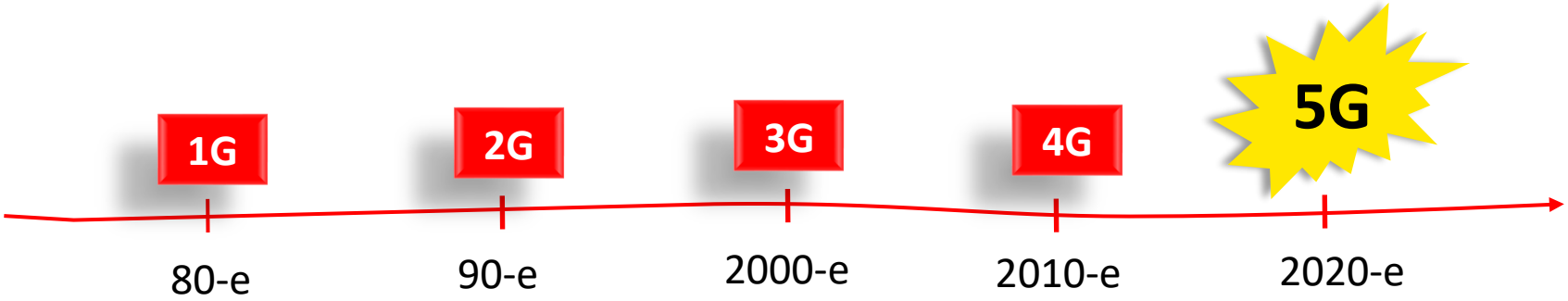
КРИПТОНИТ

Вопросы разработки и стандартизации отечественных криптографических алгоритмов и протоколов в сетях связи 5G

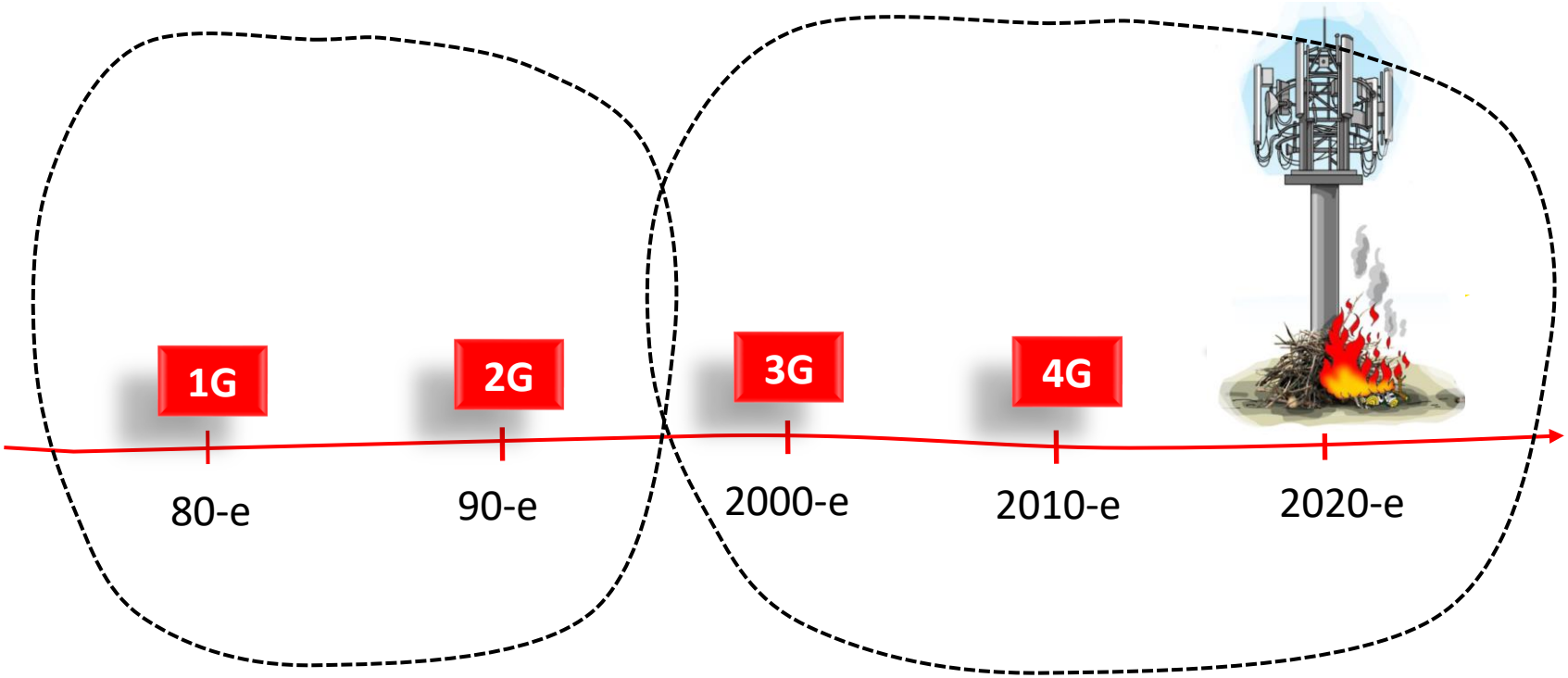
Грибоедова Екатерина

Руководитель направления стандартизации,
Лаборатория криптографии

Поколения сотовой связи



Поколения сотовой связи



Локальные стандартизирующие организации

3GPP

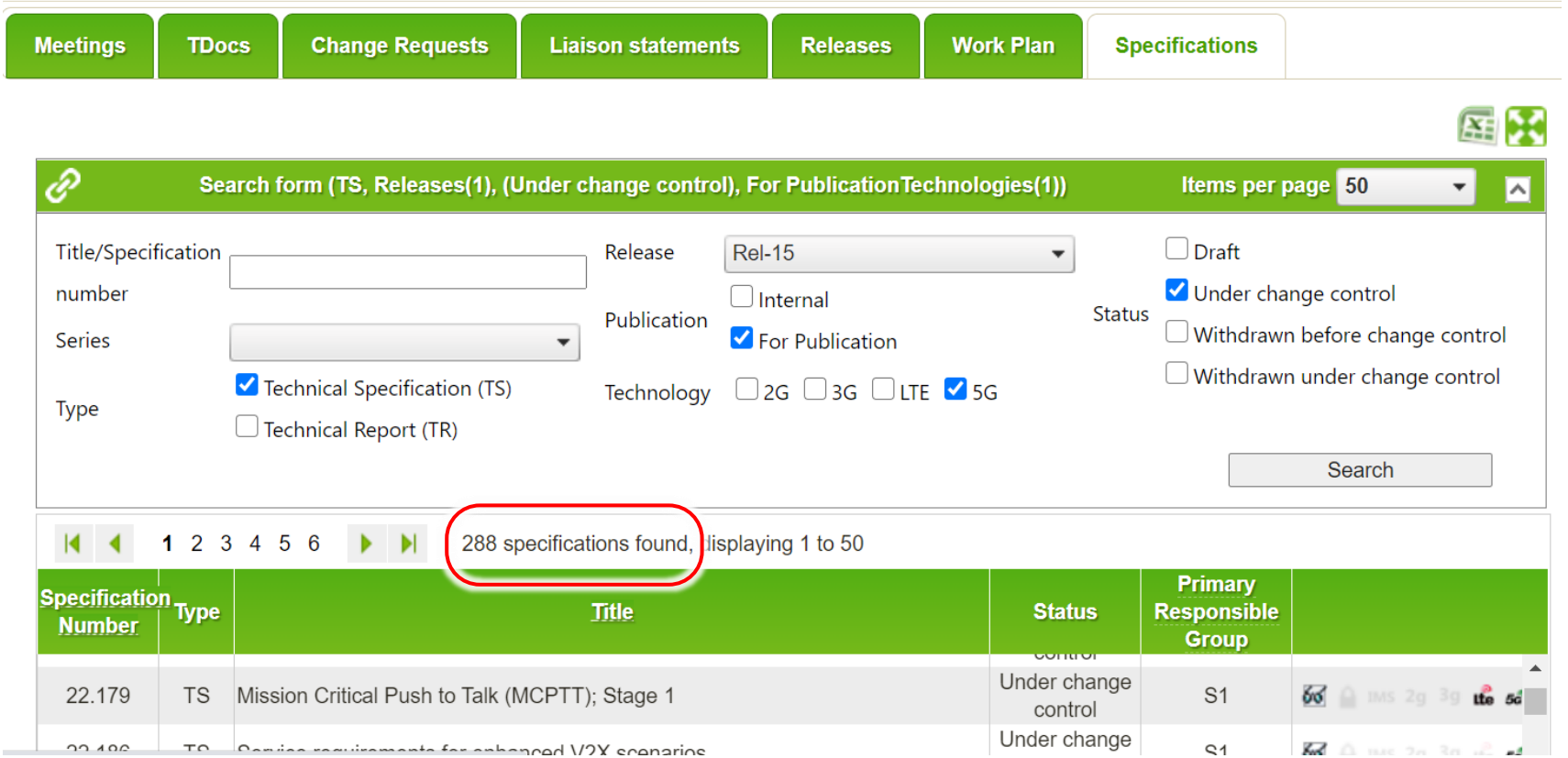
«THIRD GENERATION PARTNERSHIP PROJECT»

Консорциум, разрабатывающий спецификации для мобильной телефонии и состоящий из следующих 7 стандартизирующих организаций-партнеров:

- ARIB - (Япония)
- ATIS - (США)
- CCSA - (Китай)
- ETSI - (Европа)
- TSDSI - (Индия)
- TTA - (Корея)
- TTC - (Япония)

Стандарты 3GPP структурированы **релизами**:

Все документы 3GPP находятся в открытом доступе на ресурсе https://portal.3gpp.org/. При том для каждого релиза существует порядка трех сотен TS.



Национальная программа «Цифровая экономика РФ»
по переводу важных информационных систем на отечественные криптографические алгоритмы с целью обеспечения их технологической независимости.

Новая сетевая архитектура 5G:
реализация всех основных функций телекоммуникационного оборудования происходит на программном уровне и не требует специализированных аппаратных решений.

Множество существующих **уязвимостей**:
LFM attack [1], AMA attack [2], ReVoLTE [3],...

Ноябрь 2020 года,
заседание Президиума Правительственной комиссии по цифровому развитию:

Утверждена **дорожная карта развития мобильных сетей 5G** для развертывания телекоммуникационной сети на базе отечественного оборудования и алгоритмов.

НПК «Криптонит»

Архитектурный совет по реализации соглашения о намерениях в целях развития 5G в России

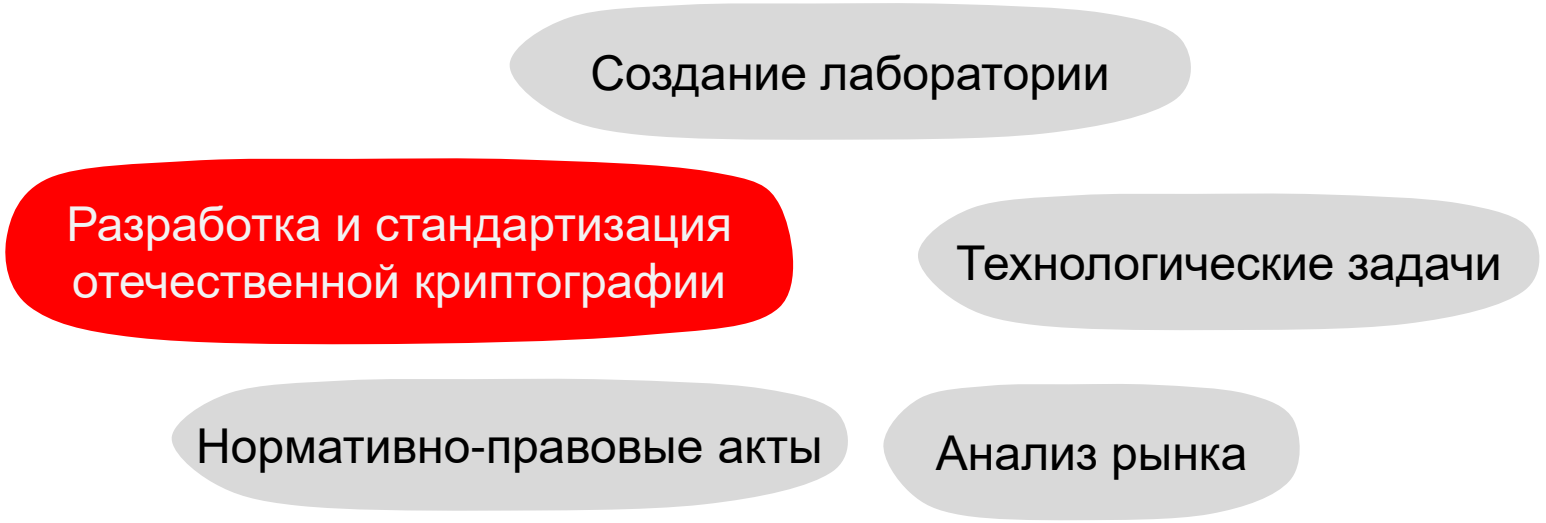
Правительство, «Ростелеком» и Ростех

Ноябрь 2020 года, заседание Президиума Правительственной комиссии по цифровому развитию:

Утверждена **дорожная карта развития мобильных сетей 5G** для развертывания телекоммуникационной сети на базе отечественного оборудования и алгоритмов.

НПК «Криптонит»

Реализация системного проекта по разработке линейки оборудования, необходимого для строительства мобильных сетей связи 5G с дальнейшим сопровождением разработки и ввода в эксплуатацию российского оборудования



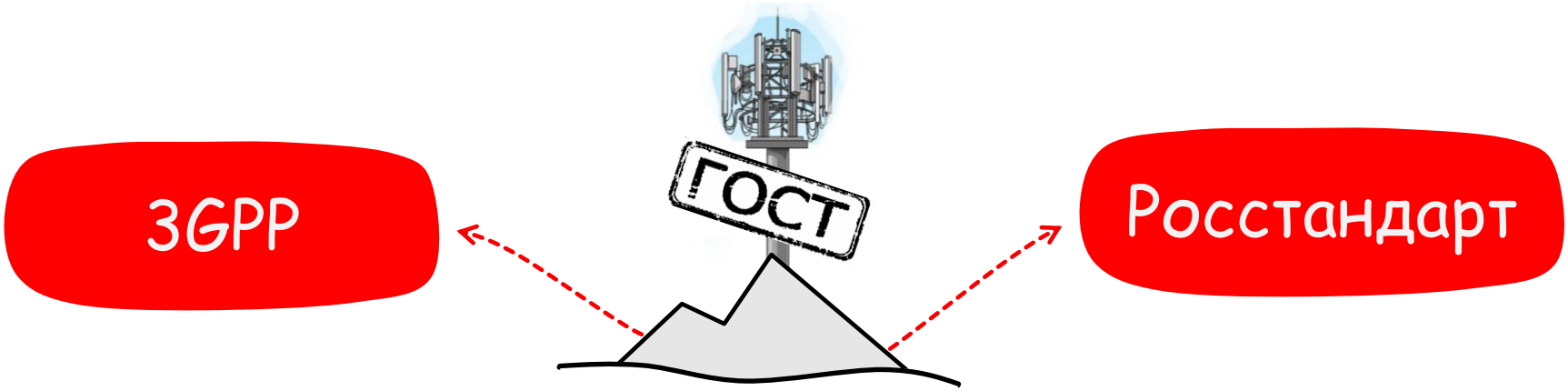
«THIRD GENERATION PARTNERSHIP PROJECT»

Консорциум, разрабатывающий спецификации для мобильной телефонии и состоящий из следующих 7 стандартизирующих организаций-партнеров:

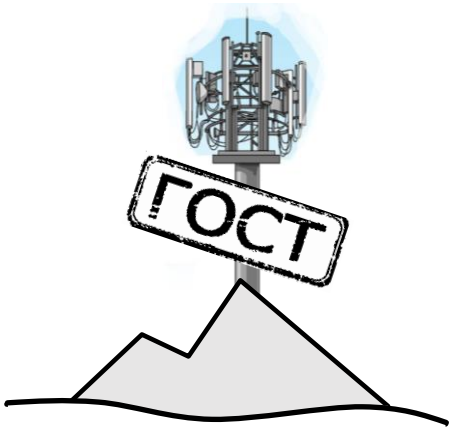
- ARIB - (Япония)
- ATIS - (США)
- CCSA - (Китай)
- ETSI - (Европа)
- TSDSI - (Индия)
- TTA - (Корея)
- TTC - (Япония)

3GPP

В России всего 3 компании являются участниками 3GPP (через ETSI):


3GPP
ГОСТ
Росстандарт

Уже знакомый процесс по стандартизации «криптонаборов» на базе российских криптостандартов (по аналогии с TLS и IPSec)

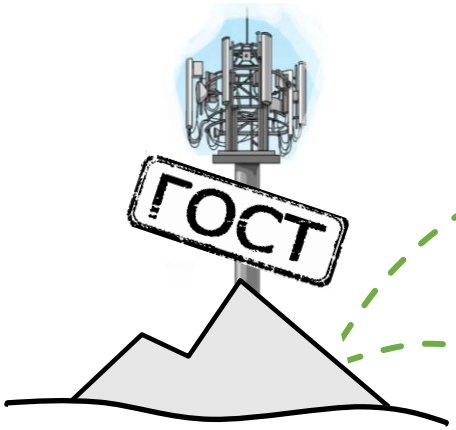


ECIES

3GPP-AKA

Data protection

Уже знакомый процесс по стандартизации «криптонаборов» на базе российских криптостандартов (по аналогии с TLS и IPSec)

