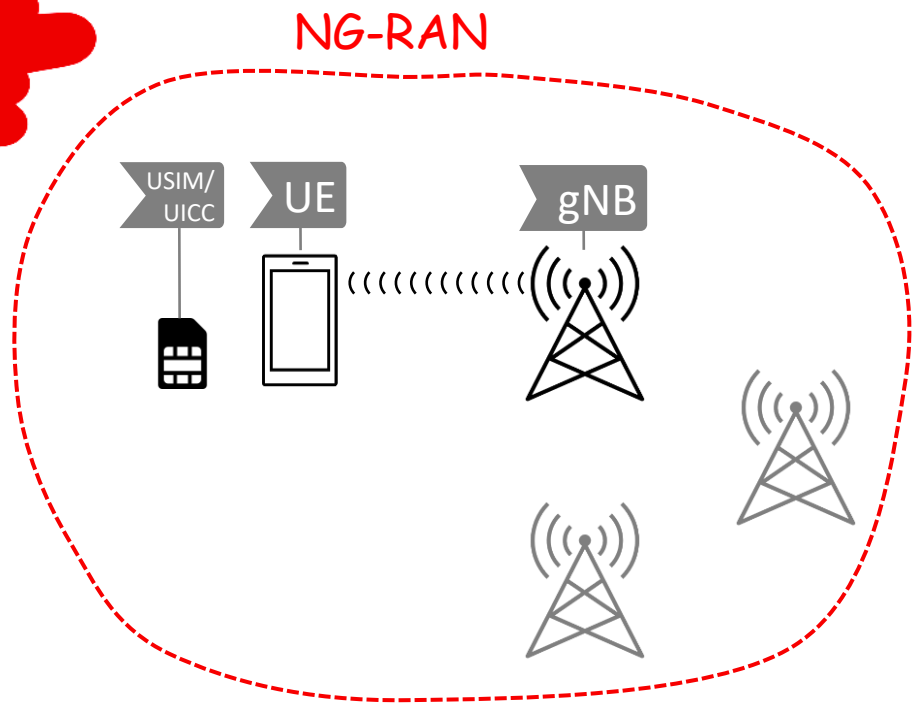
3GPP

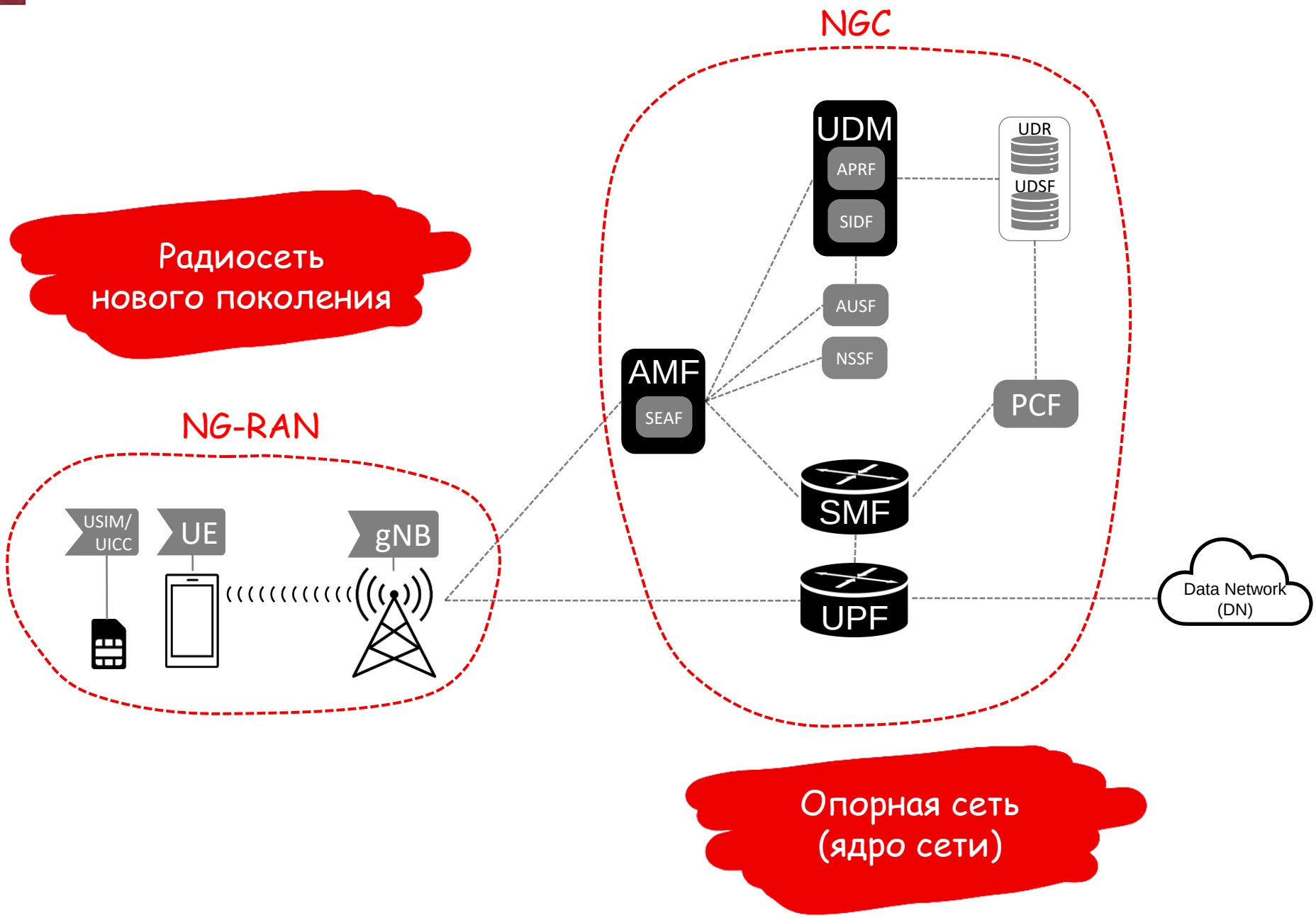
5G устройство сети

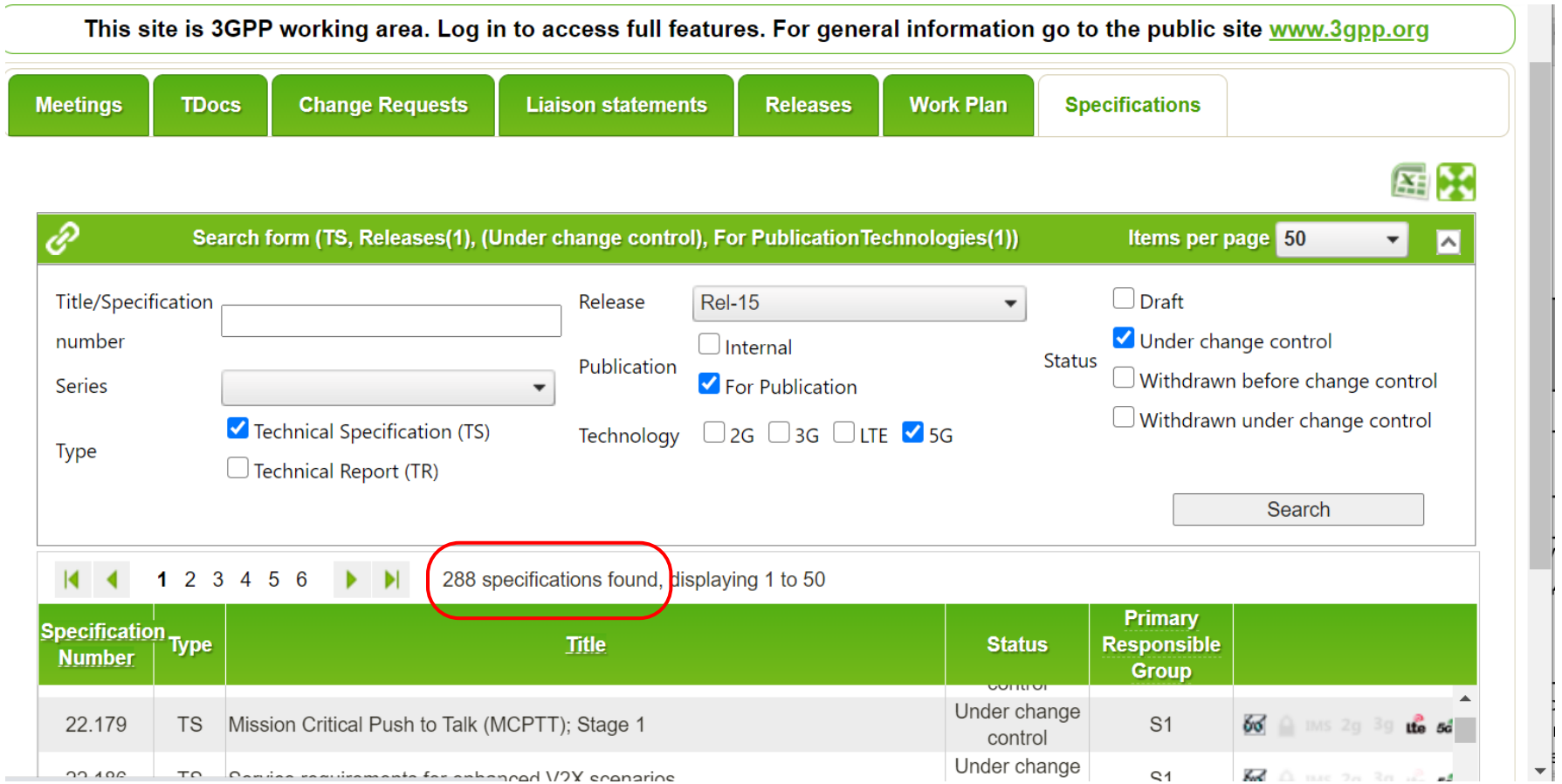



Пользовательское оборудование (User equipment)
USIM/ UICC
UE
gNB
SIM-карта
Базовая станция

Радиосеть нового поколения

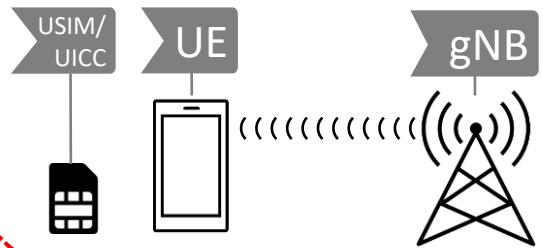



NGC
UDM
APRF
SIDF
UDR
UDSF
AUSF
NSSF
AMF
SEAF
PCF
SMF
UPF
Data Network
(DN)
Радиосеть
нового поколения
NG-RAN
USIM/
UICC
UE
gNB
Опорная сеть
(ядро сети)

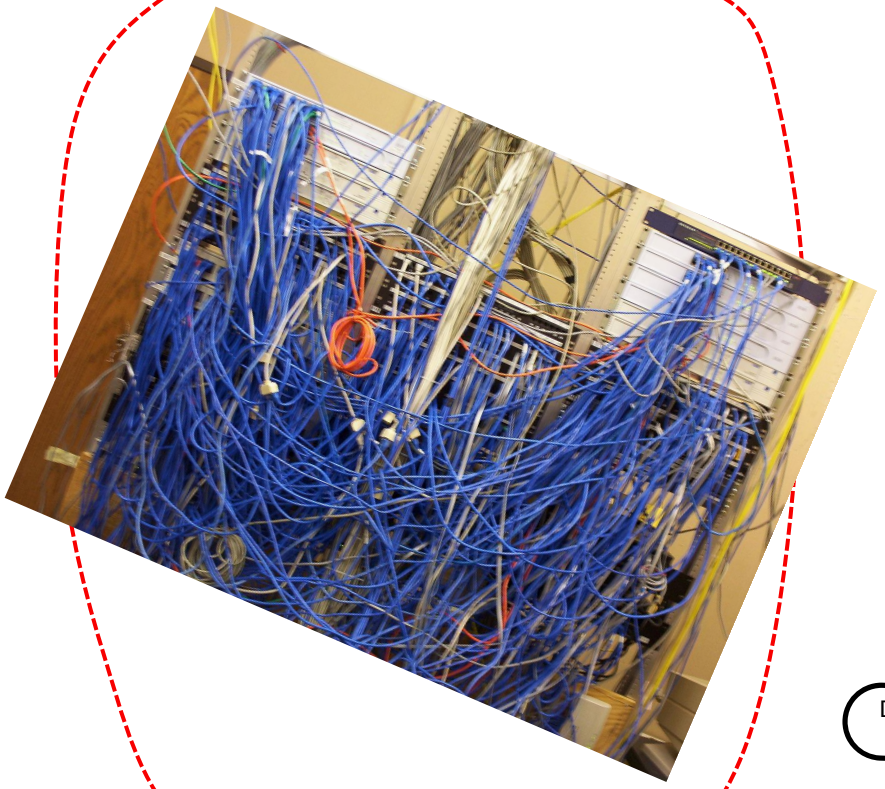

This site is 3GPP working area. Log in to access full features. For general information go to the public site www.3gpp.org
Meetings
TDocs
Change Requests
Liaison statements
Releases
Work Plan
Specifications
Search form (TS, Releases(1), (Under change control), For PublicationTechnologies(1))
Items per page 50
Title/Specification number
Series
Type
Technical Specification (TS)
Technical Report (TR)
Release
Rel-15
Publication
Internal
For Publication
Technology
2G
3G
LTE
5G
Status
Draft
Under change control
Withdrawn before change control
Withdrawn under change control
Search
1 2 3 4 5 6
288 specifications found, displaying 1 to 50
Specification Number
Type
Title
Status
Primary Responsible Group
22.179
TS
Mission Critical Push to Talk (MCPTT); Stage 1
Under change control
S1
Under change