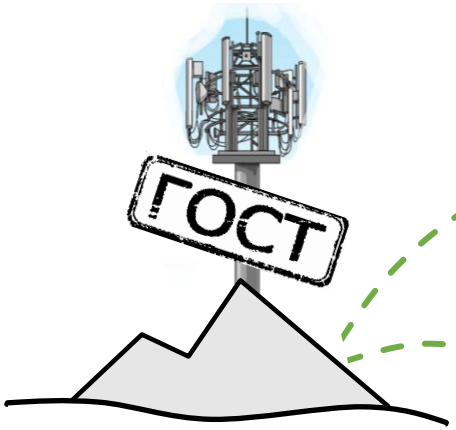


ECIES ✓ 3GPP + TK26 (Profile C)

3GPP-AKA

Data protection ✓ 3GPP + TK26 (NIA7 / NEA7)

Уже знакомый процесс по стандартизации «криптонаборов» на базе российских криптостандартов (по аналогии с TLS и IPSec)

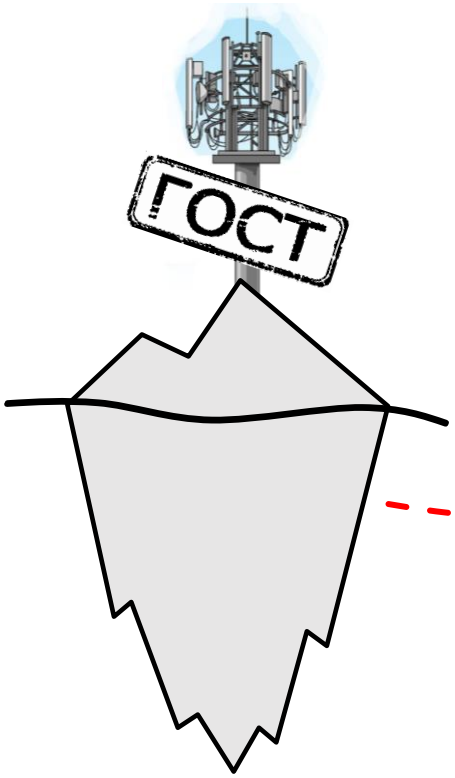


ECIES ☑ 3GPP + TK26 (Profile C)

3GPP-AKA ☑ 3GPP + TK26 (S3G, …)

Data protection ☑ 3GPP + TK26 (NIA7 / NEA7)

Зашитые зарубежные алгоритмы



ECIES

AKA

Data protection

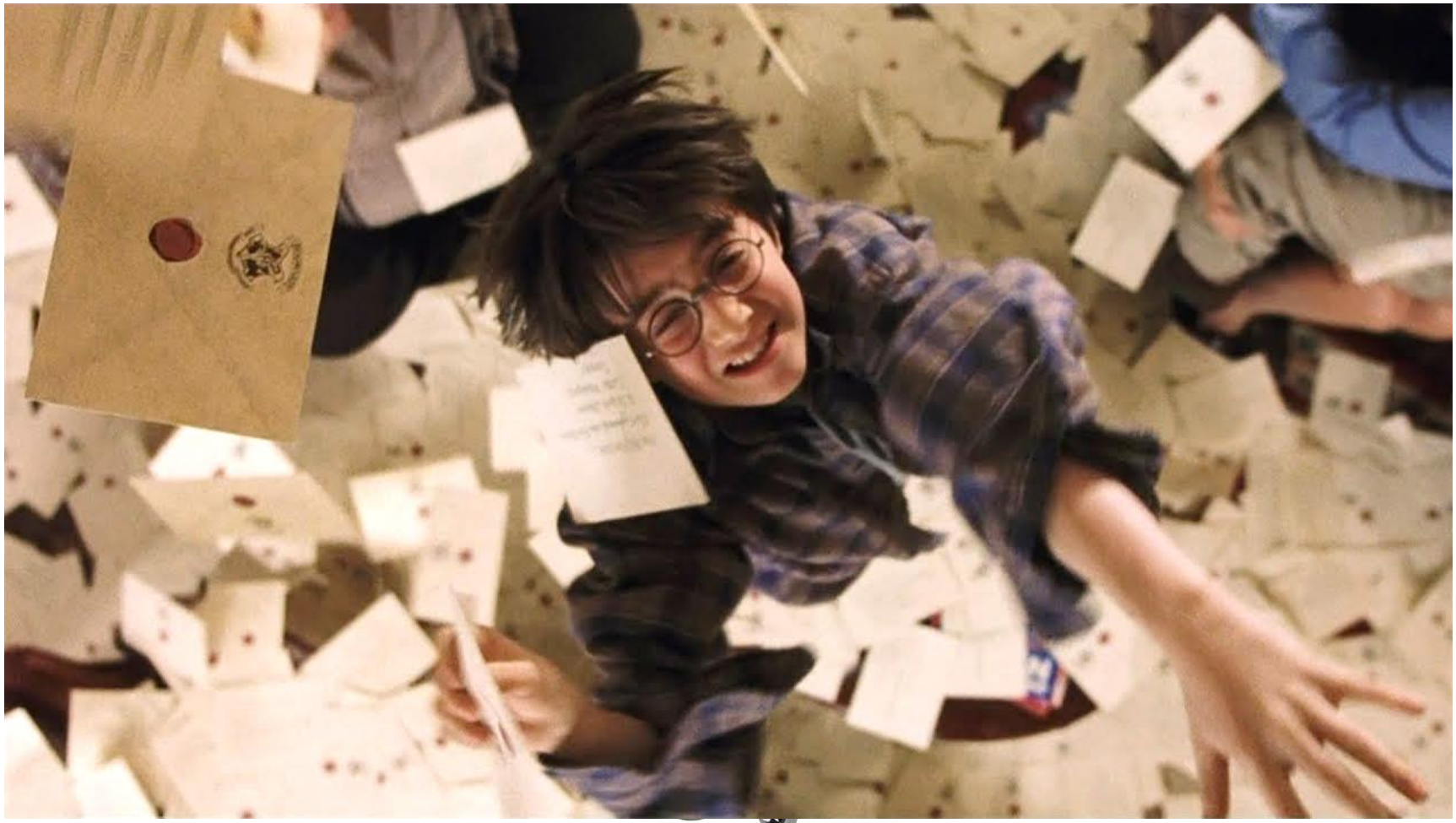
Обратная совместимость, переиспользование оборудования:

😕 Устаревшие принципы построения криптографических протоколов, наличие большого числа уязвимостей

☹ Пролиферация ad-hoc-заплаток для протокола, не затрагивающих основную структуру (вспоминаем padding oracle attacks, LUCKY13, …)

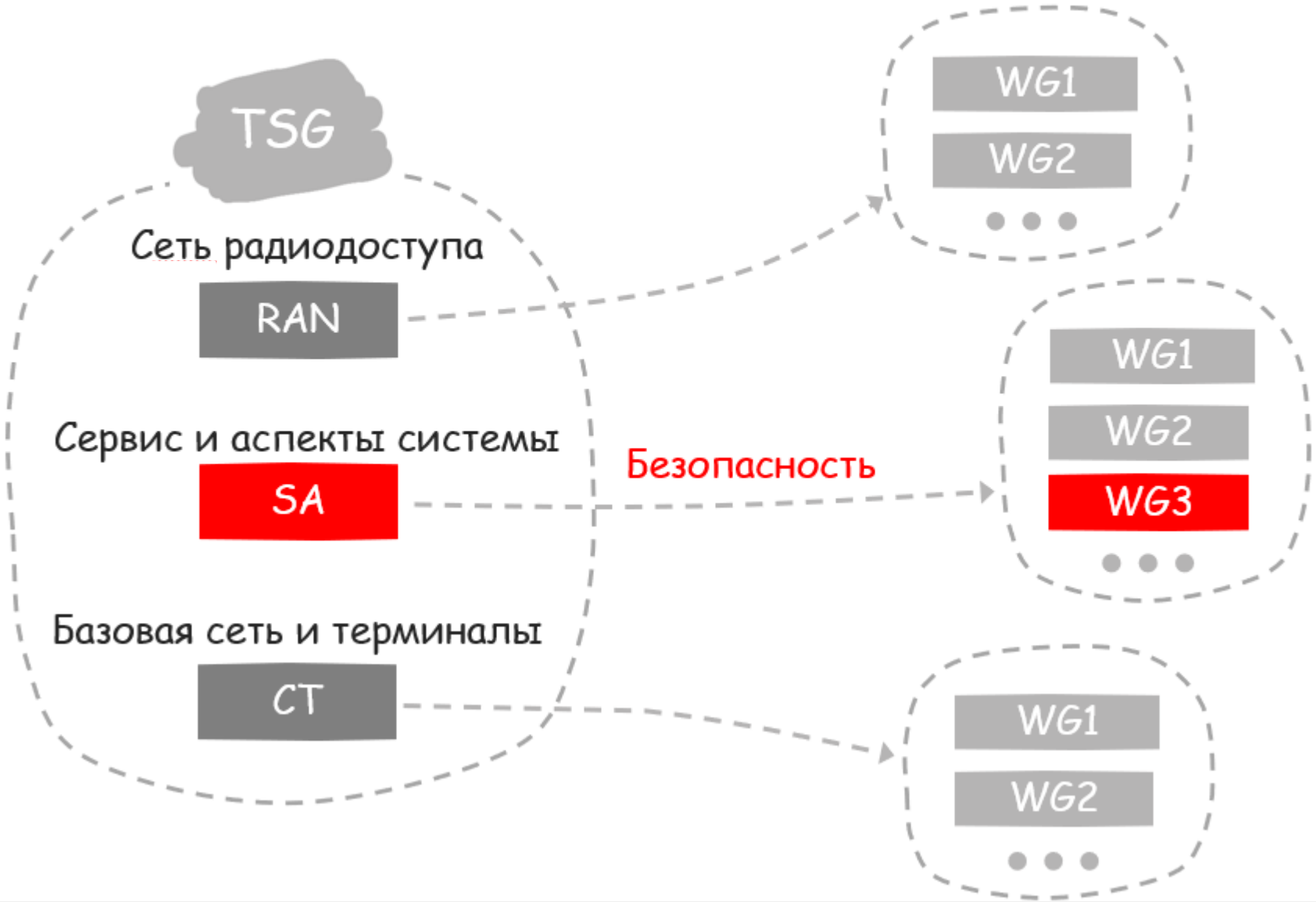
😕 Зашитые зарубежные алгоритмы

😕 Огромный объём документации, сложность проведения полного аудита безопасности за приемлемое время



ГОСТ

Работа над спецификацией 3GPP выполняется в группах технических спецификаций (**TSG**) и рабочих группах (**WG**).



5G глазами ленивого криптографа

Реализация работ по линии Стандартизации в 2021 году

Приобретение экспертного веса в 3GPP

- ✓ Участие в дискуссиях WG SA3,
- ✓ Проведение криптографического анализа и внесение предложений

- ✓ Добавлена опциональность использования криптографических механизмов на всех этапах работы системы
- ✓ Устранены фундаментальные уязвимости протокола

Разработка и анализ «криптонаборов»
на базе российских криптографических алгоритмов

Внесение предложений в 3GPP
о стандартизации отечественной криптографии в 5G

Внесение предложений в Росстандарт
о стандартизации отечественной криптографии в 5G

Реализация работ по линии Стандартизации в 2021 году

Приобретение экспертного веса в 3GPP

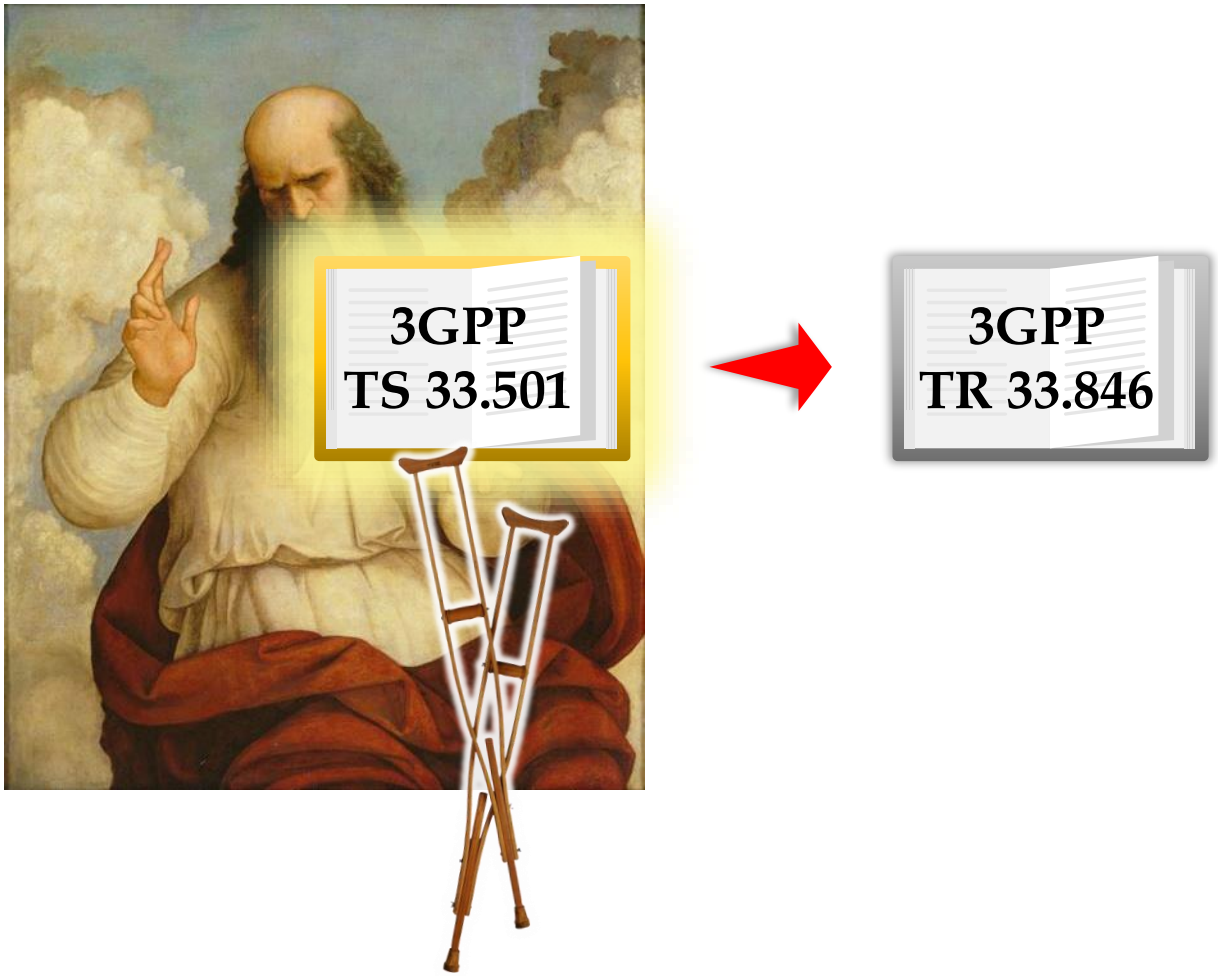
- ✓ Участие в дискуссиях WG SA3,
- ✓ Проведение криптографического анализа и внесение предложений

- ✓ Добавлена опциональность использования криптографических механизмов на всех этапах работы системы
- ✓ Устранены фундаментальные уязвимости протокола

Разработка и анализ «криптонаборов»
на базе российских криптографических алгоритмов

Внесение предложений в 3GPP
о стандартизации отечественной криптографии в 5G

Внесение предложений в Росстандарт
о стандартизации отечественной криптографии в 5G


3GPP
TS 33.501
3GPP
TR 33.846

Key Issues	Security threats	Comments
Key Issue #2.1: Linkability by distinguishing MAC failure and synchronization failure	Traceability of the user/victim by IMSI-probing when an attacker tries to find out whether the subscriber with this identity is present in a given area.	Overall impact of the attack is low as it is only one of multiple IMSI probing type attacks that can be launched and so preventing this particular attack would not resolve the overall issue.
Key Issue #2.2: Linkability by SUCI replay	Traceability of the user/victim by IMSI-probing when an attacker tries to find out whether the subscriber with this identity is present in a given area.	Overall impact of the attack is low as it is only one of multiple IMSI probing type attacks that can be launched and so preventing this particular attack would not resolve the overall issue.
Key Issue #2.2: Linkability by generation of different SUCIs	Traceability of the user/victim by IMSI-probing when an attacker tries to find out whether the subscriber with this identity is present in a given area.	Overall impact of the attack is low as it is only one of multiple IMSI probing type attacks that can be launched and so preventing this particular attack would not resolve the overall issue.
Key Issue #2.2: DoS attack	DoS attack on UDM	Overall impact of this attack is low.

Модель нарушителя до сих пор не согласована до конца: выдвигается предложения вычеркнуть основные угрозы 2.1, 2.2 и 3.2, поскольку есть более простые способы их реализовать (imsi paging).

В чем смысл IND-CPA модели, если существует молоток и паяльник?