Радиосеть
нового поколения

NG-RAN



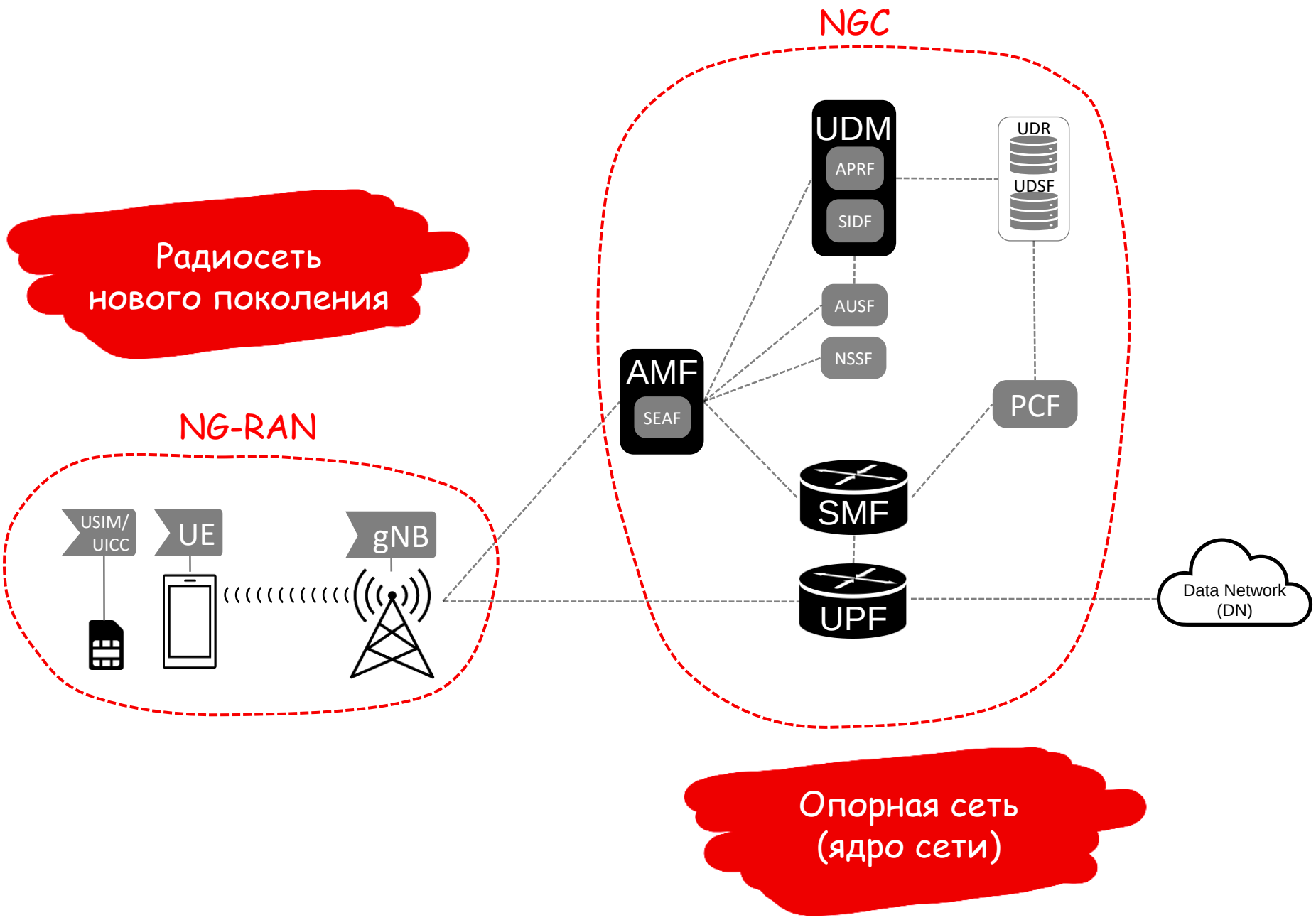
NGC

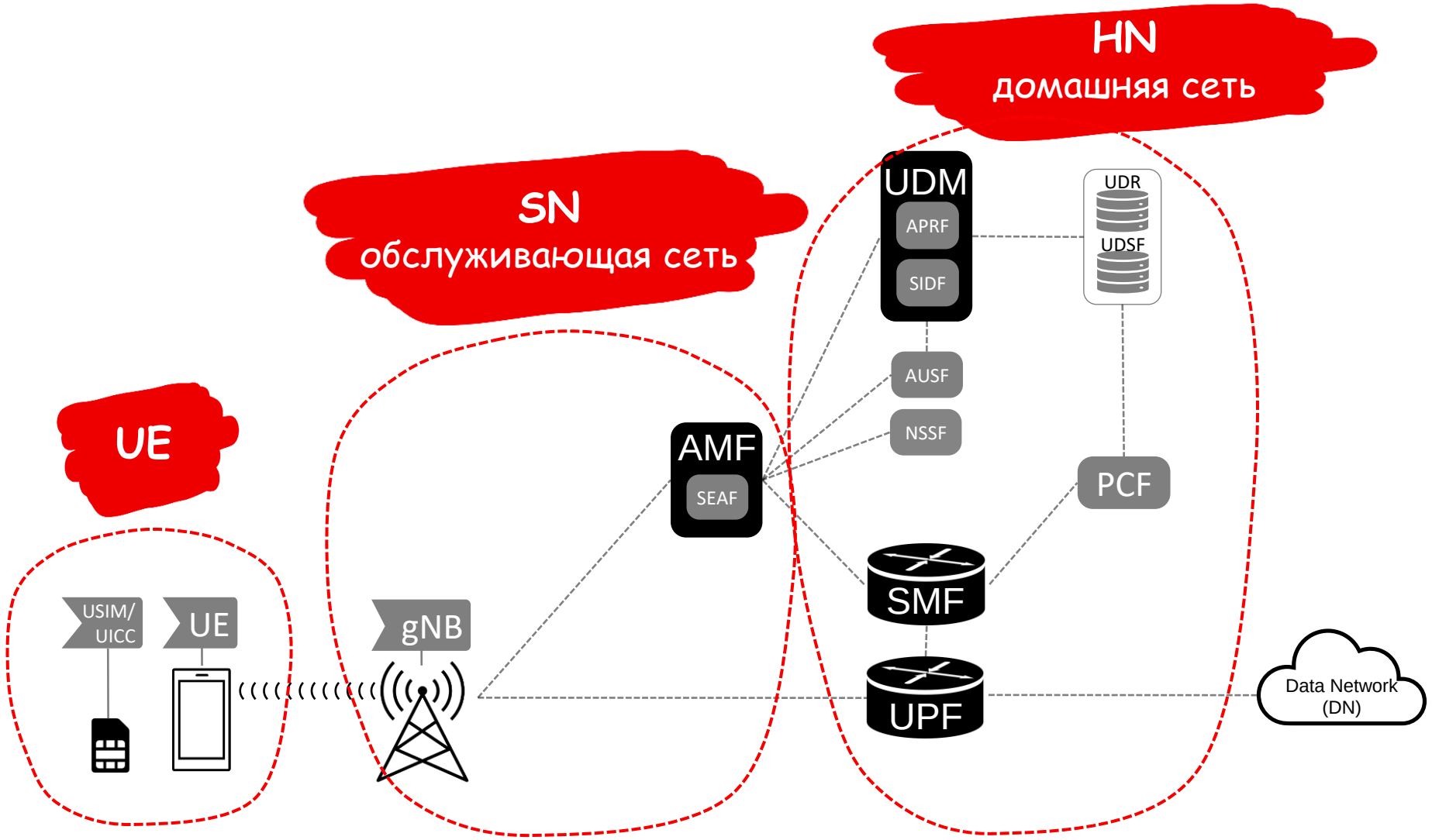


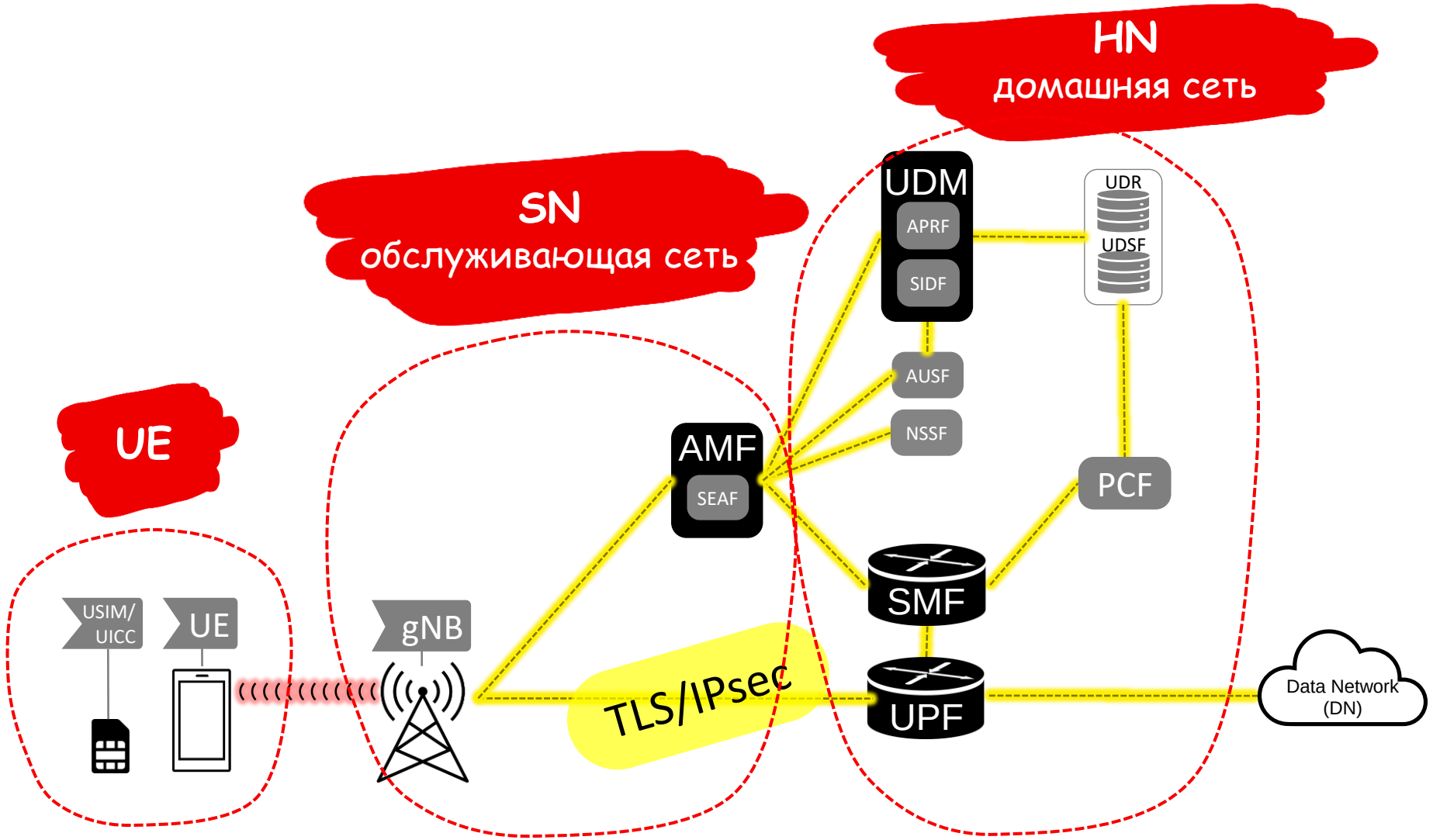
Data Network
(DN)

Опорная сеть
(ядро сети)

5G глазами ленивого криптографа


NGC
UDM
APRF
SIDF
UDR
UDSF
AUSF
NSSF
AMF
SEAF
PCF
SMF
UPF
Data Network
(DN)
Радиосеть
нового поколения
NG-RAN
USIM/
UICC
UE
gNB
Опорная сеть
(ядро сети)


HN
домашняя сеть
SN
обслуживающая сеть
UE
UDM
APRF
SIDF
UDR
UDSF
AUSF
NSSF
AMF
SEAF
PCF
SMF
UPF
USIM/
UICC
UE
gNB
Data Network
(DN)


HN
домашняя сеть
SN
обслуживающая сеть
UE
UDM
APRF
SIDF
UDR
UDSF
AUSF
NSSF
AMF
SEAF
PCF
SMF
UPF
USIM/
UICC
UE
gNB
TLS/IPsec
Data Network
(DN)