*«... The attacker could generate valid SUCI **only if he knows the home network public key** associated to the subscription...»*

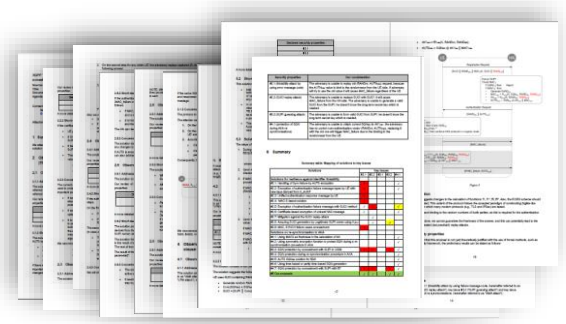
*«... **The cell area is very big so it is difficult to trace the UE**...»*

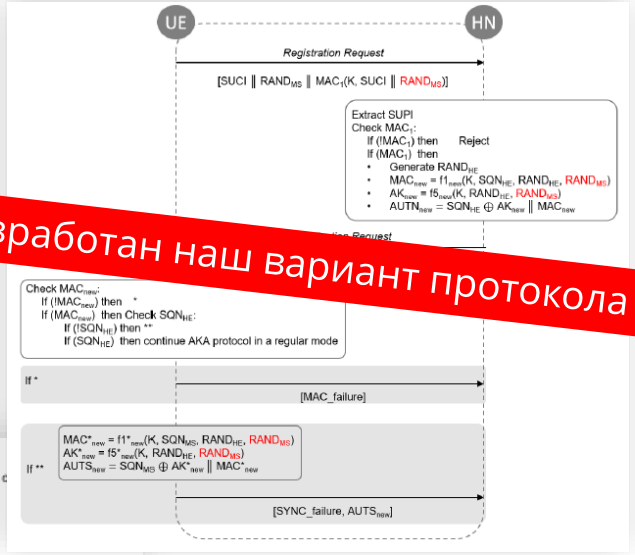
*«...encrypt the AUTS/random number and failure code, and the AUSF uses the K_{AUSF} stored during previously successful authentication to decrypt the AUTS/random number and failure code. ... If no stored K_{AUSF}, **the KEY is a 256-bit binary string of all 0s**»*

ДОКАЗАТЕЛЬНАЯ МЕДИЦИНА
Триша Гринхальх
ОСНОВЫ ДОКАЗАТЕЛЬНОЙ МЕДИЦИНЫ

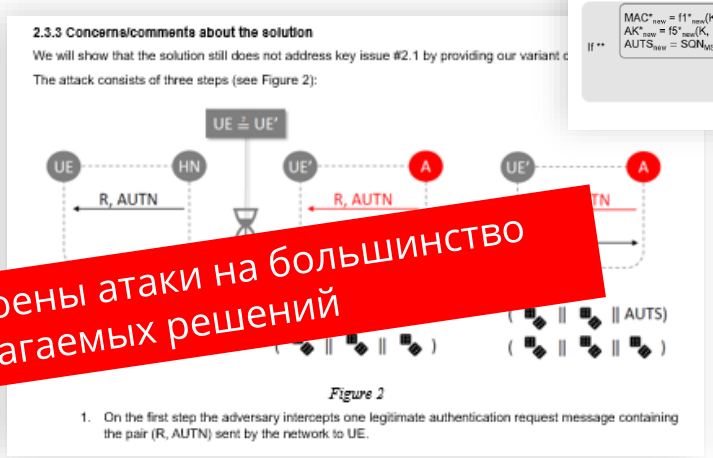
+

Подготовлен solution proposal к документу TR 33.846





Разработан наш вариант протокола



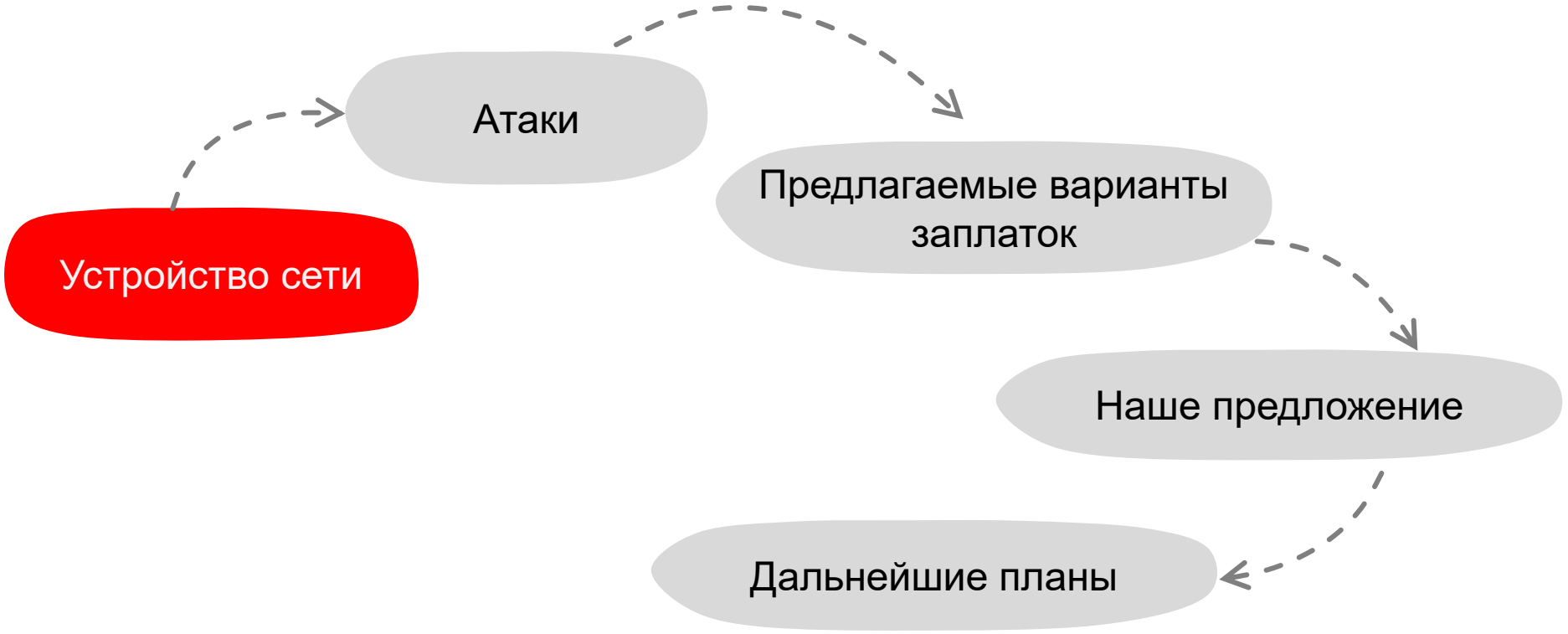
Построены атаки на большинство предлагаемых решений

В реальности подобная работа невозможна без тесного взаимодействия со специалистами в сфере телекоммуникаций!

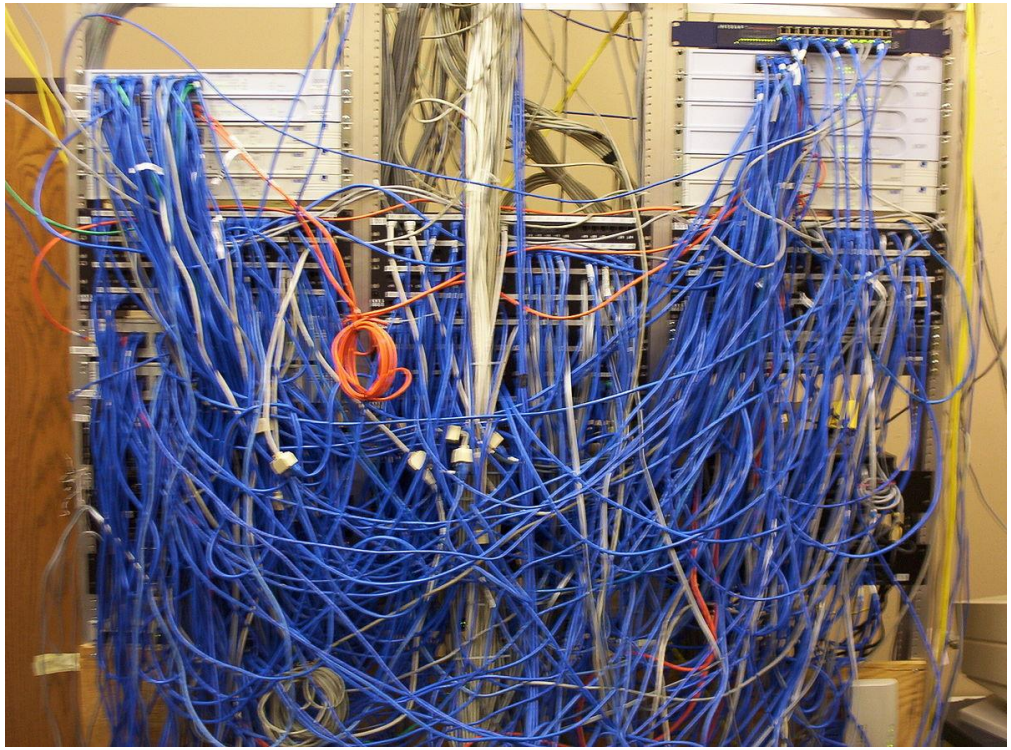
Разберемся поподробнее…

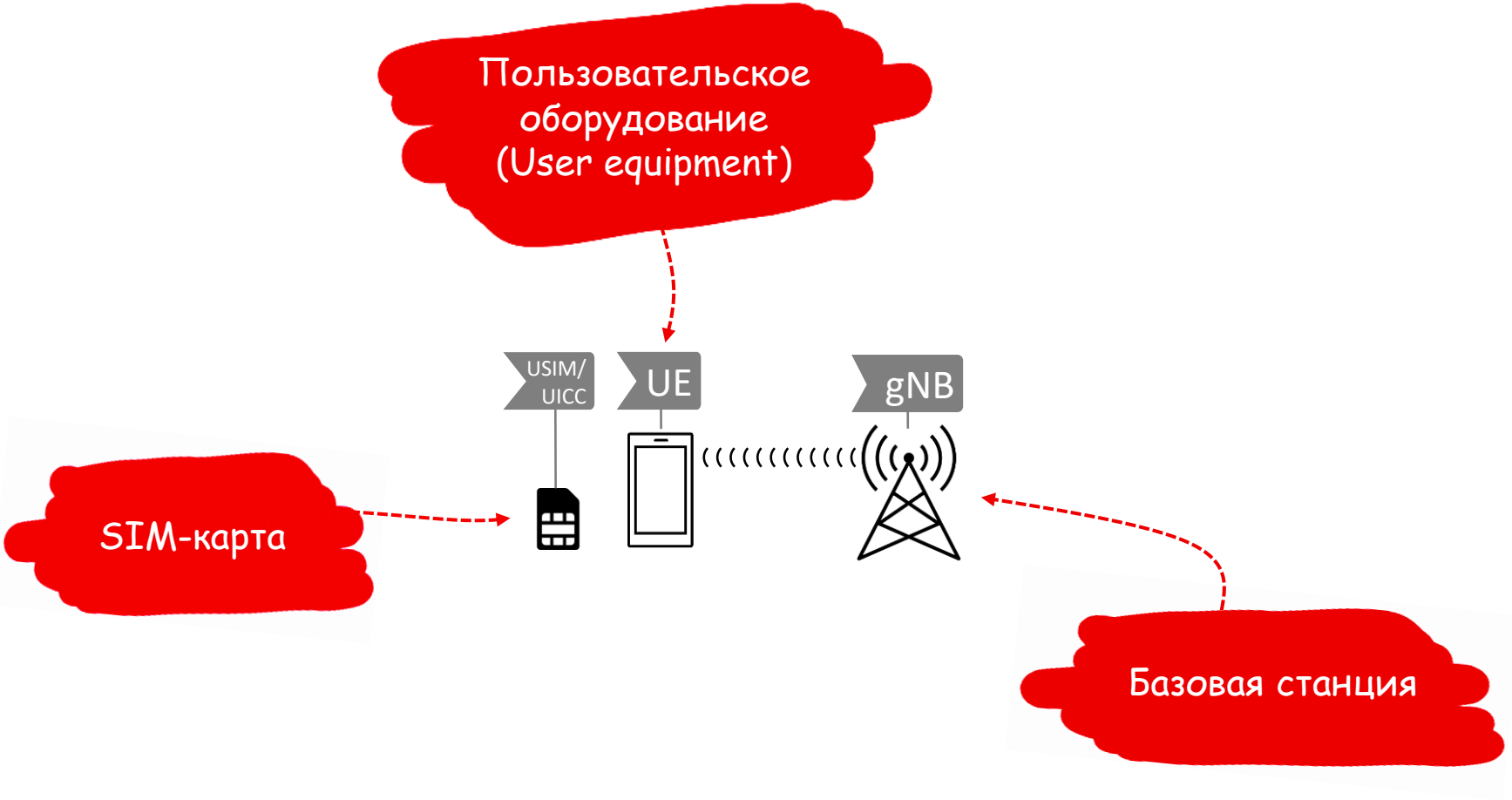
Разработан наш вариант протокола

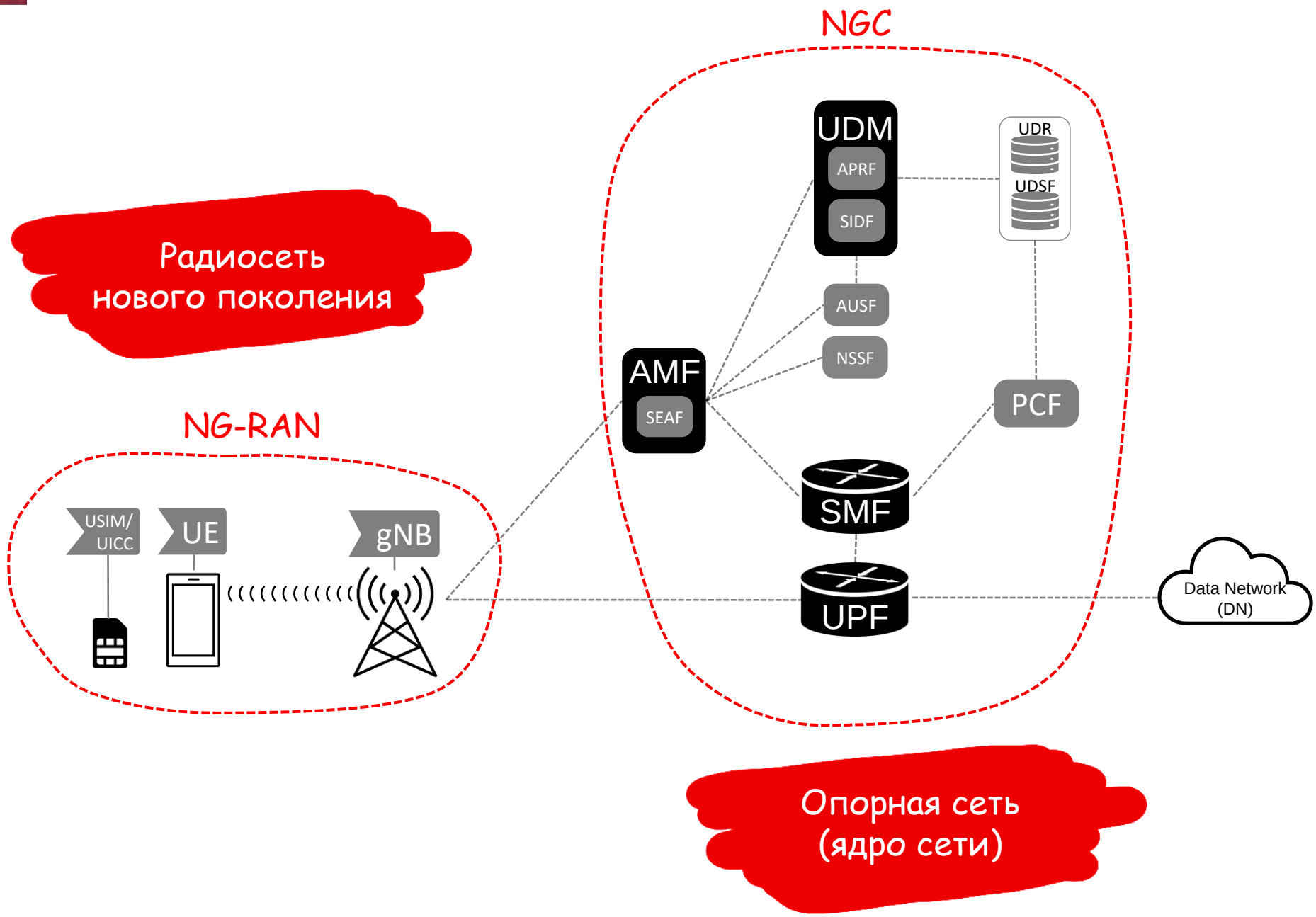
Построены атаки на большинство предлагаемых решений


Атаки
Предлагаемые варианты заплаток
Наше предложение
Дальнейшие планы
Устройство сети