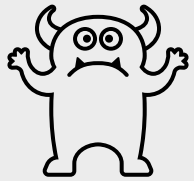
UE

SN

HN

SUPI

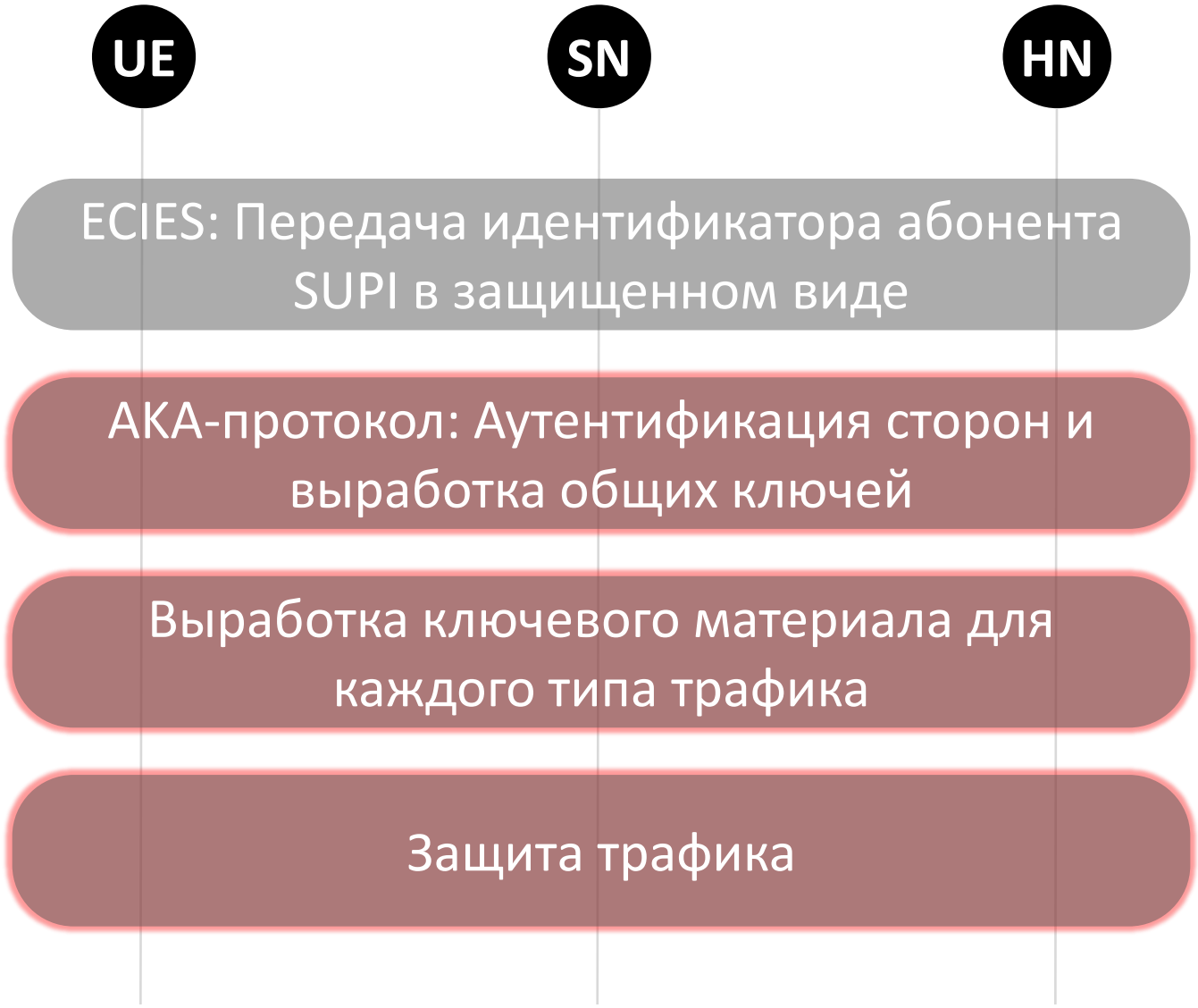
K



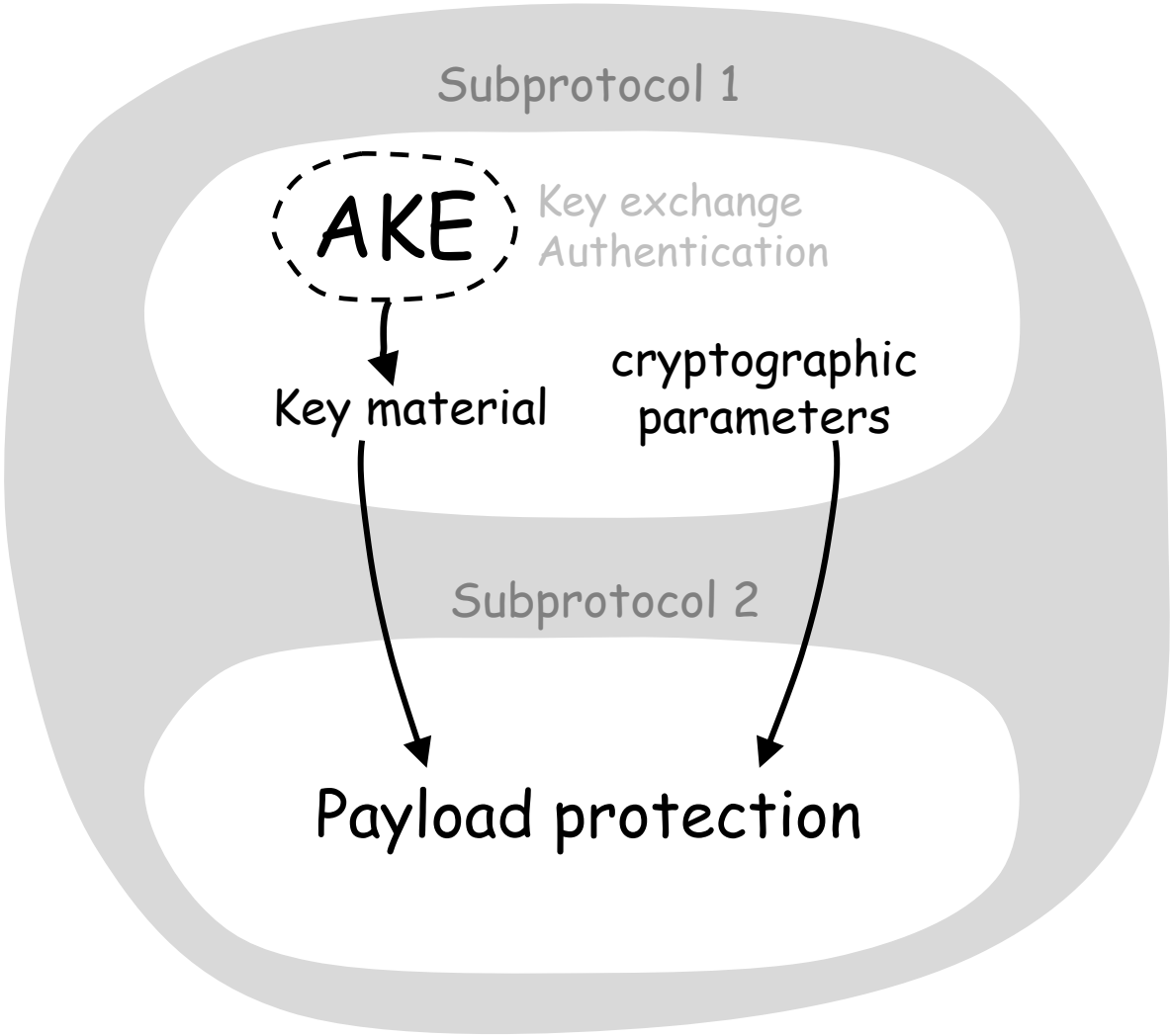
SUPI

K

Основные этапы (подпротоколы) обеспечения криптографической безопасности в сетях связи 5G

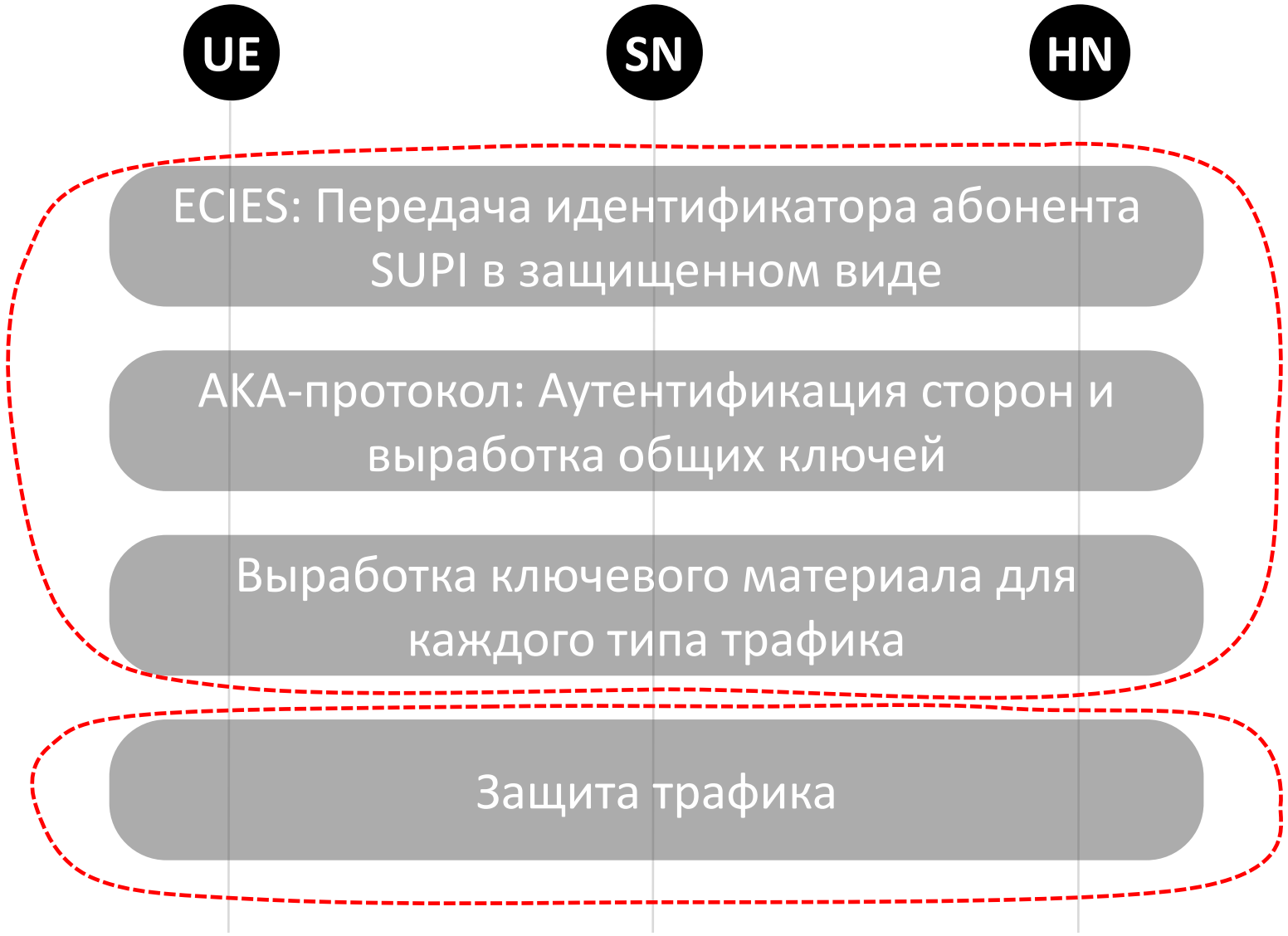

UE
SN
HN
ECIES: Передача идентификатора абонента SUPI в защищенном виде
AKA-протокол: Аутентификация сторон и выработка общих ключей
Выработка ключевого материала для каждого типа трафика
Защита трафика

Стандартный протокол обеспечения защищенного канала связи



Стандартный протокол обеспечения защищенного канала связи

Примеры:


UE
SN
HN
ECIES: Передача идентификатора абонента SUPI в защищенном виде
AKA-протокол: Аутентификация сторон и выработка общих ключей
Выработка ключевого материала для каждого типа трафика
Защита трафика

Authenticated

- Асимметричный подход (SIGN)
- Симметричный подход (обладание общим секретом)

Key Exchange

- ECDHE
- PSK

Confidentiality

Integrity

Anonymity

Authenticated

- Асимметричный подход (SIGN)
- Симметричный подход (обладание общим секретом)

Key Exchange

- ECDHE
- PSK

К

Confidentiality

Integrity

Анонимность

5 Security features

5.1 Network access security

5.1.1 User identity confidentiality

The following security features related to user identity confidentiality are provided:

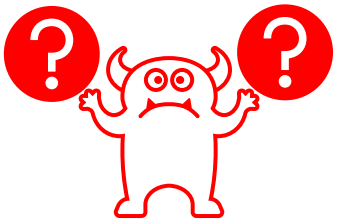
- **user identity confidentiality:** the property that the permanent user identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;
- **user location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **user untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

Анонимность

- ✓ **Конфиденциальность идентификатора пользователя**: постоянный идентификатор пользователя должен быть защищен от перехвата/подслушивания в радиоэфире.

- ✓ **Конфиденциальность местоположения пользователя**: присутствие или прибытие пользователя в определенную местность не может быть определено путем прослушивания радиоэфира.

- ✓ **Невозможность сопоставления проведенных операций (untraceability, неотслеживаемость)**: прослушивая радиоэфир злоумышленник не должен иметь возможность узнать, были ли различные услуги предоставлены одному и тому же абоненту.



UE SN HN

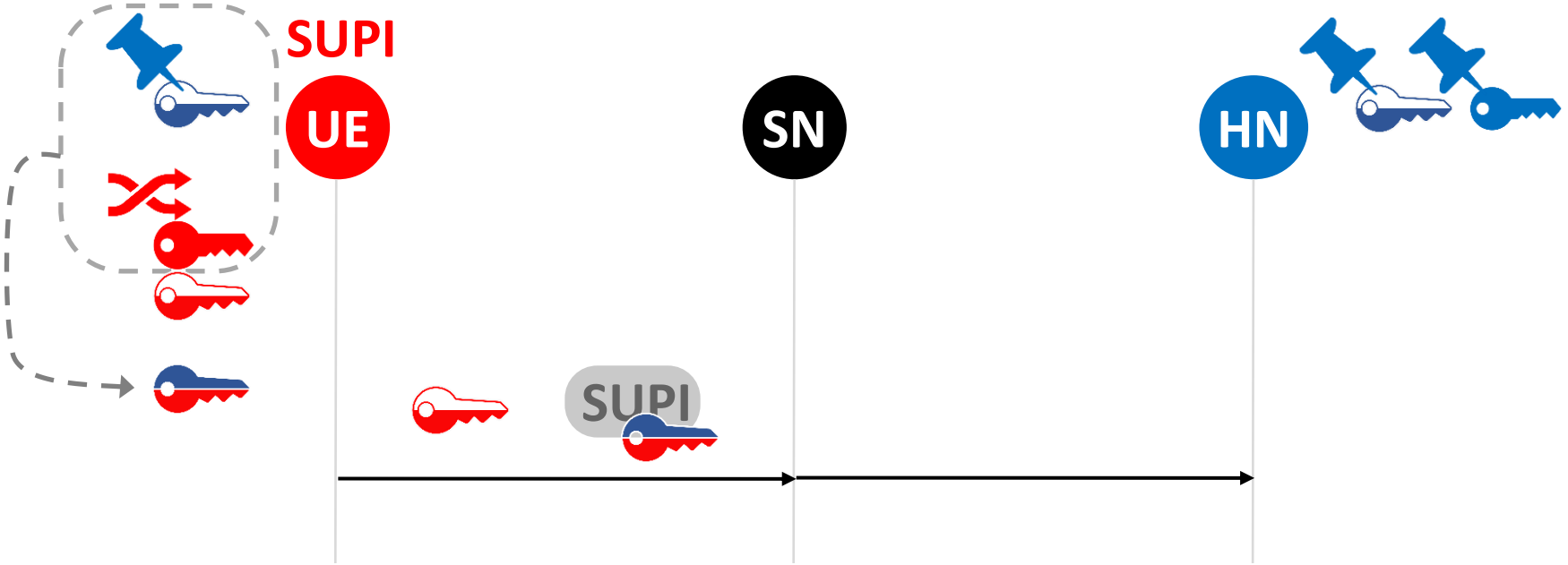
ECIES: Передача идентификатора абонента SUPI в защищенном виде

AKA-протокол: Аутентификация сторон и выработка общих ключей

Выработка ключевого материала для каждого типа трафика

Защита трафика

1. ECIES



✓Идентификатор абонента (SUPI) передается домашней сети в защищенном виде.

✓Защита происходит на ключевом материале, выработанном на основе протокола Диффи-Хеллмана (ECDHE eph-static).

✓TS 33.501 позволяют задавать конкретные параметры схемы с помощью специального идентификатора (профиля схемы ESIES). Для нашего профиля мы зададим свой шифр, имитовставку, kdf и эллиптическую кривую.

UE SN HN

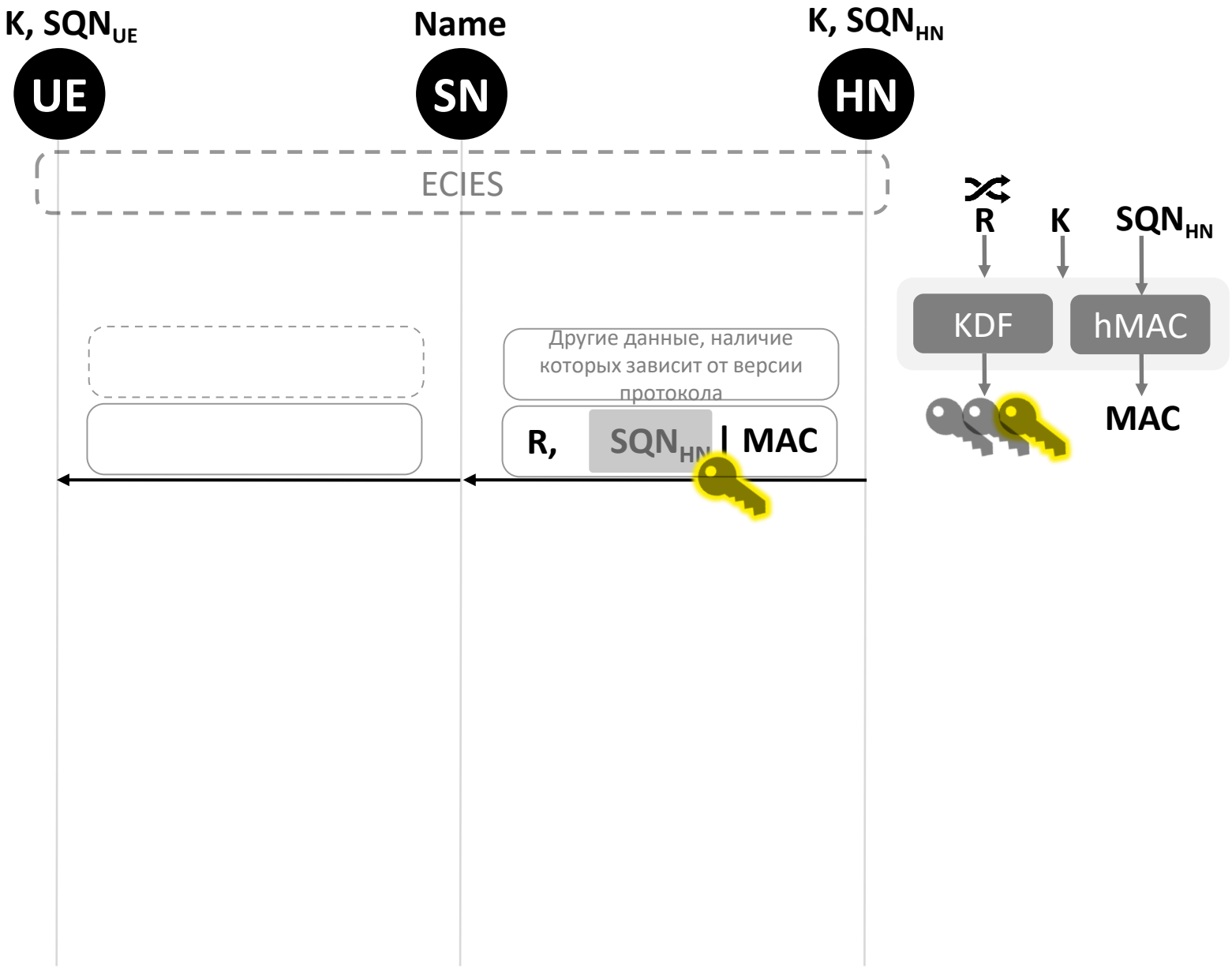
ECIES: Передача идентификатора абонента SUPI в защищенном виде

AKA-протокол: Аутентификация сторон и выработка общих ключей

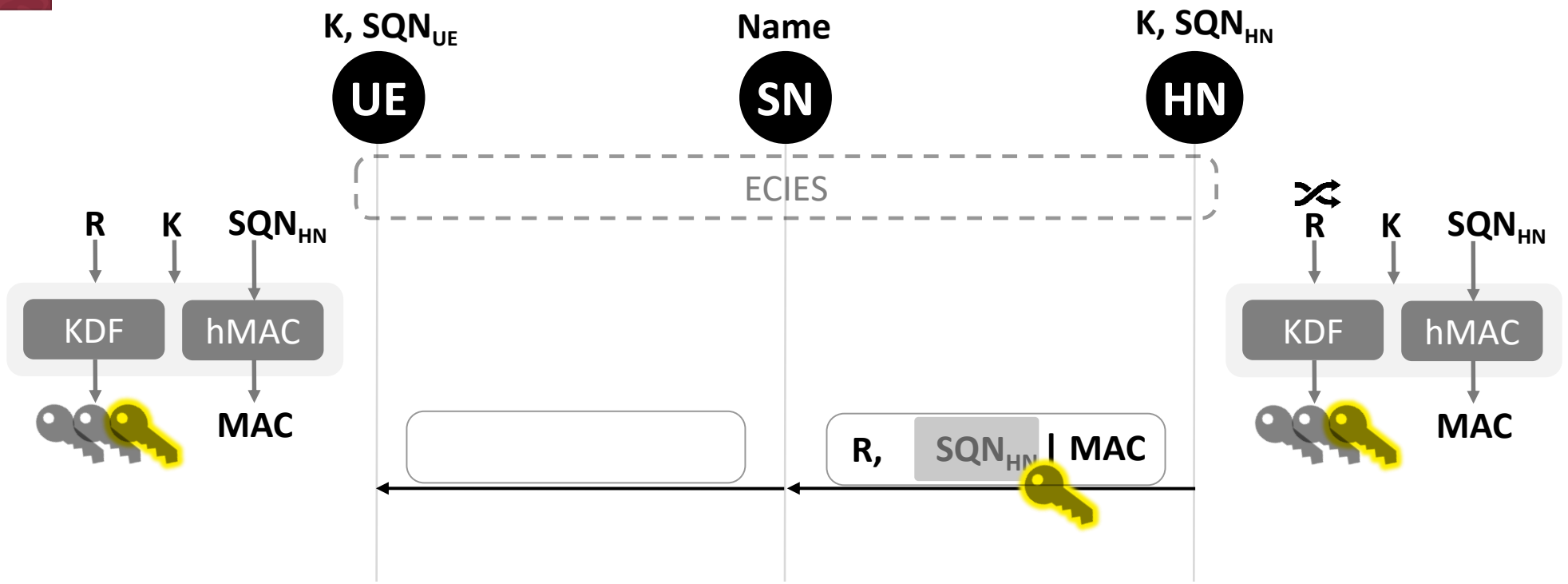
Выработка ключевого материала для каждого типа трафика

Защита трафика

2. 3GPP-AKA


K, SQN_UE
Name
K, SQN_HN
UE
SN
HN
ECIES
R
K
SQN_HN
KDF
hMAC
MAC
Другие данные, наличие которых зависит от версии протокола
R,
SQN_HN
MAC

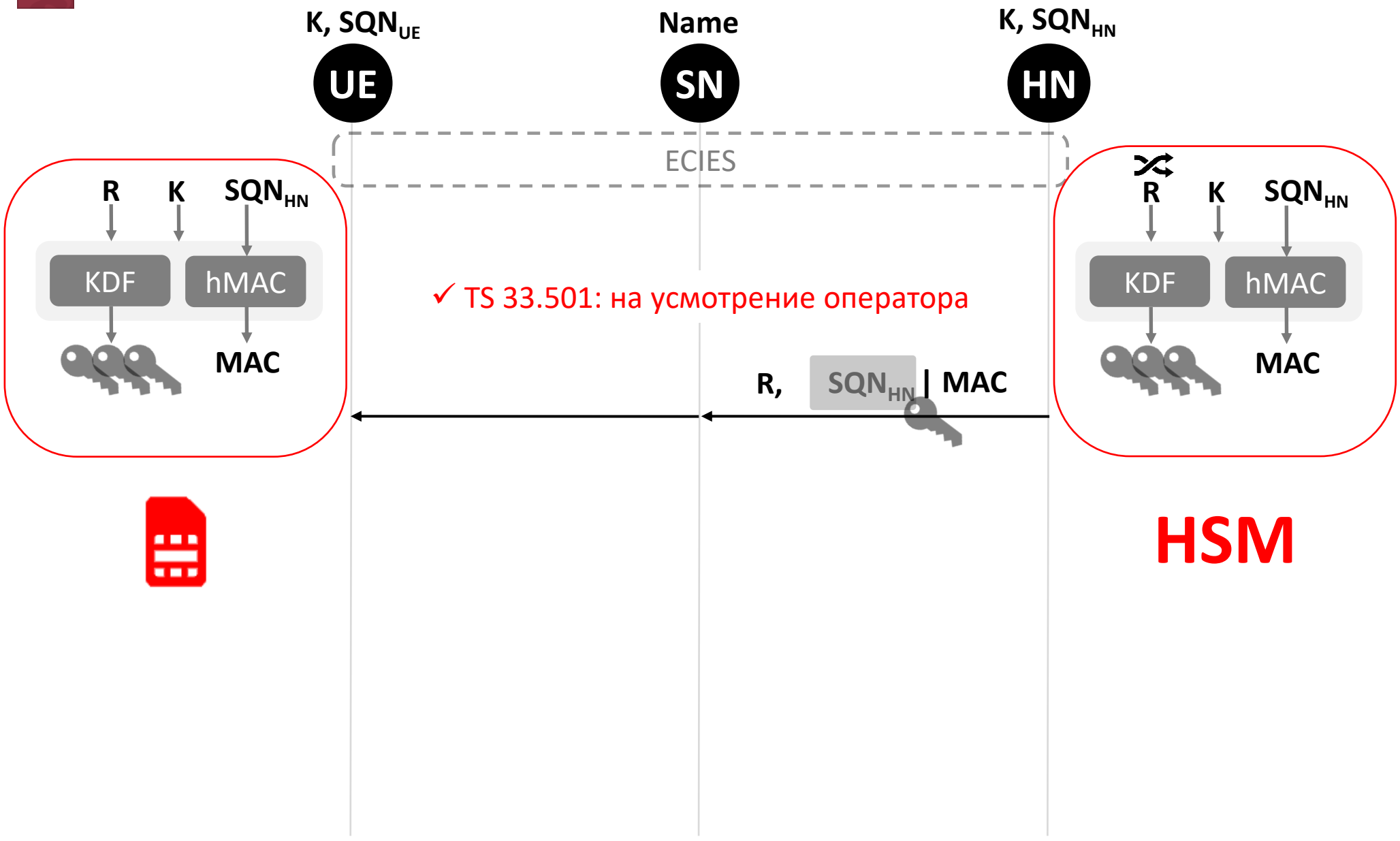
2. 3GPP-AKA



✓“Аутентификация” **HN** (факт обладания секретом **K**)