5G устройство сети

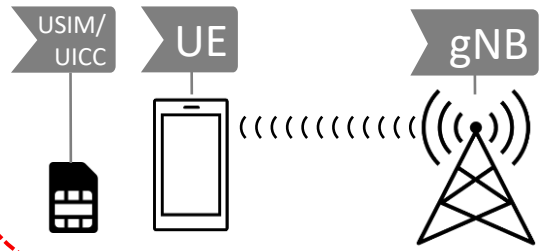



Пользовательское оборудование (User equipment)
USIM/ UICC
UE
gNB
SIM-карта
Базовая станция

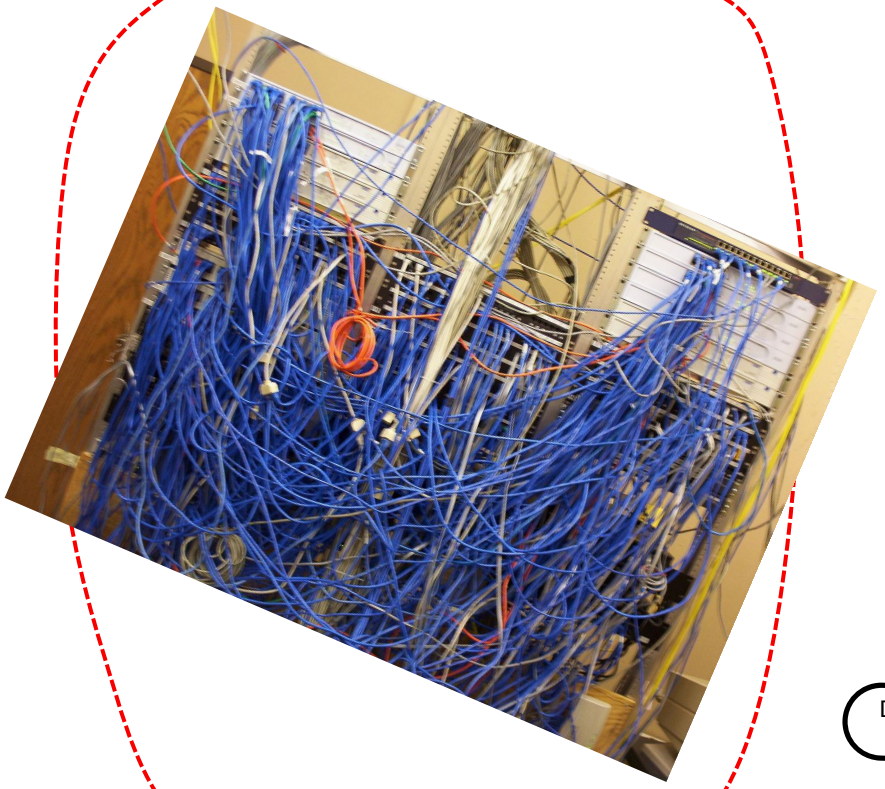

NGC
UDM
APRF
SIDF
UDR
UDSF
AUSF
NSSF
AMF
SEAF
PCF
SMF
UPF
Data Network
(DN)
Радиосеть
нового поколения
NG-RAN
USIM/
UICC
UE
gNB
Опорная сеть
(ядро сети)

Радиосеть
нового поколения

NG-RAN



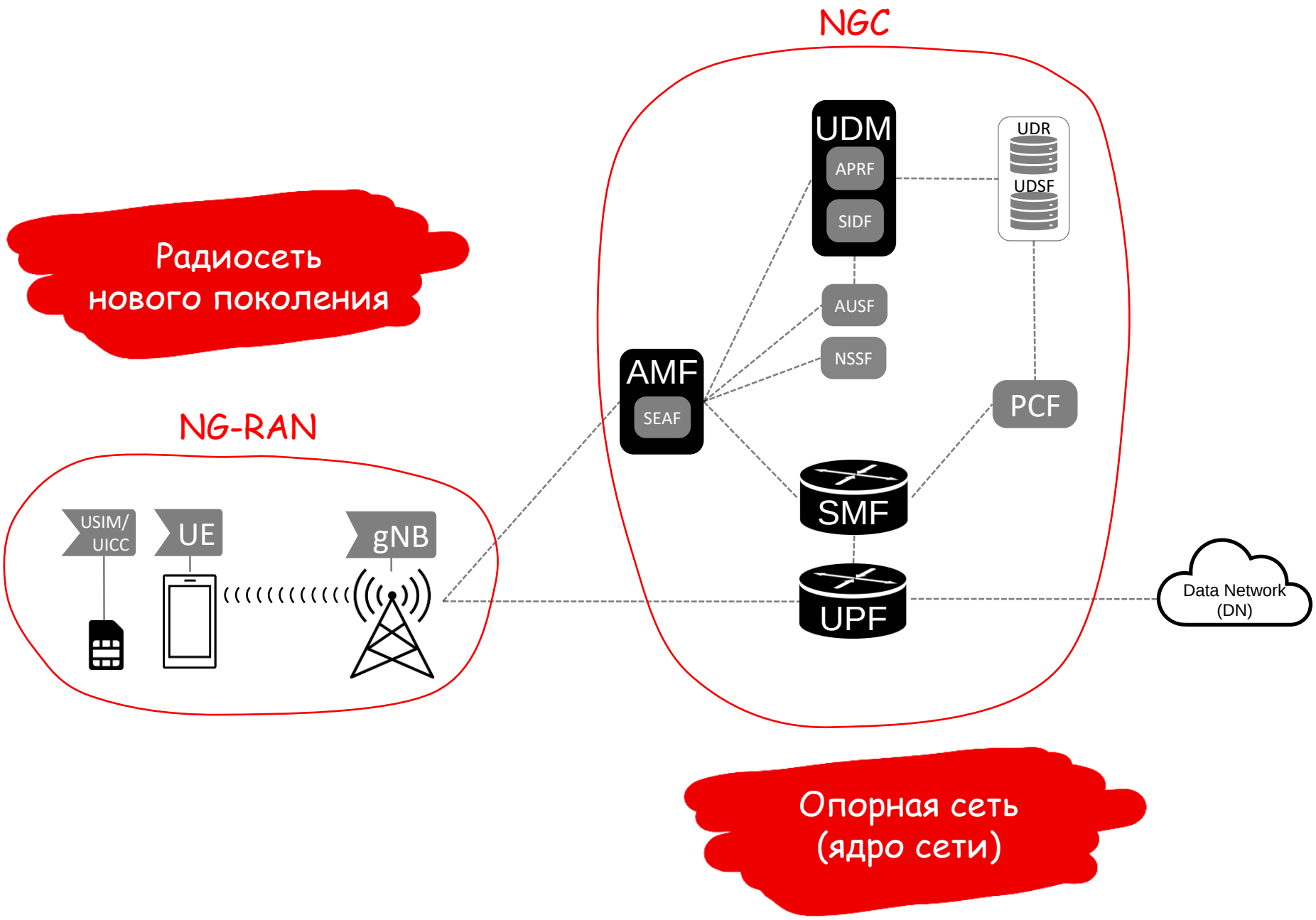
NGC

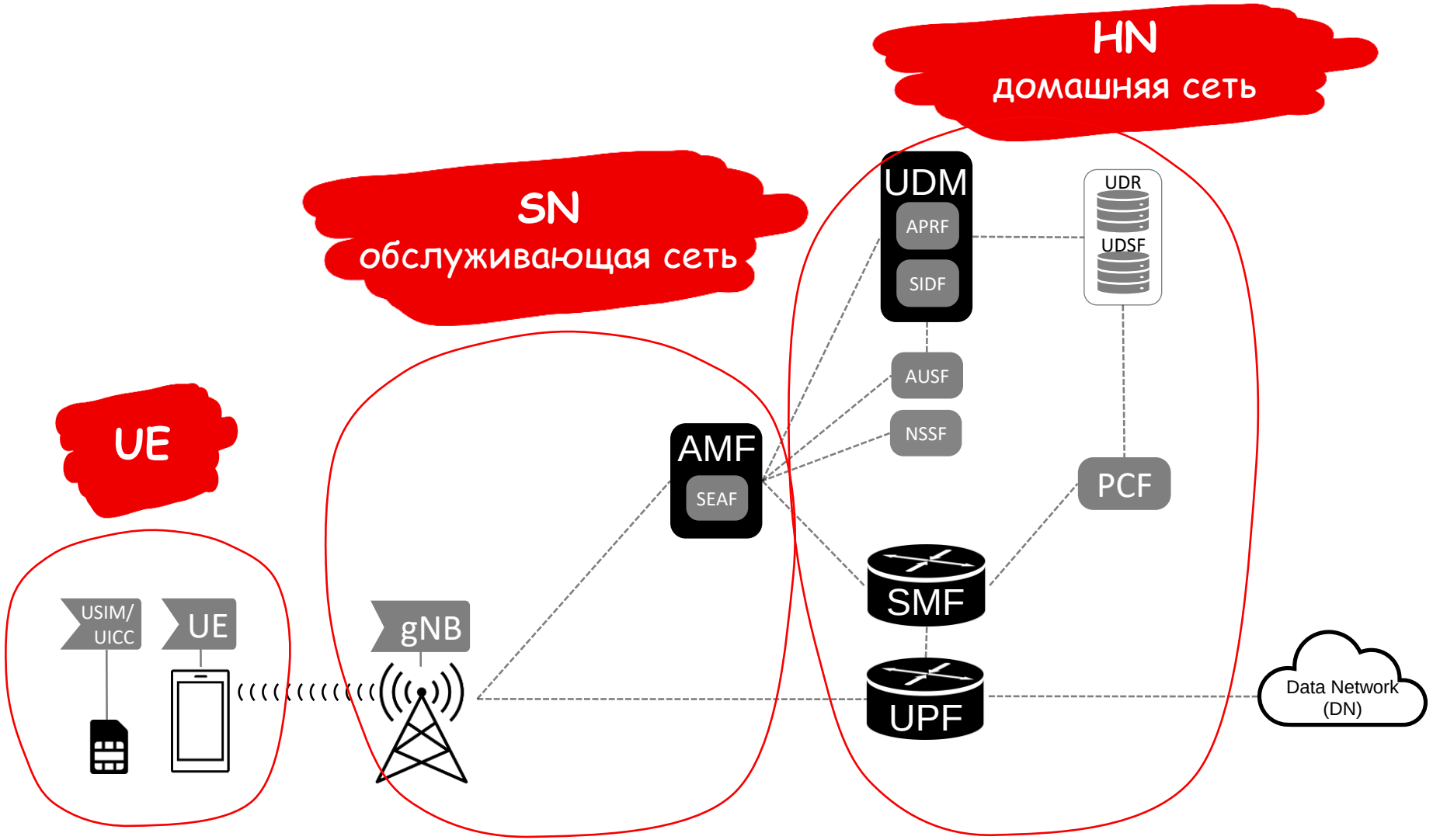


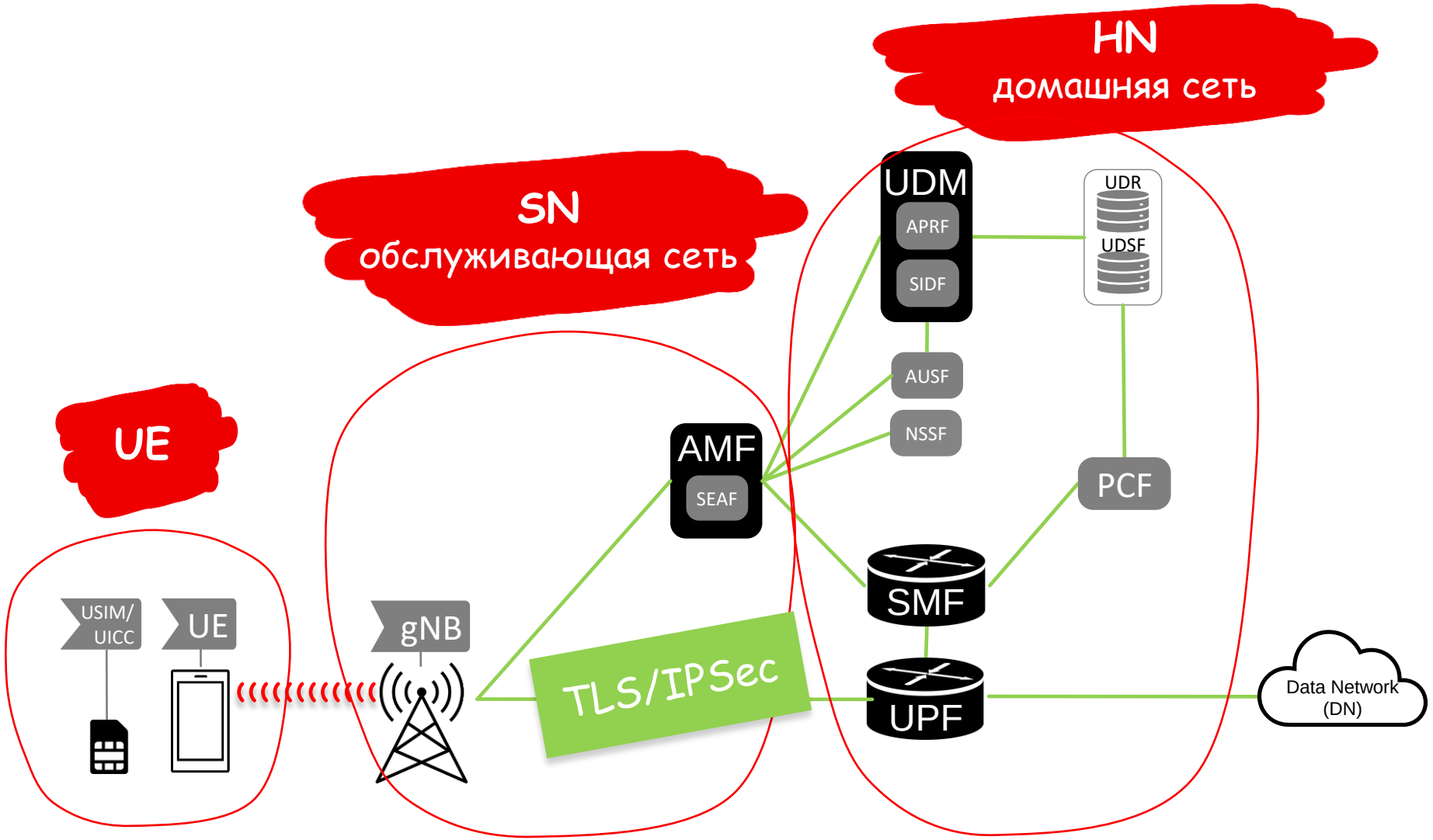
Data Network
(DN)

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)

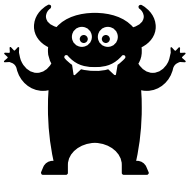

HN
домашняя сеть
SN
обслуживающая сеть
UE
UDM
APRF
SIDF
UDR
UDSF
AUSF
NSSF
AMF
SEAF
PCF
SMF
USIM/
UICC
UE
gNB
TLS/IPSec
UPF
Data Network
(DN)