✓ Защищенная передача $\mathbf{SQN_{HN}}$

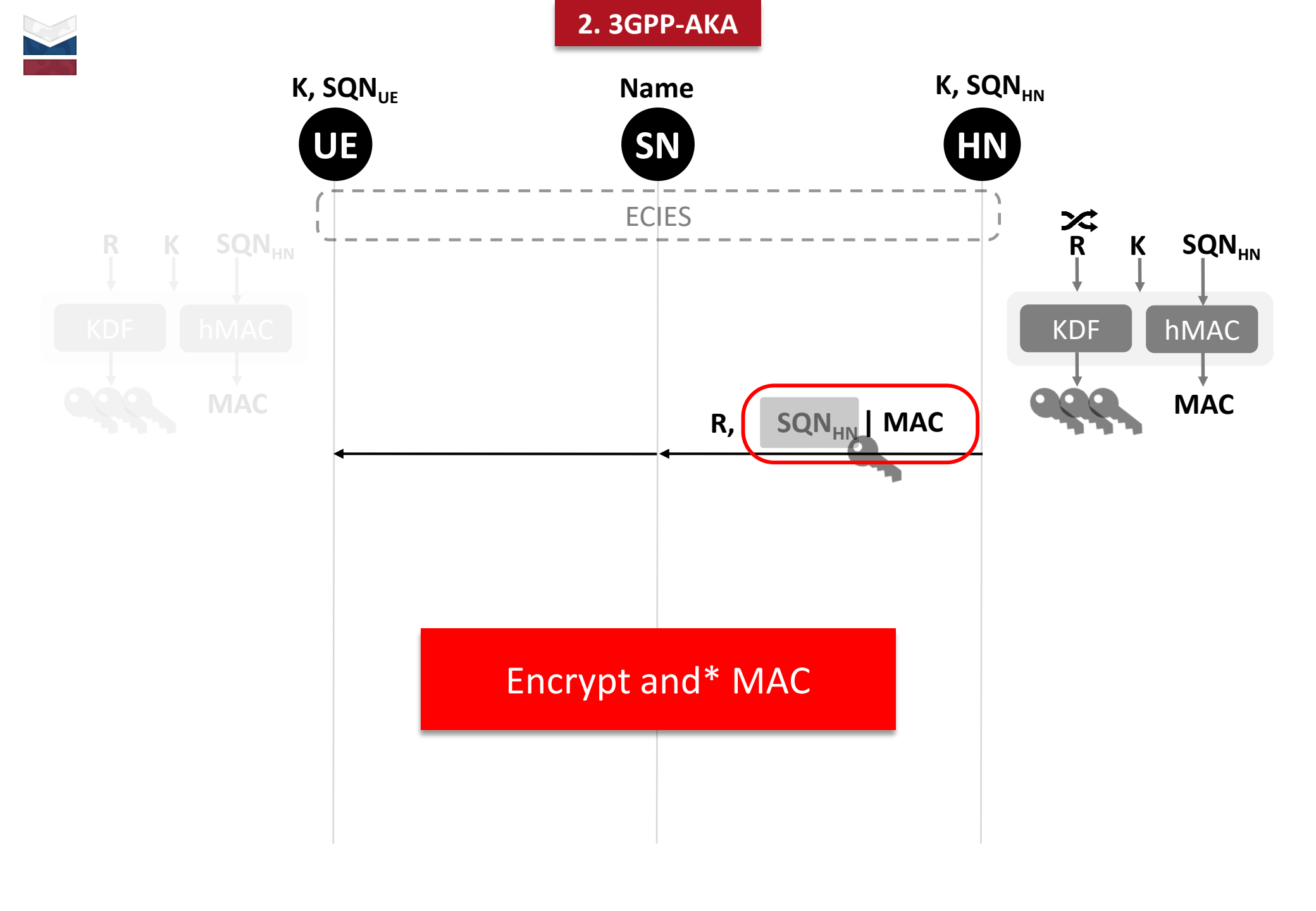
2. 3GPP-AKA


K, SQN_UE
Name
K, SQN_HN
UE
SN
HN
ECIES
R
K
SQN_HN
KDF
hMAC
MAC
✓ TS 33.501: на усмотрение оператора
R,
SQN_HN | MAC
R
K
SQN_HN
KDF
hMAC
MAC
HSM

2. 3GPP-AKA


K, SQN_UE
Name
K, SQN_HN
UE
SN
HN
ECIES
✓ TS 33.501: на усмотрение оператора
R, SQN_HN | MAC
HSM

Encrypt and* MAC


2. 3GPP-AKA
K, SQN_UE
Name
K, SQN_HN
UE
SN
HN
ECIES
R
K
SQN_HN
KDF
hMAC
MAC
R,
SQN_HN | MAC
Encrypt and* MAC

Breaking and Provably Repairing the SSH Authenticated Encryption Scheme: A Case Study of the Encode-then-Encrypt-and-MAC Paradigm

Mihir Bellare* Tadayoshi Kohno† Chanathip Namprempre‡

Theorem 7.1 (Privacy for Encode-then-E&M with respect to Chosen-Plaintext Attacks) Let $\mathcal{SE}$, $\mathcal{MA}$, and $\mathcal{EC}$ respectively be an encryption, a message authentication, and an encoding scheme. Let $\overline{\mathcal{SE}}$ be the encryption scheme associated to them as per Construction 6.1. Then, given any ind-cpa adversary S against $\overline{\mathcal{SE}}$, we can construct adversaries A, D, and C such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\overline{\mathcal{SE}}}(S) \leq \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) + 2 \cdot \mathbf{Adv}^{\text{prf}}_{\mathcal{MA}}(D) + 2 \cdot \mathbf{Adv}^{\text{coll-cpa}}_{\mathcal{EC}}(C) \ .$$

Furthermore, A, D, and C use the same resources as S except that A's and D's inputs to their respective oracles may be of different lengths than those of S (due to the encoding). ▌

Для построения безопасной схемы MAC помимо стандартного требования “о невозможности подделки” должно выполняться дополнительное свойство неотличимости от случайной строки (prf).

5.1.6.2 f1

f1: the network authentication function

f1: (K; SQN, RAND, AMF) → MAC-A (or XMAC-A)

f1 should be a MAC function. In particular, it shall be computationally infeasible to derive K from knowledge of RAND, SQN, AMF and MAC-A (or XMAC-A).

5.1.6.3 f1*

f1*: the re-synchronisation message authentication function

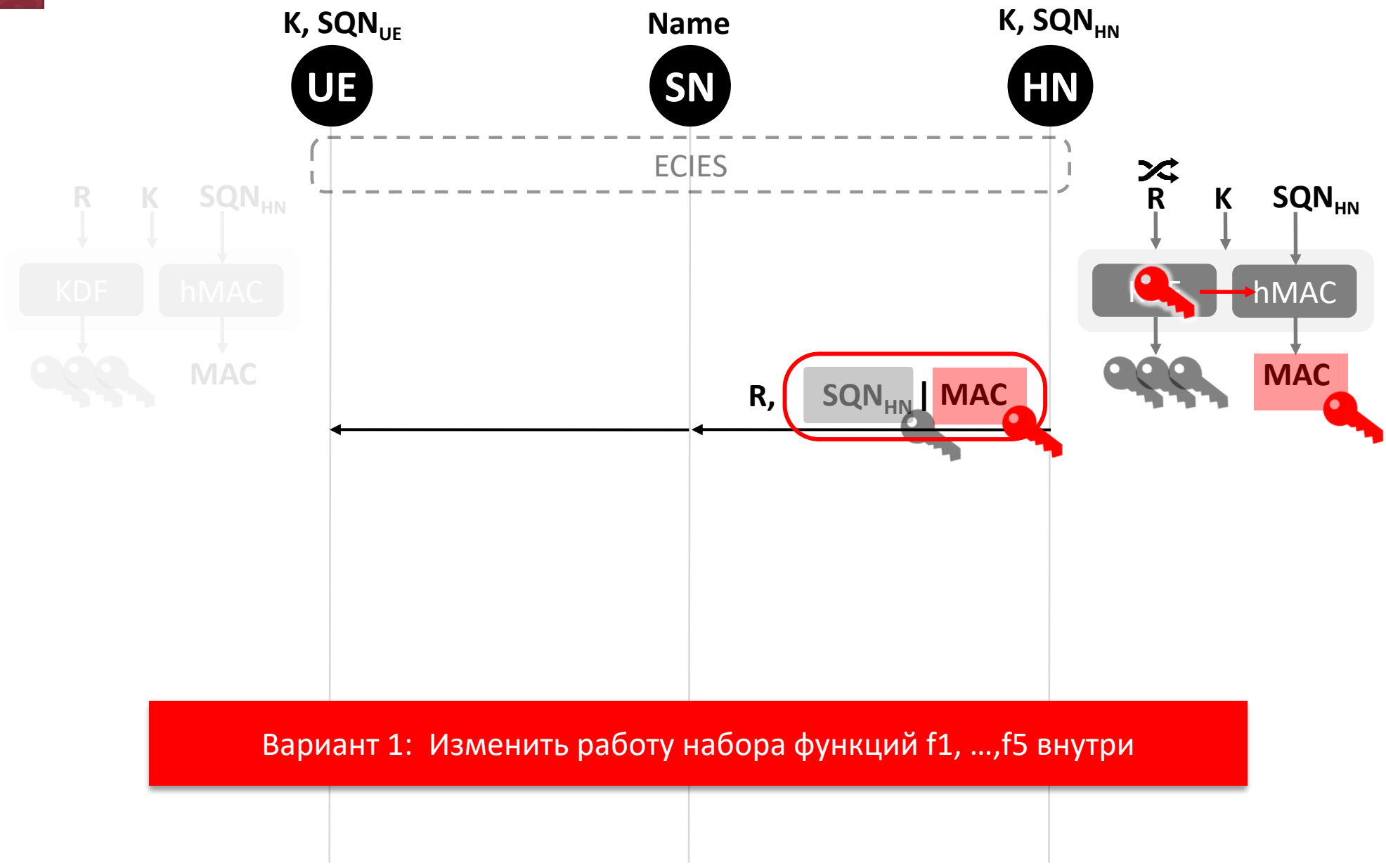
f1*: (K; SQN, RAND, AMF) → MAC-S (or XMAC-S)

f1 should be a MAC function. In particular, it shall be computationally infeasible to derive K from knowledge of RAND, SQN, AMF and MAC-S (or XMAC-S).