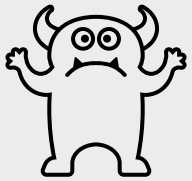
UE

SN

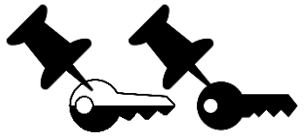
HN

SUPI, K

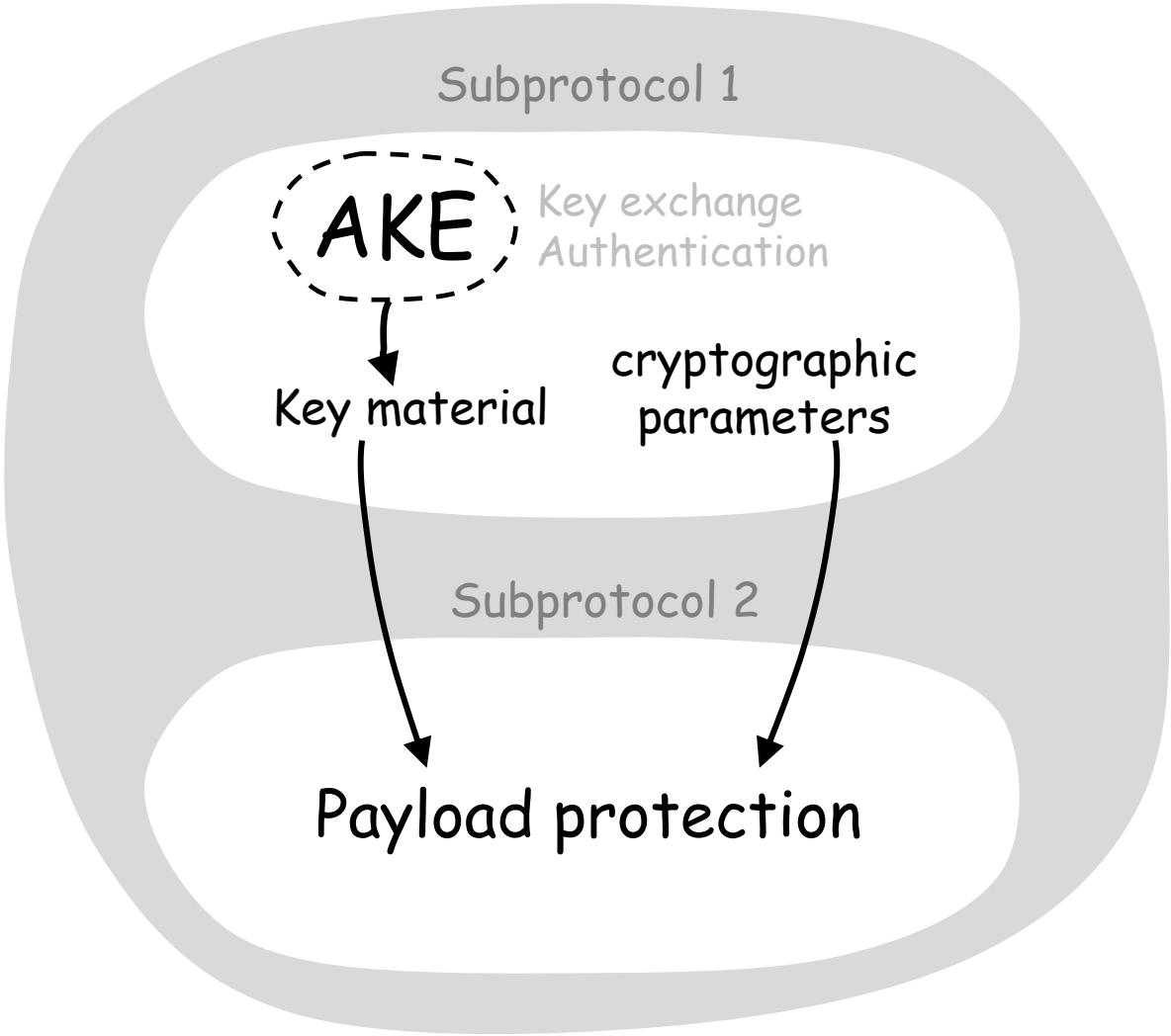




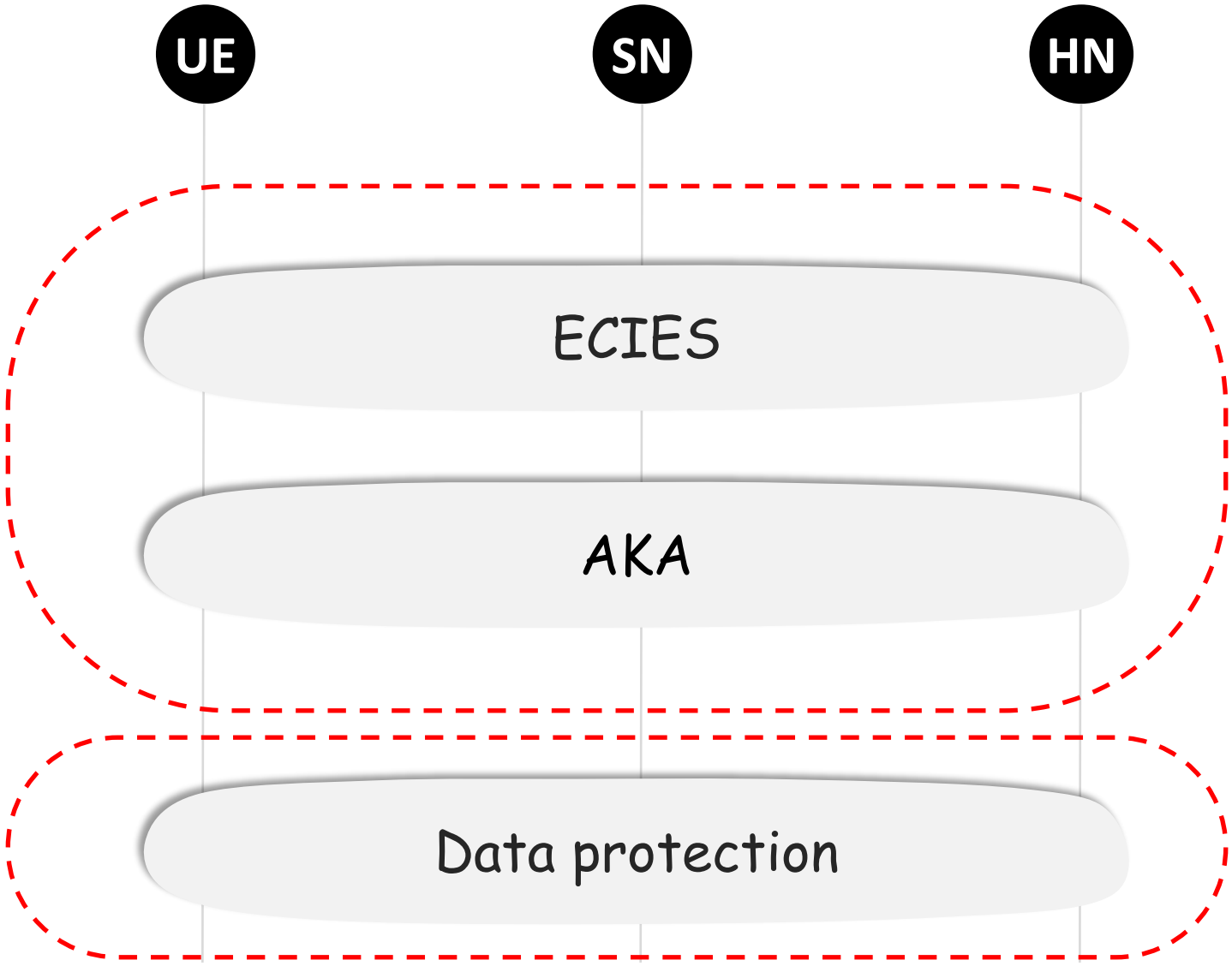
SUPI, K

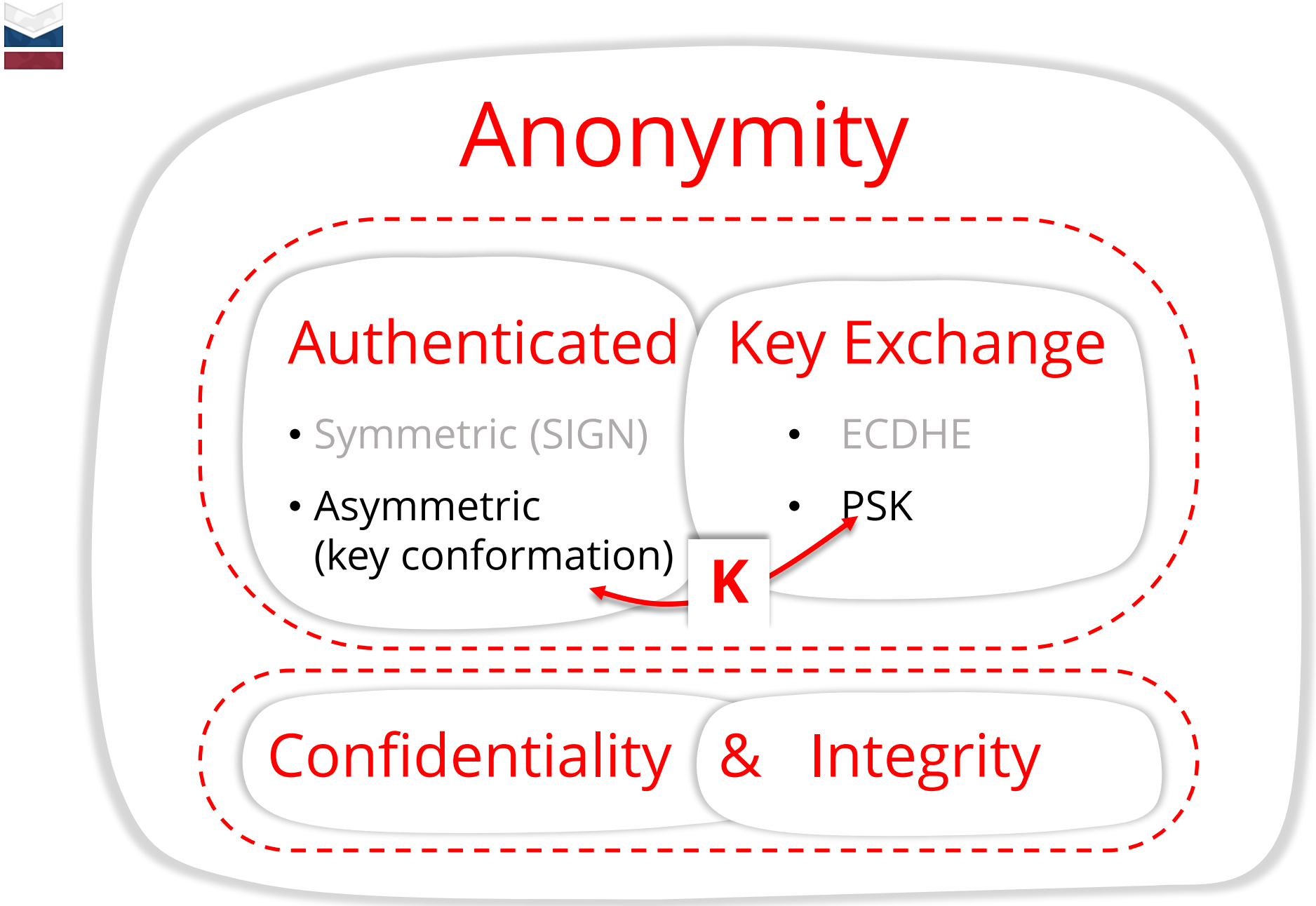


Стандартный протокол обеспечения защищенного канала связи



Примеры:


UE
SN
HN
ECIES
AKA
Data protection

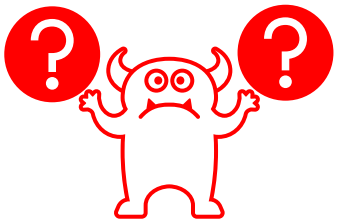

Anonymity
Authenticated
Key Exchange
• Symmetric (SIGN)
• Asymmetric
(key conformation)
• ECDHE
• PSK
K
Confidentiality
&
Integrity

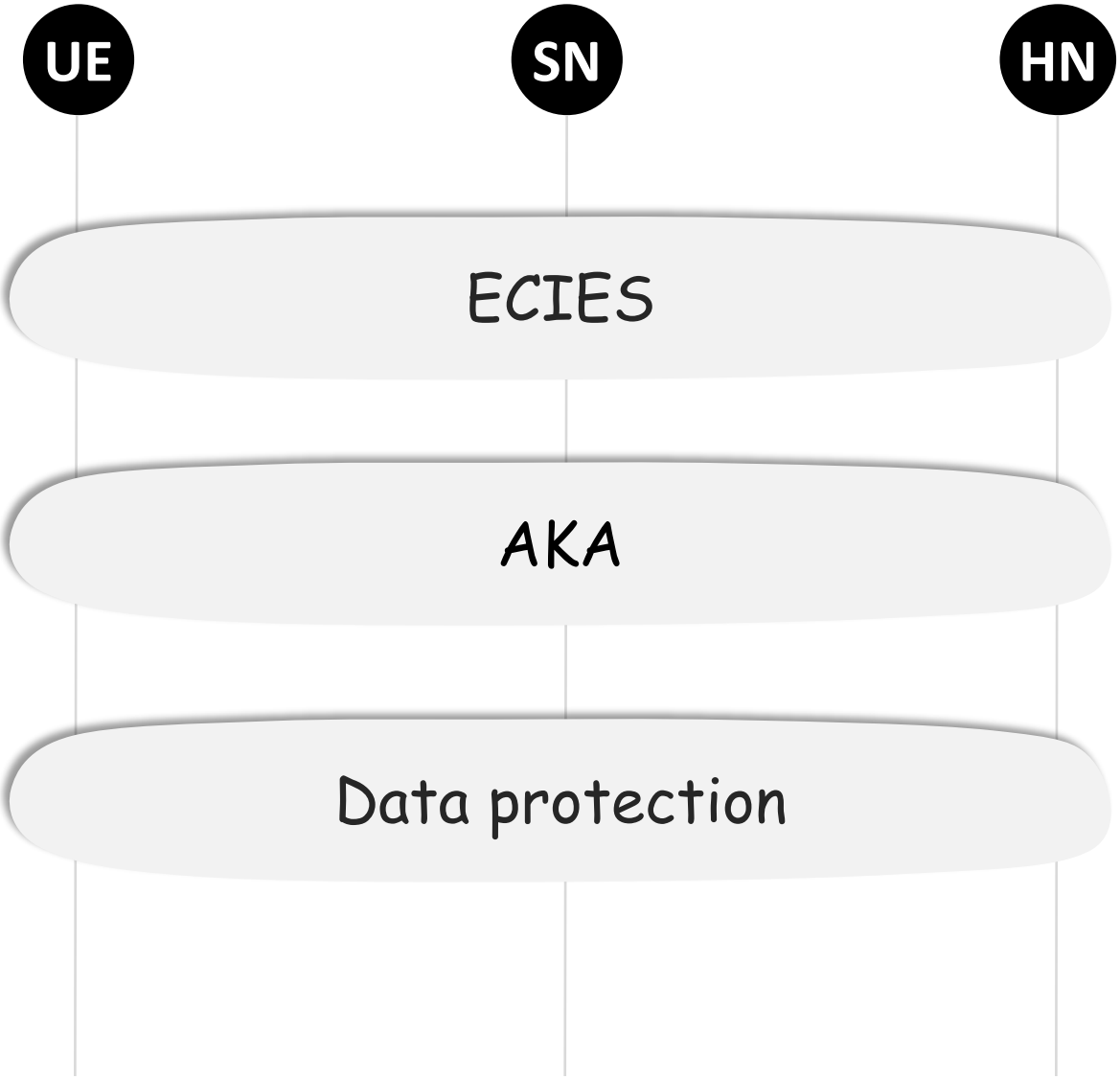
Анонимность (TS 33.102)

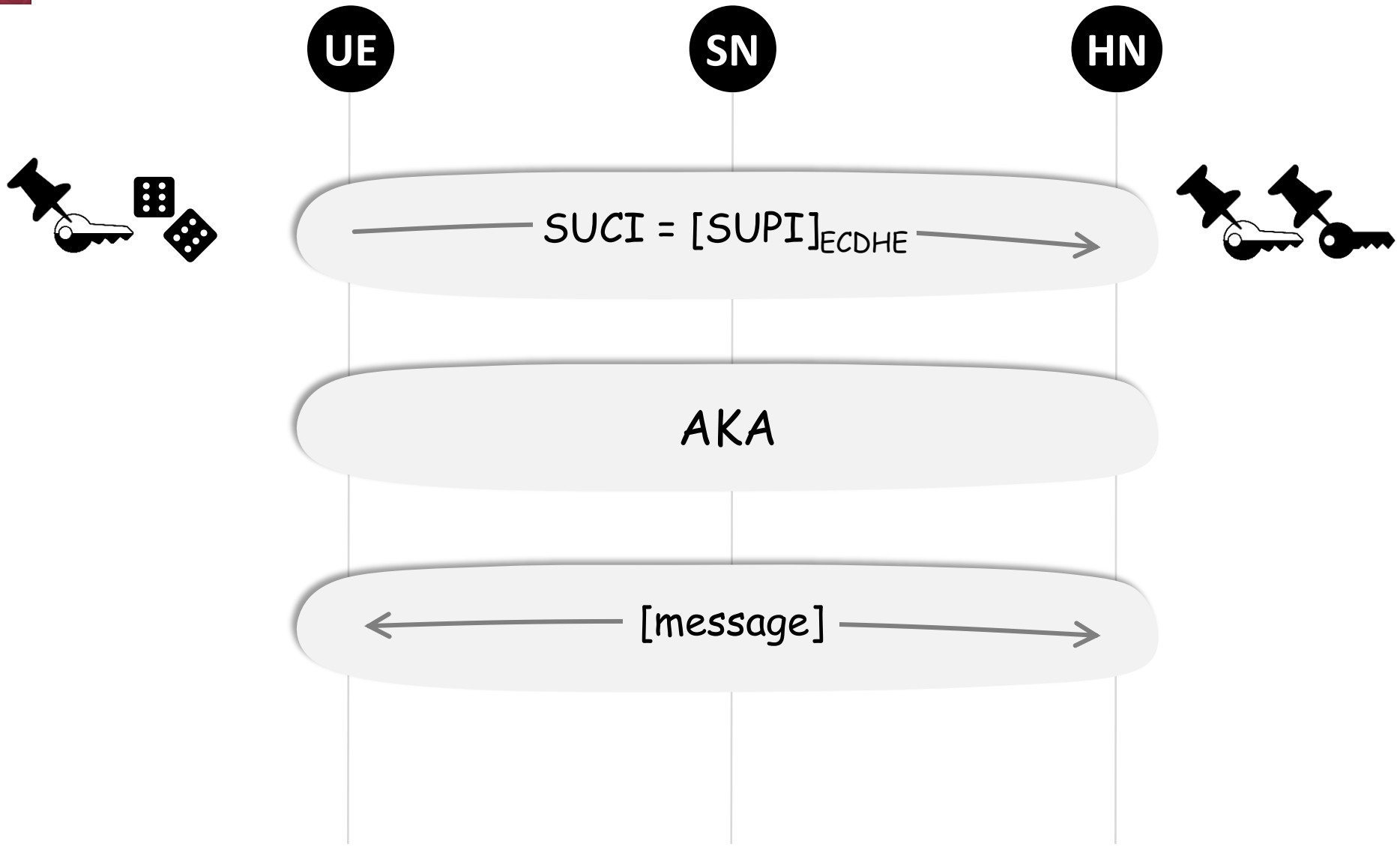
- ✓ **Конфиденциальность идентификатора пользователя**:
  постоянный идентификатор пользователя должен быть защищен от перехвата/подслушивания в радиоэфире.