5.1.6.4 f2

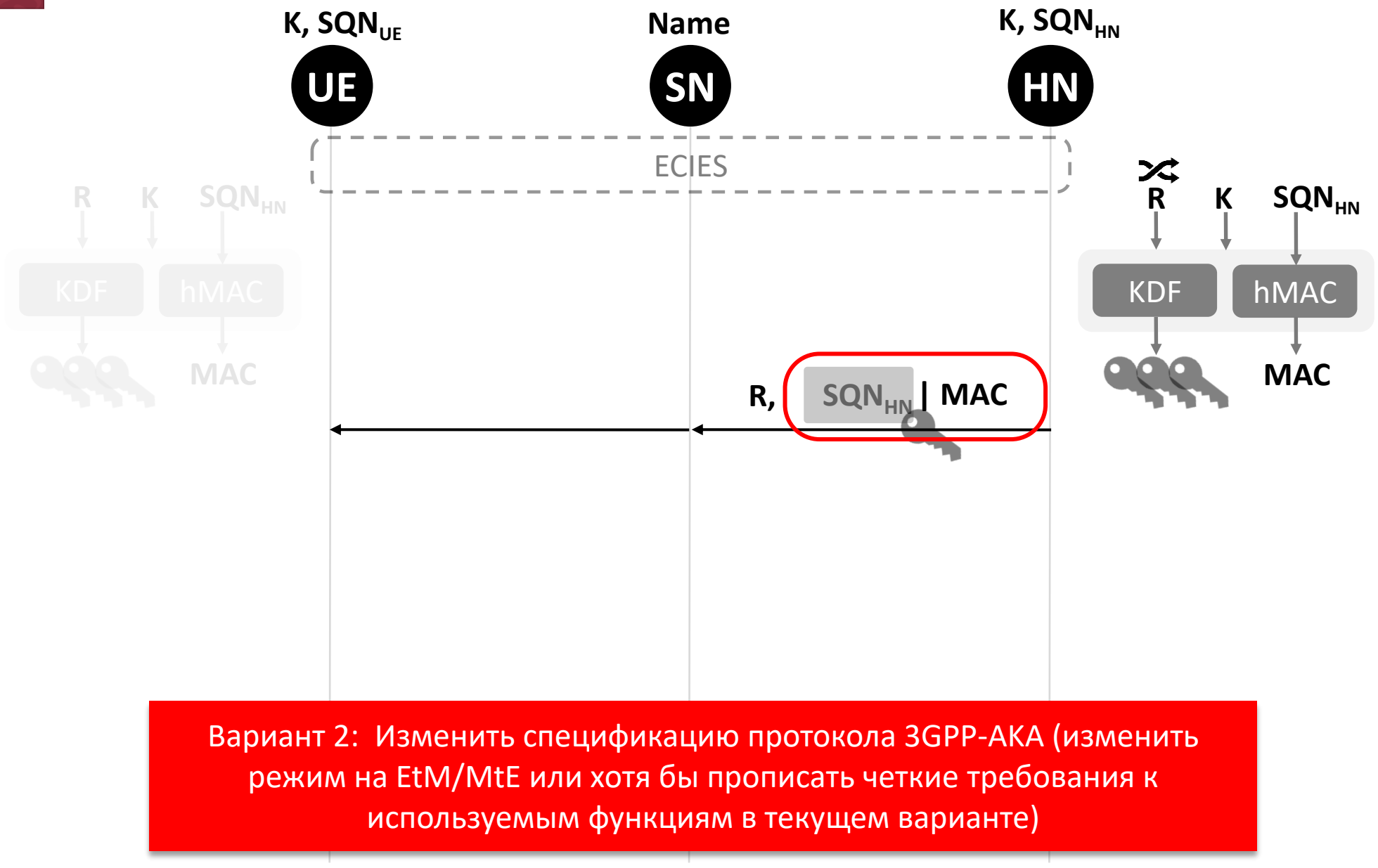
В общем случае (для любого MAC) подобный способ не является стойким.

2. 3GPP-AKA



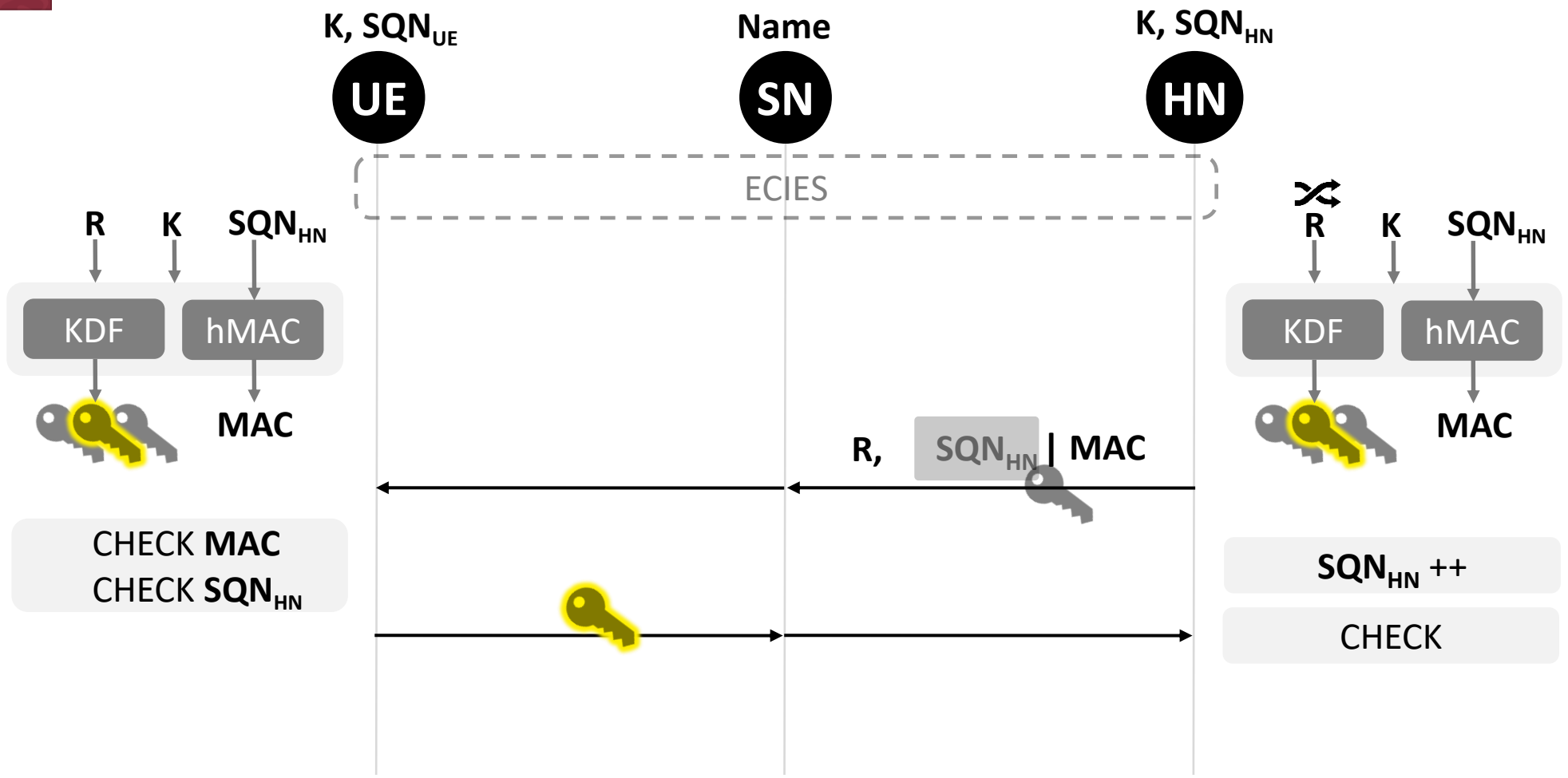
Вариант 1: Изменить работу набора функций f1, …,f5 внутри

2. 3GPP-AKA



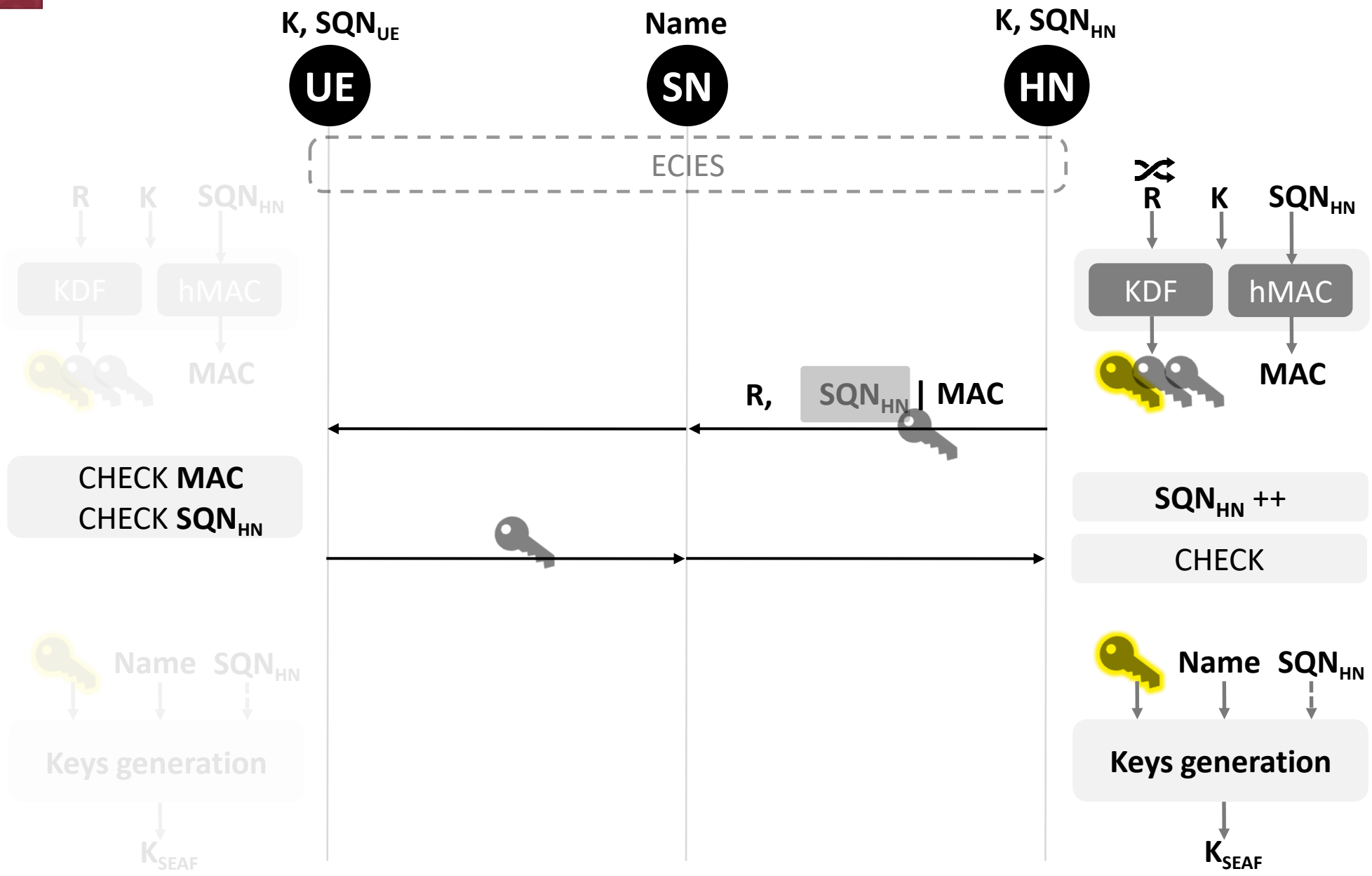
Вариант 2: Изменить спецификацию протокола 3GPP-AKA (изменить режим на EtM/MtE или хотя бы прописать четкие требования к используемым функциям в текущем варианте)

2. 3GPP-AKA

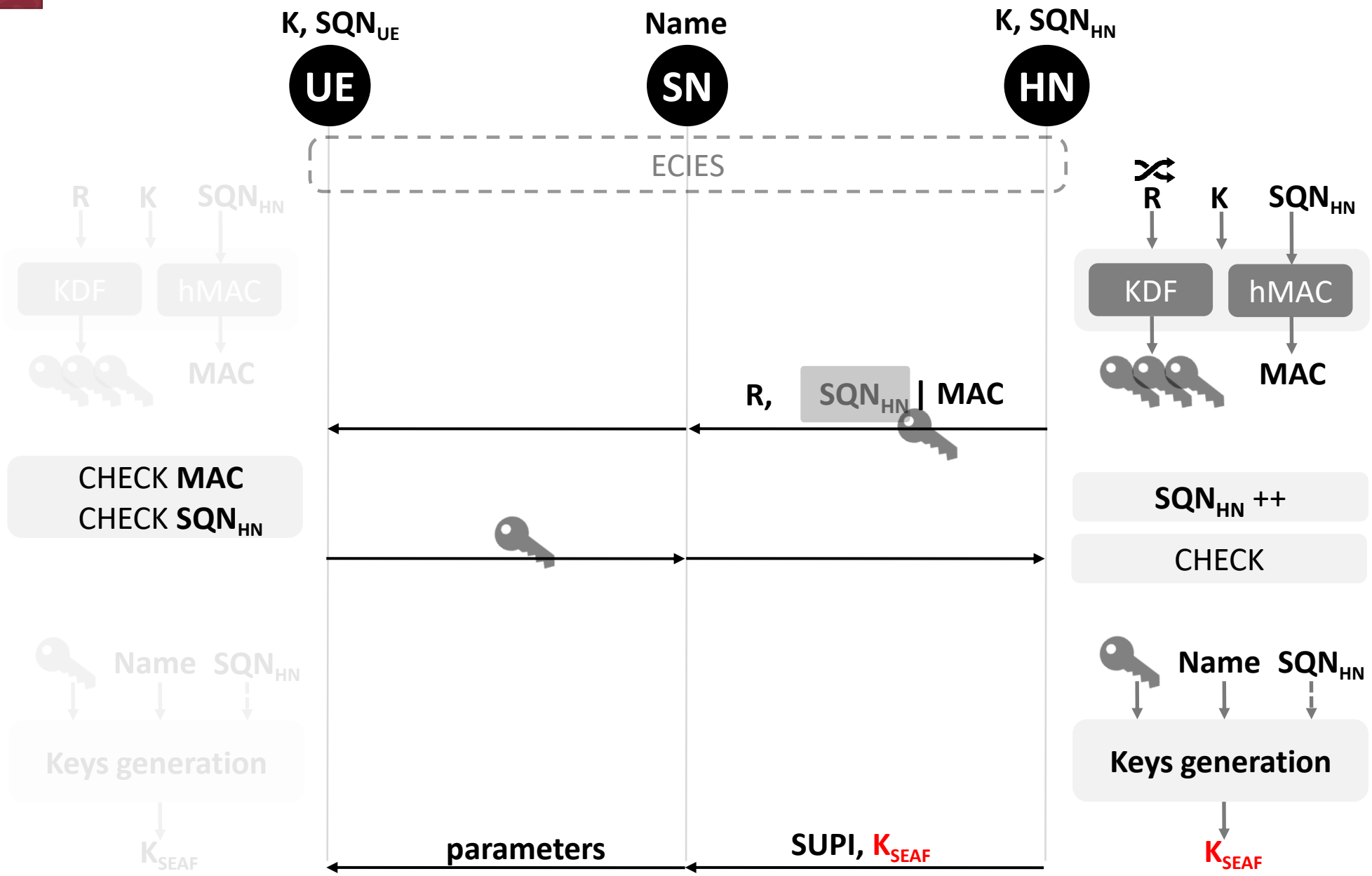


✓Аутентификация **UE** (факт обладания секретом **K**)