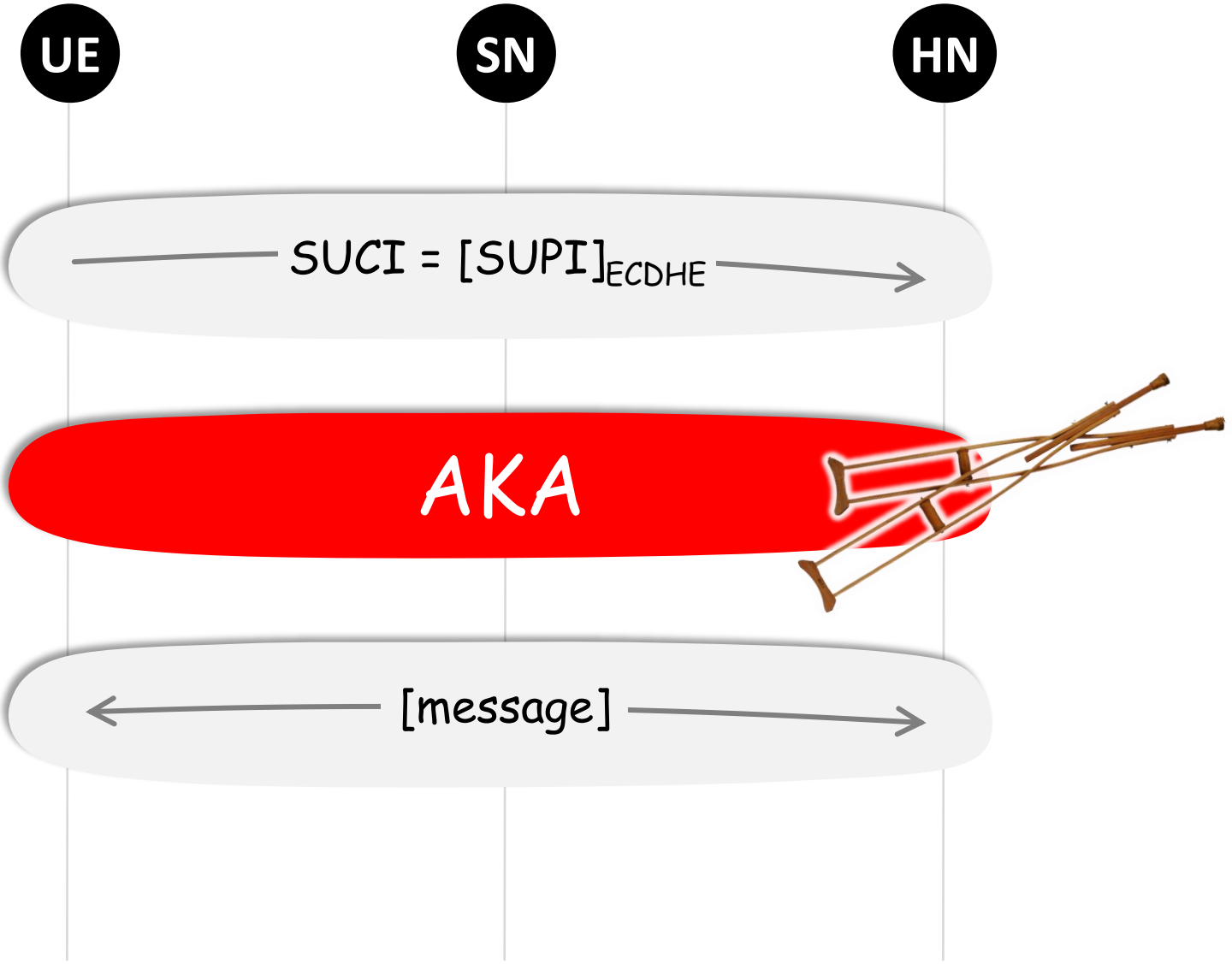
- ✓ **Конфиденциальность местоположения пользователя**:
  присутствие или прибытие пользователя в определенную местность не может быть определено путем прослушивания радиоэфира.

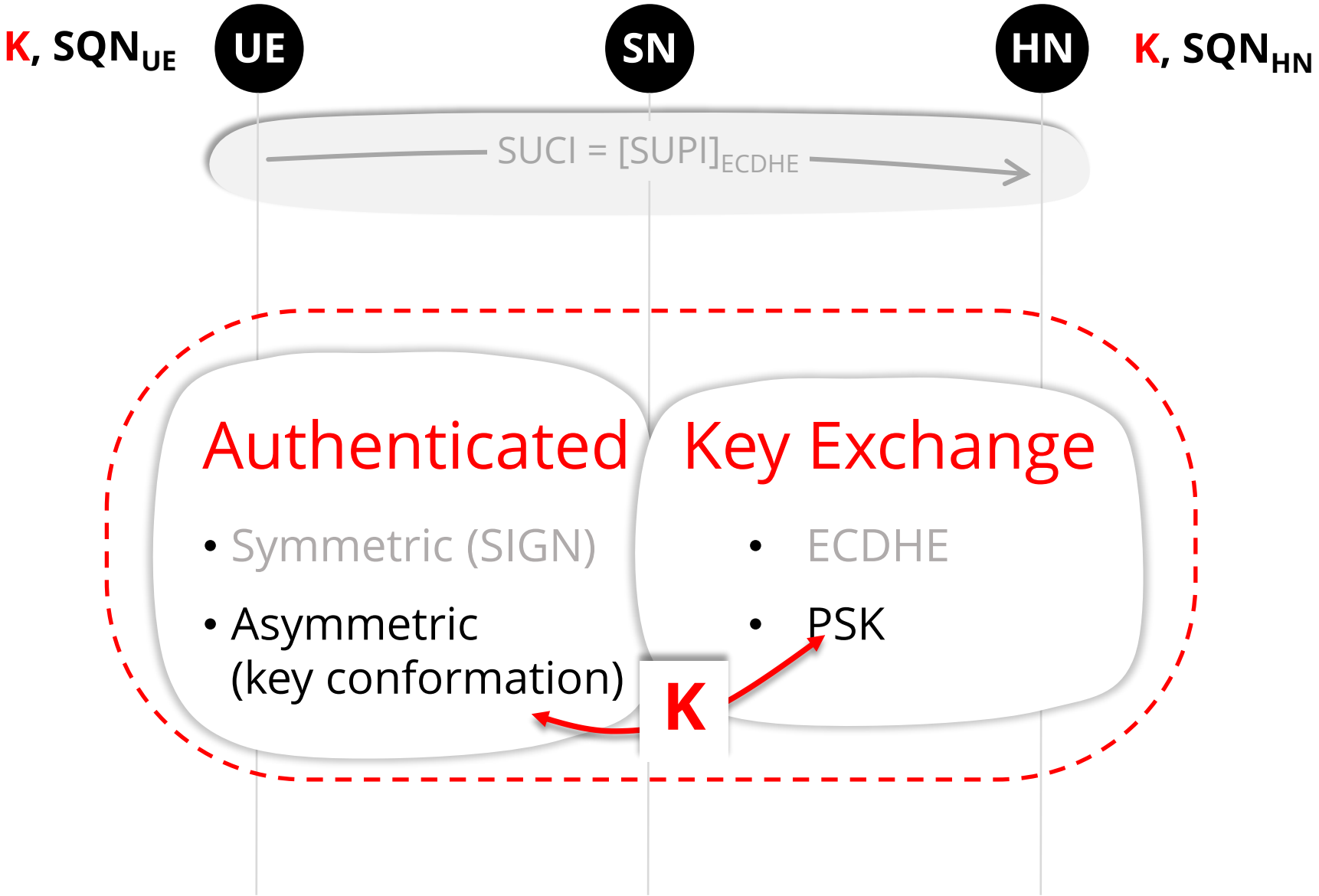
- ✓ **Невозможность сопоставления проведенных операций (untraceability, неотслеживаемость)**:
  прослушивая радиоэфир злоумышленник не должен иметь возможность узнать, были ли различные услуги предоставлены одному и тому же абоненту.

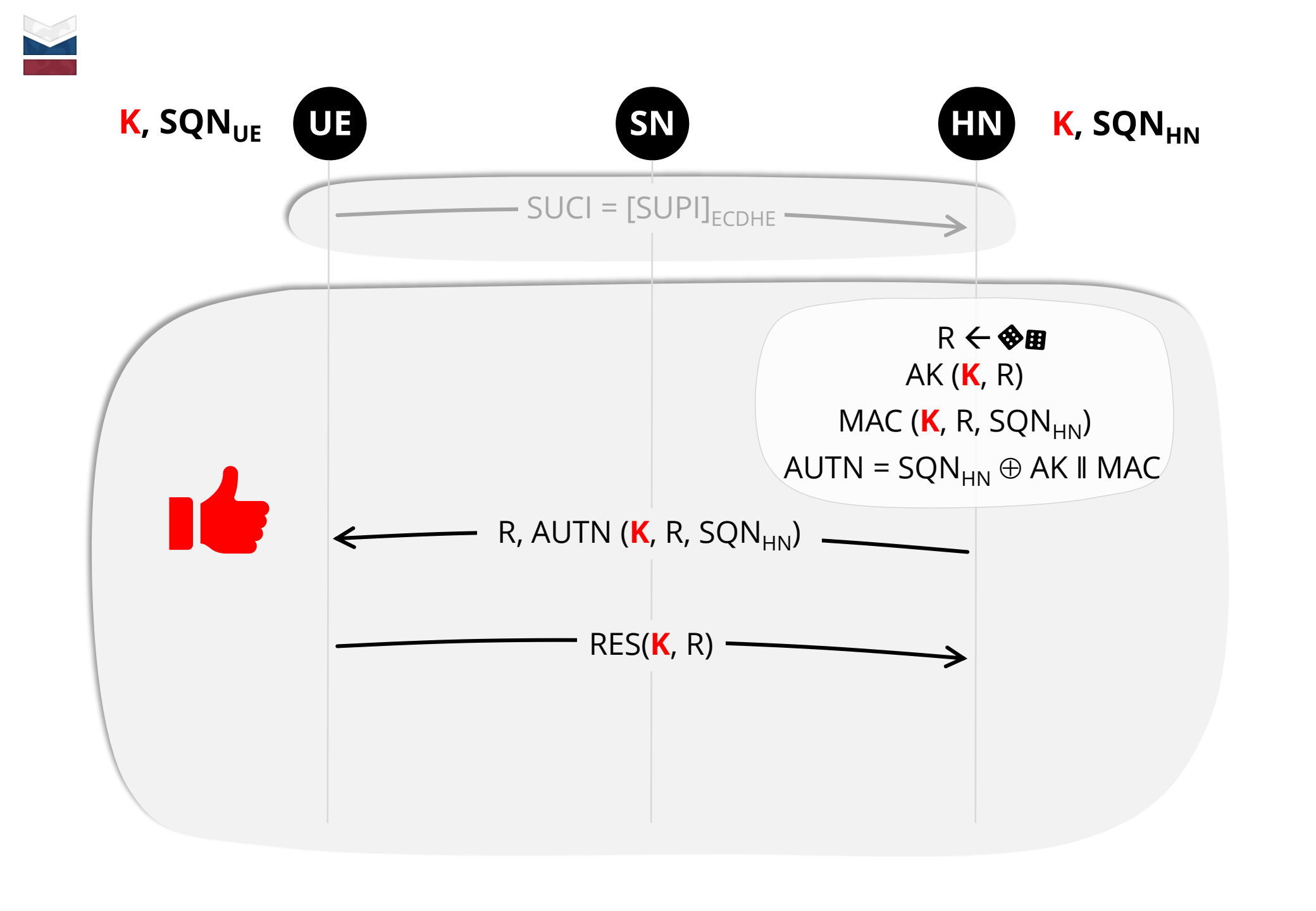


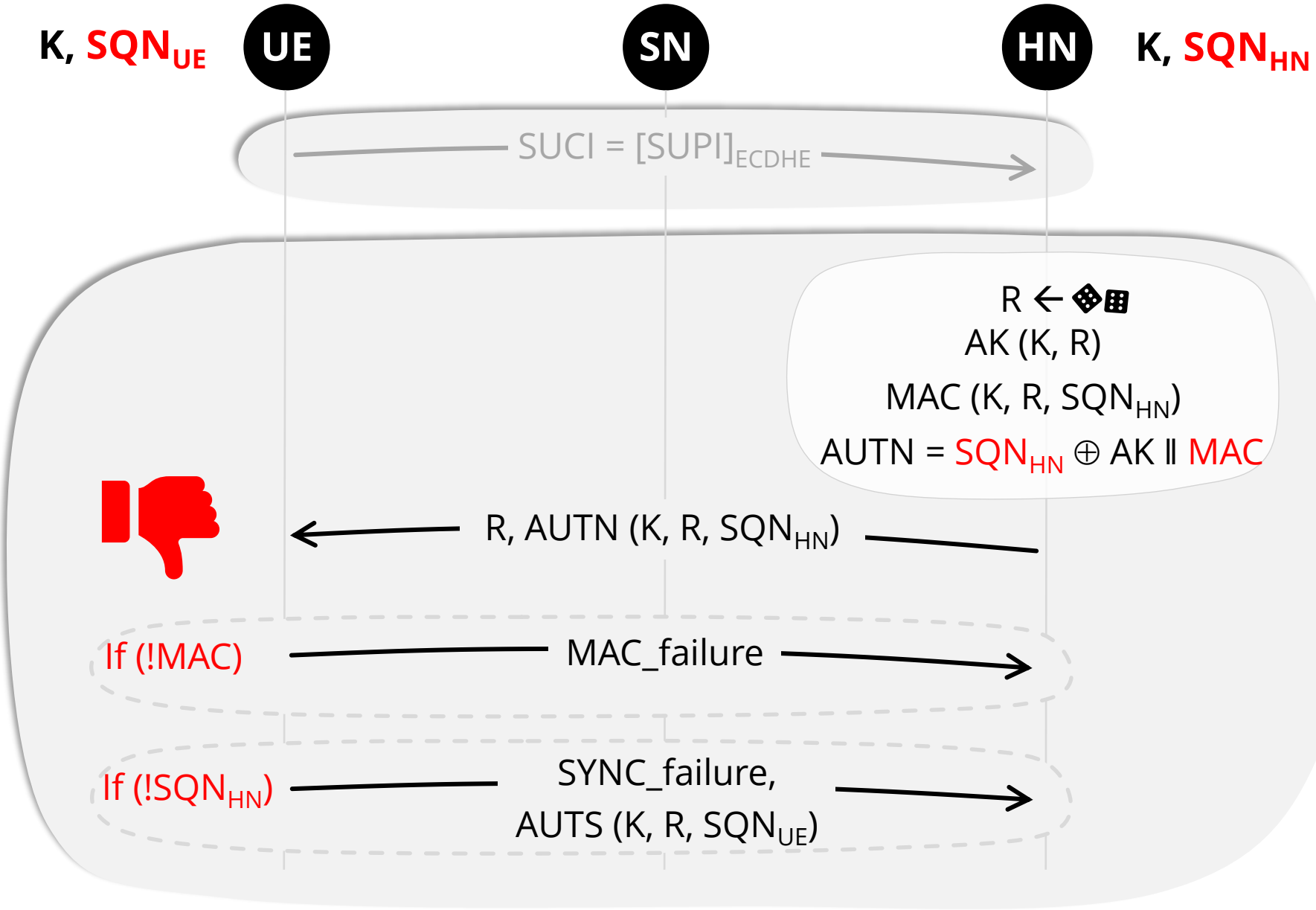

UE
SN
HN
ECIES
AKA
Data protection

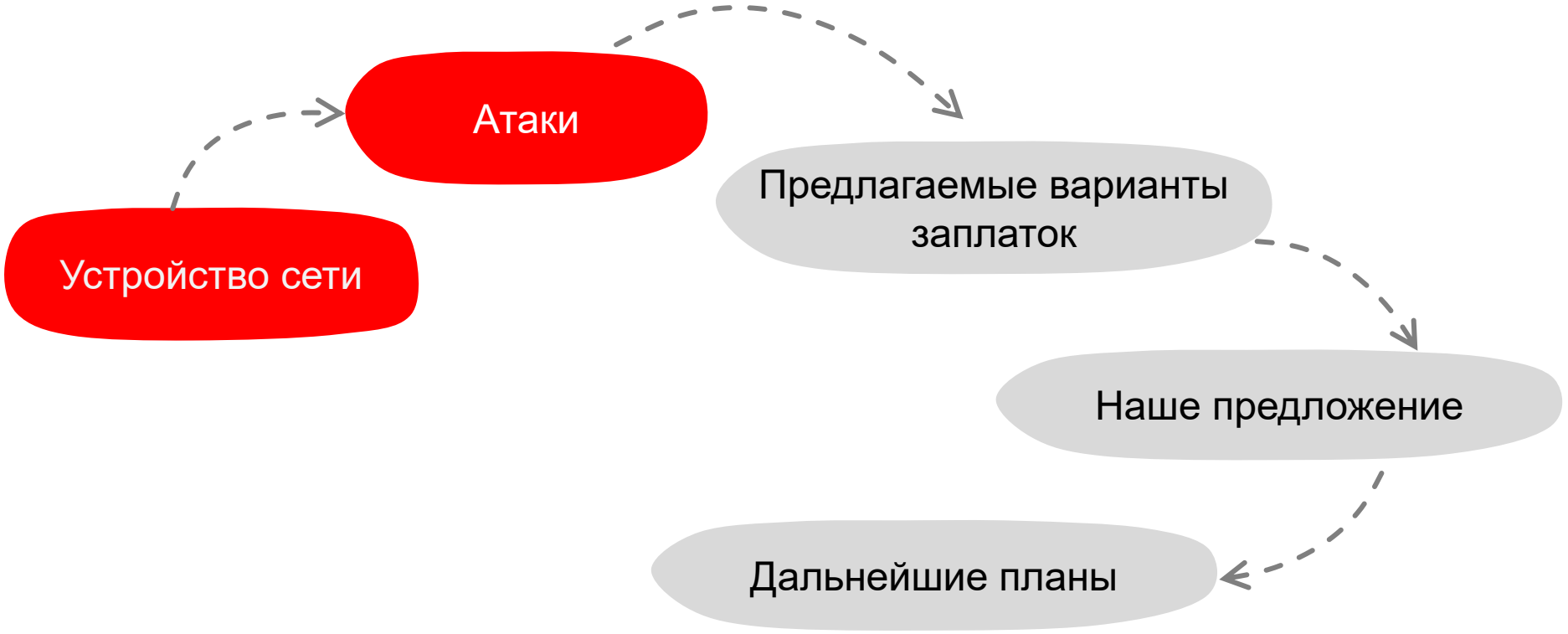

UE
SN
HN
SUCI = [SUPI]ECDHE
AKA
[message]