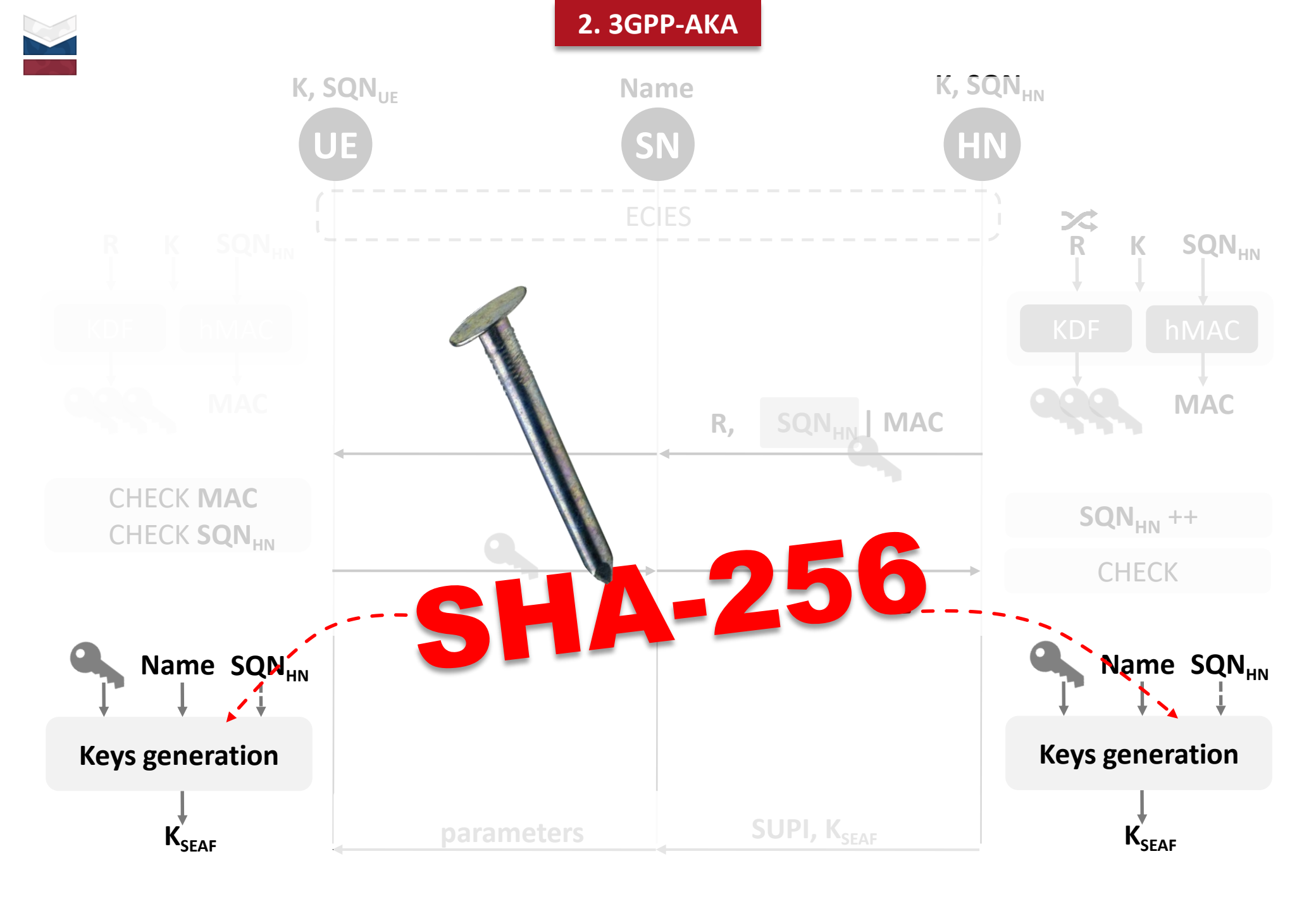
2. 3GPP-AKA


K, SQN_UE
Name
K, SQN_HN
UE
SN
HN
ECIES
R
K
SQN_HN
KDF
hMAC
MAC
R,
SQN_HN | MAC
CHECK MAC
CHECK SQN_HN
SQN_HN ++
CHECK
Name
SQN_HN
Keys generation
K_SEAF

2. 3GPP-AKA


K, SQN_UE
Name
K, SQN_HN
UE
SN
HN
ECIES
R
K
SQN_HN
KDF
hMAC
MAC
R, SQN_HN ⊕ MAC
CHECK MAC
CHECK SQN_HN
SQN_HN ++
CHECK
Name
SQN_HN
Keys generation
K_SEAF
parameters
SUPI, K_SEAF

Фиксированный SHA-256

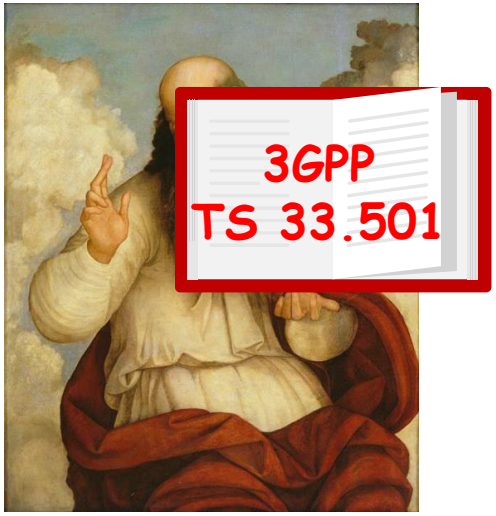

2. 3GPP-AKA
K, SQN_UE
Name
K, SQN_HN
UE
SN
HN
ECIES
R
K
SQN_HN
KDF
hMAC
MAC
R,
SQN_HN | MAC
CHECK MAC
CHECK SQN_HN
SQN_HN ++
CHECK
SHA-256
Name
SQN_HN
Keys generation
K_SEAF
parameters
SUPI, K_SEAF

2. 3GPP-AKA

3GPP-AKA

EAP-AKA'

5G-AKA



2. 3GPP-AKA

3GPP-AKA

EAP-AKA'

- ☹ Более громоздкий, больше лишних вычислений и неиспользуемого функционала
- ☺ Параметр AT_KDF позволяет задавать функцию KDF и выработку общего ключевого материала
- ☺ Описан в RFC

5G-AKA

- ☺ Избавлен от ряда лишних вычислений
- ☹ Не предусматривает опциональности в выборе криптографических примитивов
- ☹ Описан в TS 3GPP

Replay атаки

Стандартный способ защиты от replay-атак — привязка к случайности.

Например, в протоколе TLS 1.2 Handshake такой способ реализуется за счет обмена сторонами случайными значениями r_C, r_S.

Формирование параметров и действия со стороны клиента C	Передаваемые сообщения	Формирование параметров и действия со стороны сервера S
Выработка случайного значения r_c	ClientHello r_c →	
	← ServerHello r_S	Выработка случайного значения r_S
Этап выработки общего секрета		
	← Certificate $Cert_S$ (содержит ключ Q_-)	

Стандартный способ защиты от replay-атак — привязка к случайности.

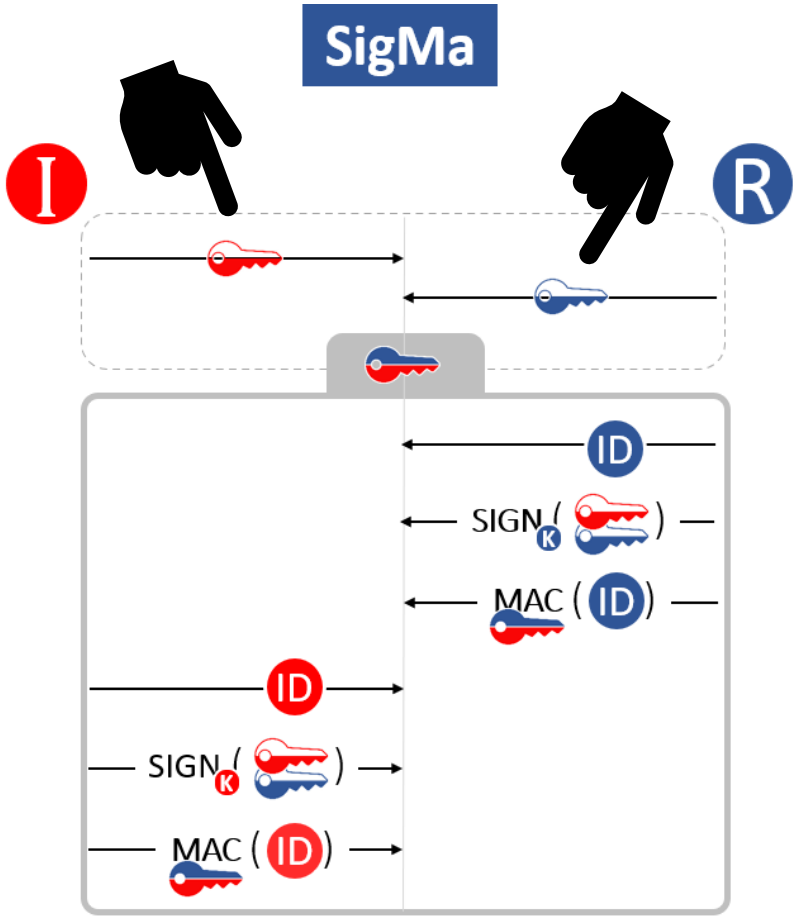
Например, в протоколе TLS 1.2 Handshake такой способ реализуется за счет обмена сторонами случайными значениями r_C, r_S.

Разумеется, просто обменяться случайностью недостаточно, необходимо еще привязать ее к сеансу связи.

$H = HASH(r_C \mid r_S);$ $K_{MAC}^{Exp} \mid K_{ENC}^{Exp} = KEG(k_{EPH}, Q_S, H)$		
Формирование экспортного представления общего секрета PS: $IV = H[25..24 + n/2];$ $PSExp = KExp15(PS, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV)$	ClientKeyExchange $Q_{EPH}, PSExp$	$H = HASH(r_C \mid r_S);$ $K_{MAC}^{Exp} \mid K_{ENC}^{Exp} = KEG(k_S, Q_{EPH}, H)$
		Извлечение общего секрета из экспортного представления: $IV = H[25..24 + n/2];$ $PS = KImp15(PSExp, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV)$
$sgn_C = SIGN_{k_C}(HM_1)$	CertificateVerify* sgn_C	Проверка sgn_C

Привязка сессии к случайности не обязательно должна реализовываться за счет отдельной пересылки специальных случайных строк.

Так, в оригинальном протоколе семейства SigMa привязка к случайности осуществляется на стадии выполнения протокола ECDHE.



Привязка к случайности дает нам возможность гарантировать следующее свойство протокола:

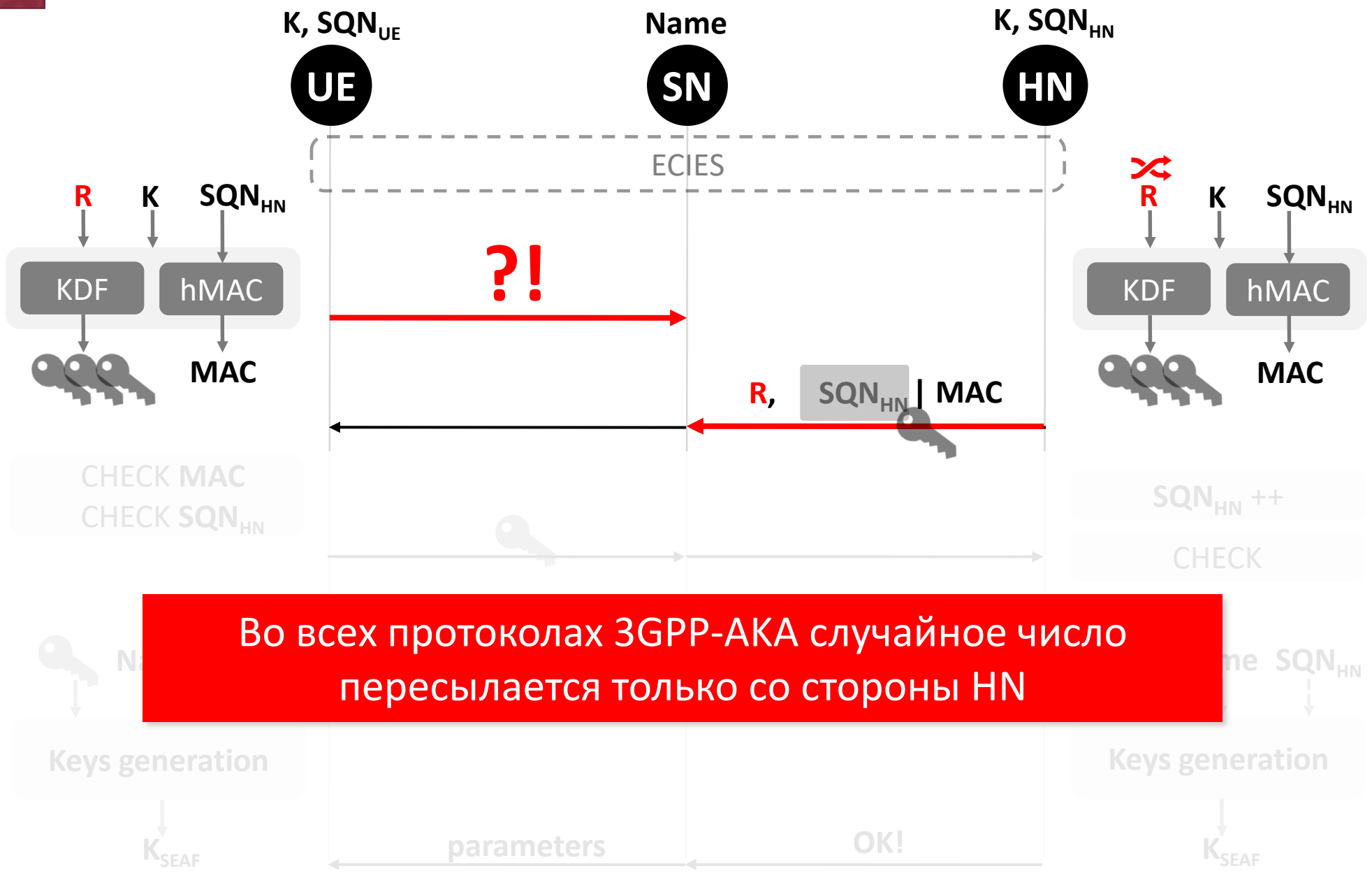
Если ответ на запрос участника A корректен, то он сформирован:

1. Кем-то, кто имеет общий с A секретный ключ
   (т. е. предположительно участником B)

2. В ответ на данный конкретный запрос A
   (т. е. кем-то, кто в данный момент находится «он-лайн»).

В таком случае противнику остается либо просто пересылать сообщения от участника A к участнику B (*relay*), либо ждать повторения случайности для проведения атаки повтора (*replay*).

2. 3GPP-AKA



Во всех протоколах 3GPP-AKA случайное число пересылается только со стороны HN

Ну это теория, а что на практике?

Рассмотрим два примера реальных атак, которых бы не существовало, если бы протокол строился корректно.

LFM

Linkability of Failure Mesages

Int. J. Inf. Secur. (2017) 16:491–523
DOI 10.1007/s10207-016-0338-9

CrossMark

REGULAR CONTRIBUTION

Analysis of privacy in mobile telephony systems

Myrto Arapinis[1] · Loretta Ilaria Mancini[2] · Eike Ritter[2] · Mark Dermot Ryan[2]

AMA

Activity Monitoring Attack

sciendo

Proceedings on Privacy Enhancing Technologies ; 2019 (3):108–127

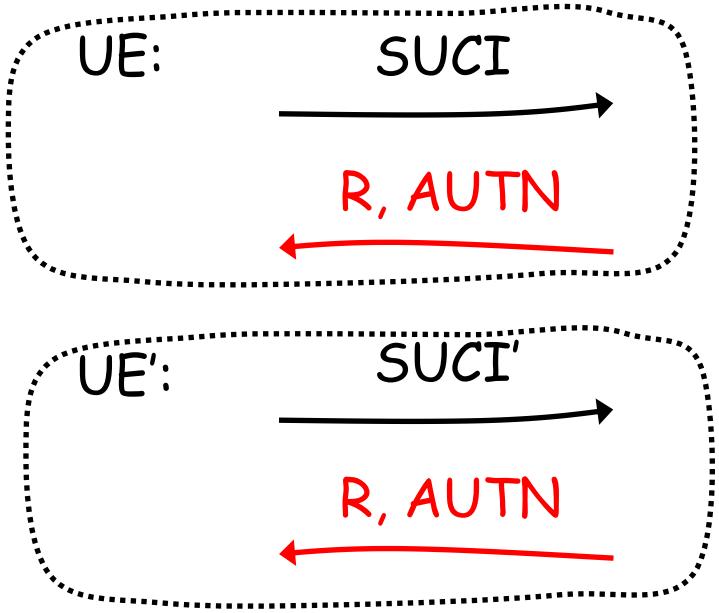
Ravishankar Borgaonkar, Lucca Hirschi*, Shinjo Park, and Altaf Shaik

New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols

Abstract: Mobile communications are used by more than two-thirds of the world population who expect security and privacy guarantees. The *3rd Generation Partnership Project* (3GPP) responsible for the world-a crucial need to provide security and privacy protection to mobile subscribers.

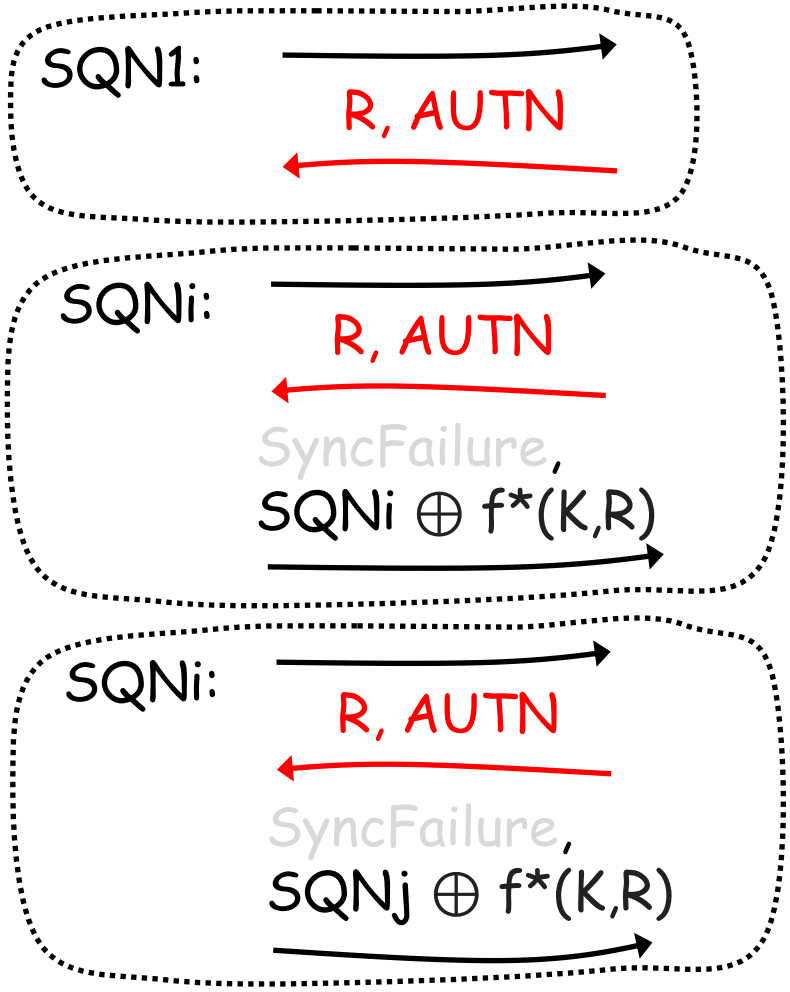
The *3rd Generation Partnership Project* (3GPP) group, responsible for the standardization of 3G, 4G,

LFM



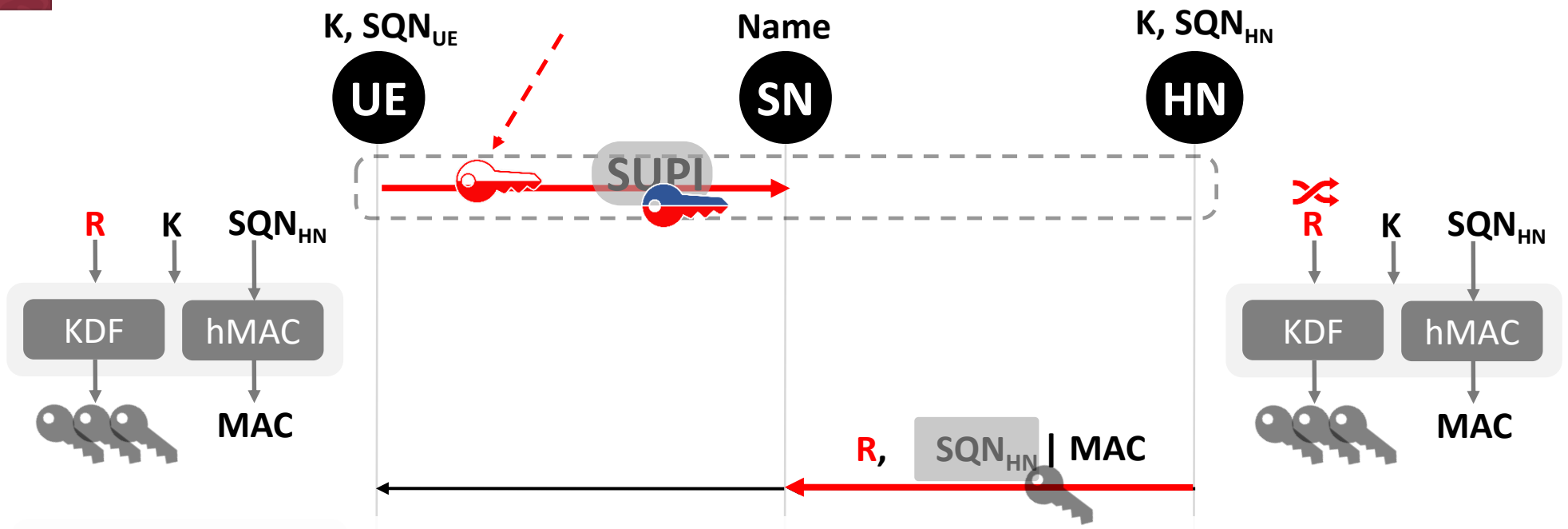
UE = UE' -> SyncFailure
UE ≠ UE' -> MACFailure

AMA



SQNi ⊕ SQNj

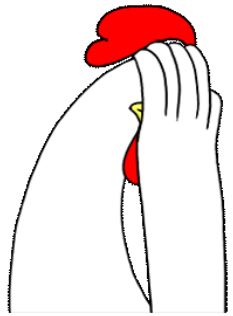
2. 3GPP-AKA



Проблема №3: Во всех протоколах 3GPP-AKA случайное число пересылается только со стороны HN

Возможное решение: задействовать ECIES

В 3GPP более интересный взгляд на вещи:



«...encrypt the AUTS/random number and failure code, and the AUSF uses the K_{AUSF} stored during previously successful authentication to decrypt the AUTS/random number and failure code. … If no stored K_{AUSF}, ***the KEY is a 256-bit binary string of all 0s****»*

Следствие подхода – пролиферация ad-hoc-заплаток для протокола, не затрагивающих основную структуру. (см. padding oracle attacks, LUCKY13, …).

UE SN HN

ECIES: Передача идентификатора абонента SUPI в защищенном виде

AKA-протокол: Аутентификация сторон и выработка общих ключей

To be continued in the next series…

Выработка ключевого материала для каждого типа трафика

Защита трафика

В работе над докладом принимали участие

Грибоедова Екатерина

Руководитель направления стандартизации,
Лаборатория криптографии
e.griboedova@kryptonite.ru

Царегородцев Кирилл

Специалист-исследователь,
Лаборатория криптографии
k.tsaregorodtsev@kryptonite.ru

Давыдов Степан

Специалист-исследователь,
Лаборатория криптографии
s.davydov@kryptonite.ru