UE
SN
HN
SUCI = [SUPI]ECDHE
AKA
[message]

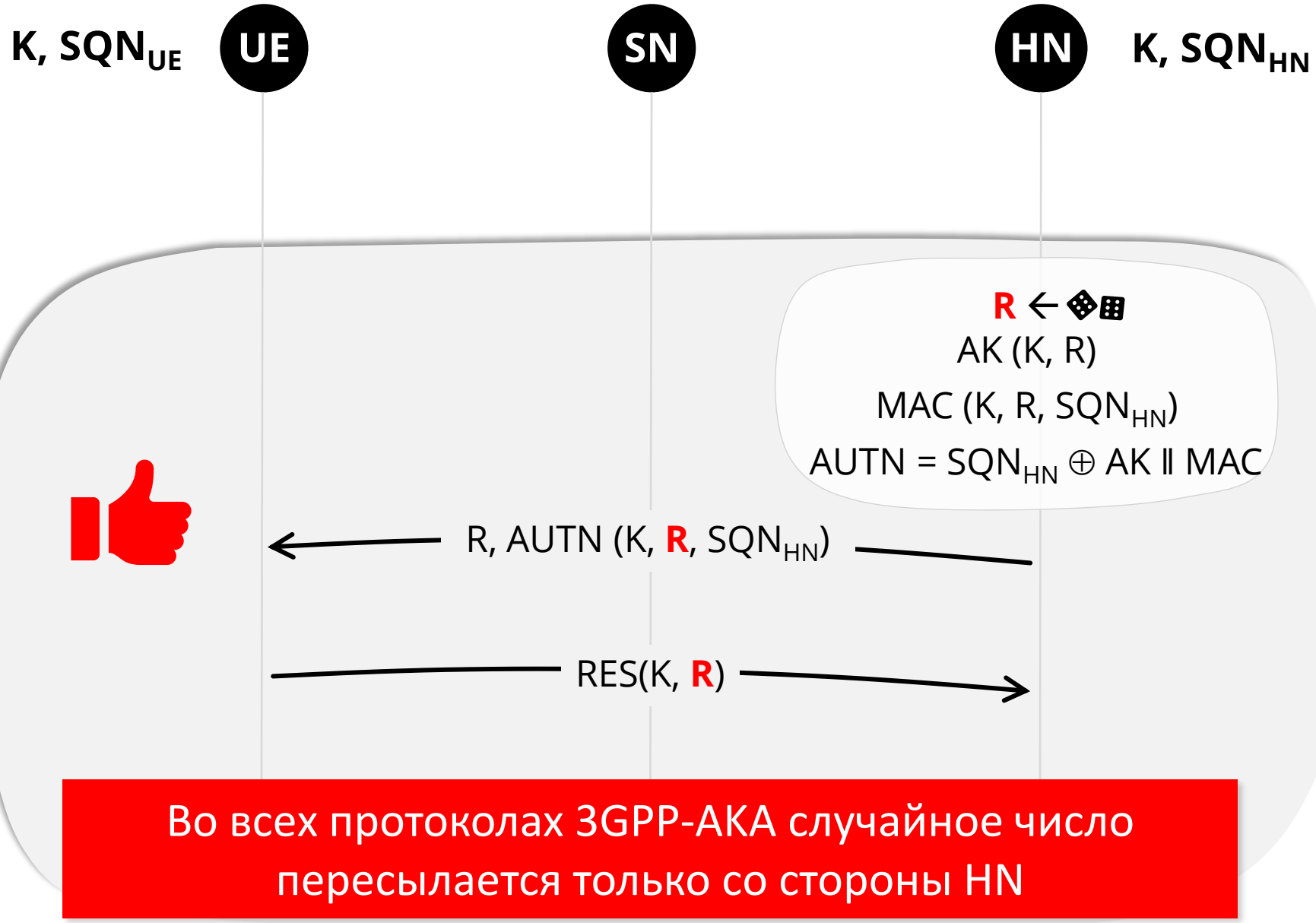

K, SQN_UE
UE
SN
HN
K, SQN_HN
SUCI = [SUPI]_ECDHE
Authenticated
• Symmetric (SIGN)
• Asymmetric (key conformation)
Key Exchange
• ECDHE
• PSK
K


K, SQN_UE
UE
SN
HN
K, SQN_HN
SUCI = [SUPI]_ECDHE
R ← 🎲
AK (K, R)
MAC (K, R, SQN_HN)
AUTN = SQN_HN ⊕ AK ‖ MAC
R, AUTN (K, R, SQN_HN)
RES(K, R)


K, SQN_UE
UE
SN
HN
K, SQN_HN
SUCI = [SUPI]_ECDHE
R ← ⚄
AK (K, R)
MAC (K, R, SQN_HN)
AUTN = SQN_HN ⊕ AK ‖ MAC
R, AUTN (K, R, SQN_HN)
If (!MAC)
MAC_failure
If (!SQN_HN)
SYNC_failure,
AUTS (K, R, SQN_UE)


Атаки
Устройство сети
Предлагаемые варианты заплаток
Наше предложение
Дальнейшие планы

Replay атаки


K, SQN_UE
UE
SN
HN
K, SQN_HN
R ← 🎲
AK (K, R)
MAC (K, R, SQN_HN)
AUTN = SQN_HN ⊕ AK ‖ MAC
R, AUTN (K, R, SQN_HN)
RES(K, R)
Во всех протоколах 3GPP-AKA случайное число пересылается только со стороны HN

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

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.

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

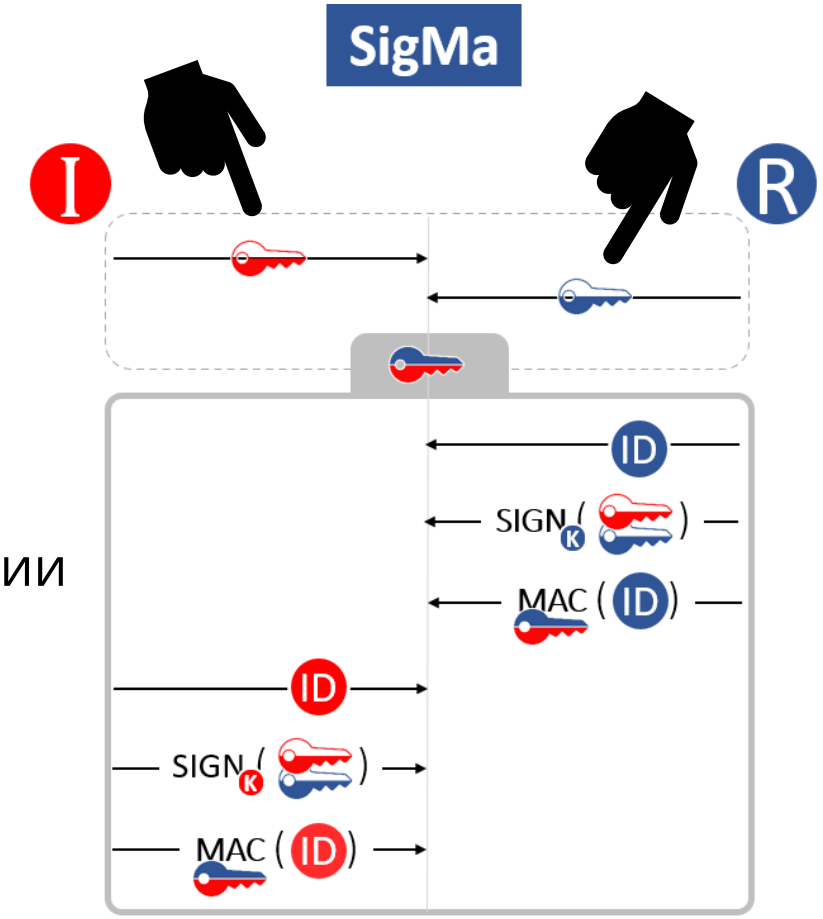
Например, в протоколе TLS 1.2 Handshake такой способ реализуется за счет обмена сторонами случайными значениями r_C, r_S.

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:

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

Ну это теория, а что на практике?

Рассмотрим три 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

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

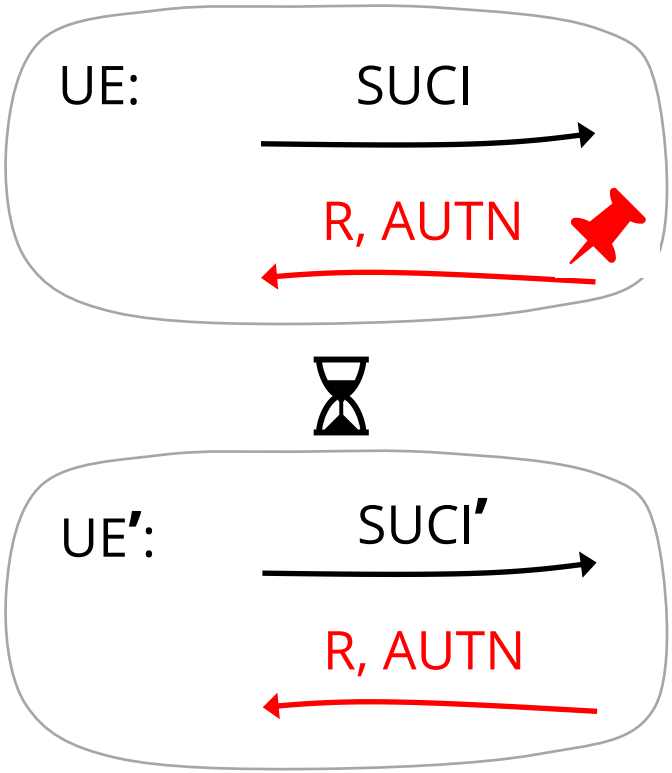
Ravishankar Borgaonkar, Lucca Hirschi*, Shinjo Park, and Altaf Shaik

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,

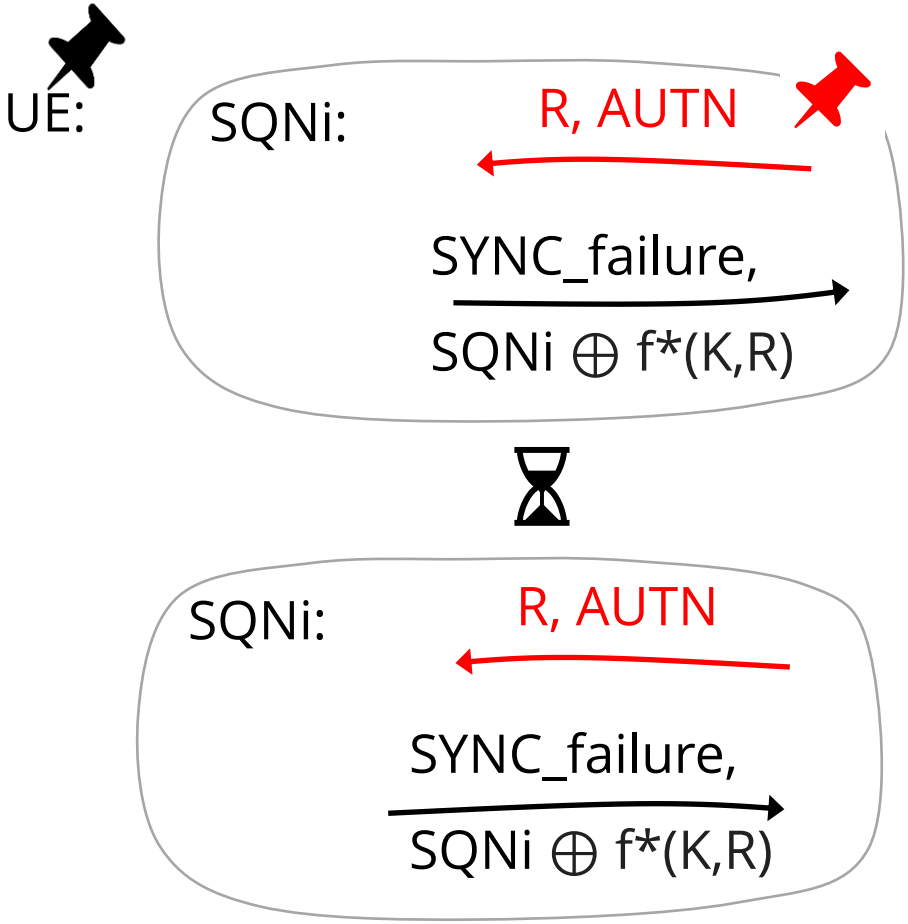
LFM



UE = UE' → SYNC_failure

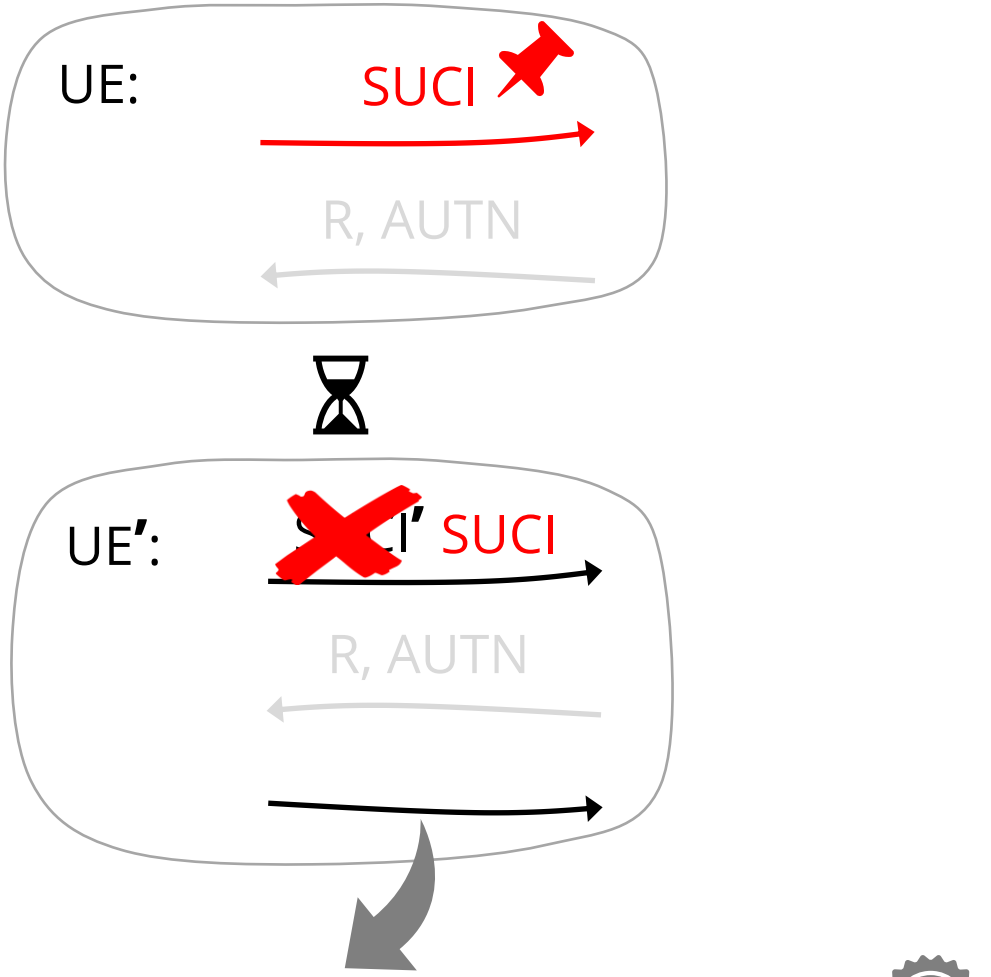
UE ≠ UE' → MAC_failure

AMA



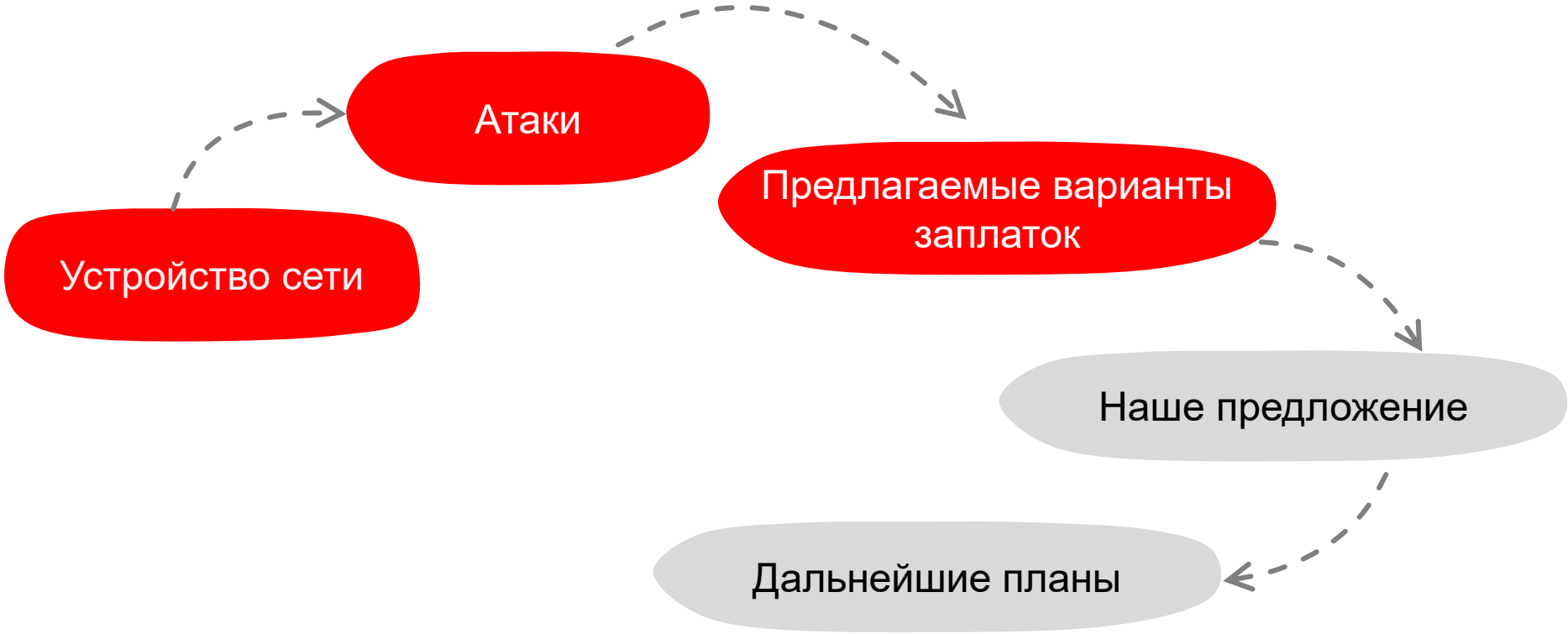
SQNi ⊕ SQNj

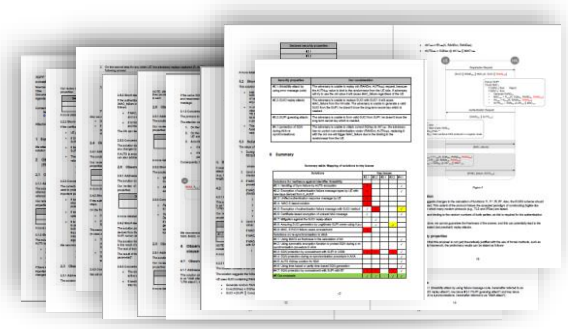
SUCI replay



UE = UE' → Continue protocol....

UE ≠ UE' → MAC_failure


Атаки
Устройство сети
Предлагаемые варианты заплаток
Наше предложение
Дальнейшие планы



2.3.3 Concerns/comments about the solution

We will show that the solution still does not address key issue #2.1 by providing our variant of LFM attack.

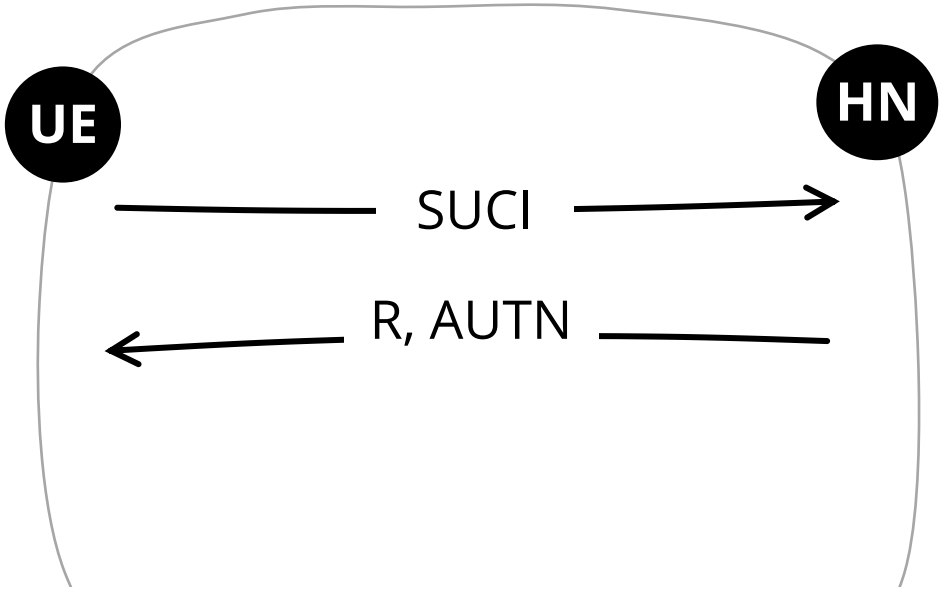
The attack consists of three steps (see Figure 2):

Figure 2

1. On the first step the adversary intercepts one legitimate authentication request message containing the pair (R, AUTN) sent by the network to UE.

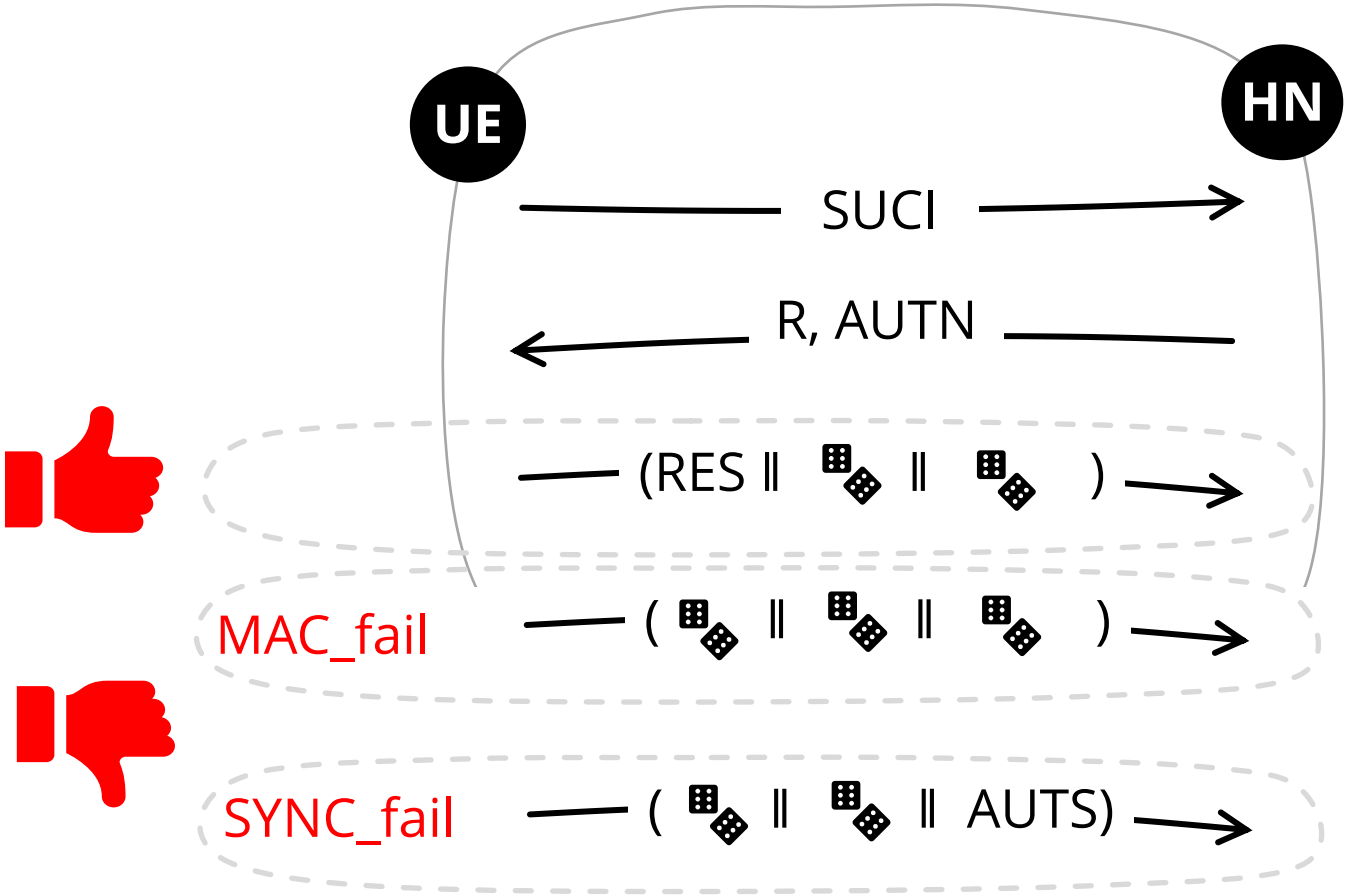
Построены атаки на большинство предлагаемых решений

Solution #2.3

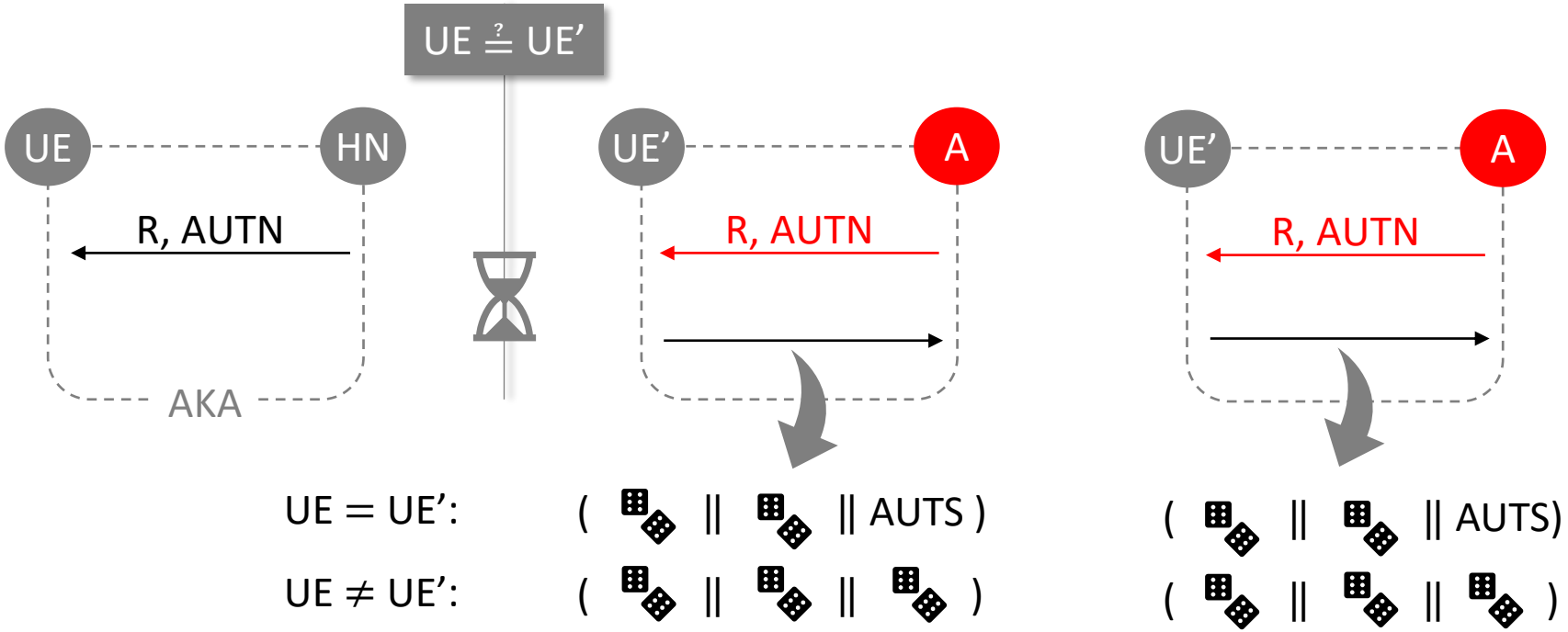


Идея: унифицируем ответ во всех 3 случаях (RES, CAUSE, AUTS)

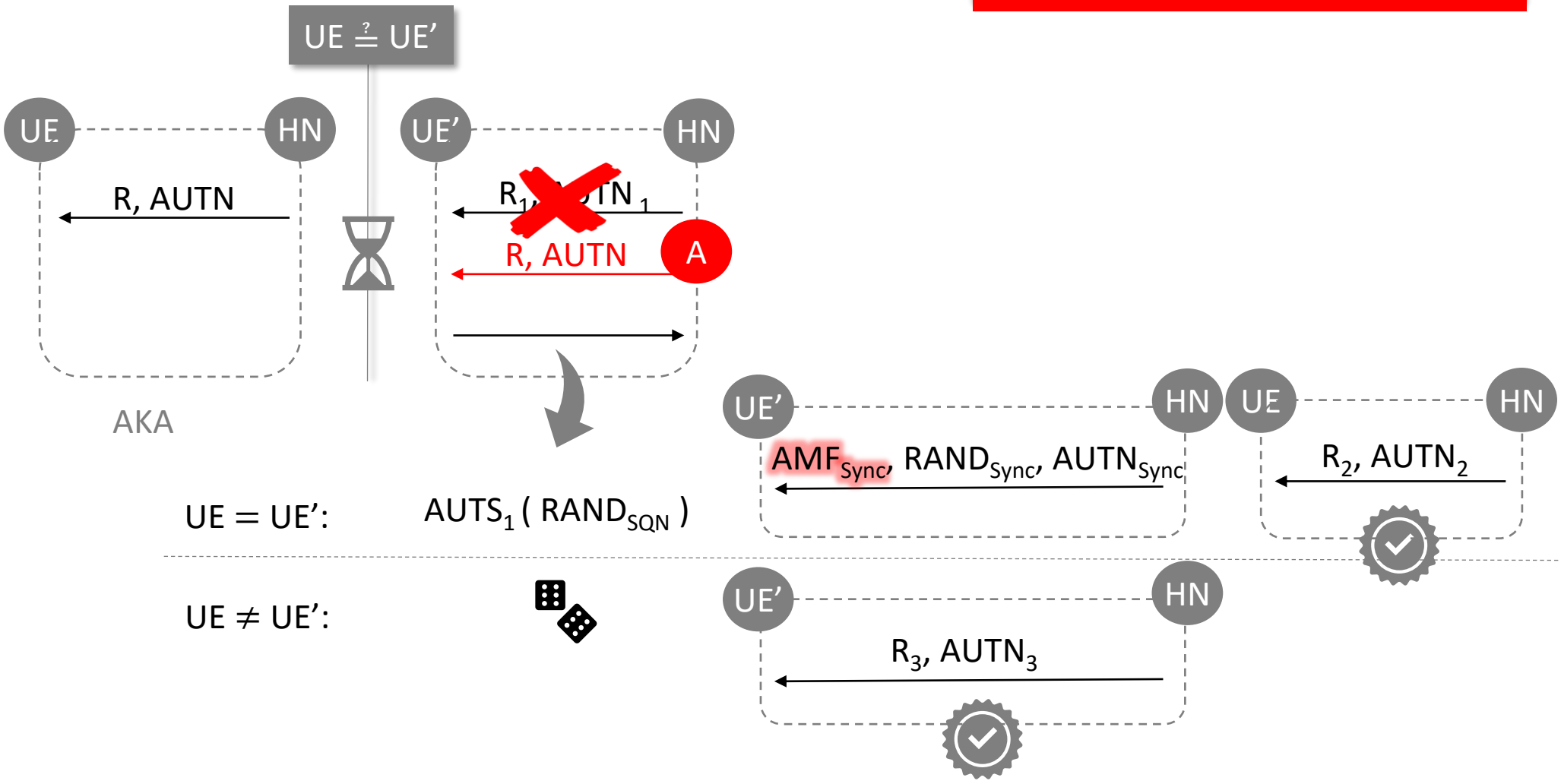
Solution #2.3



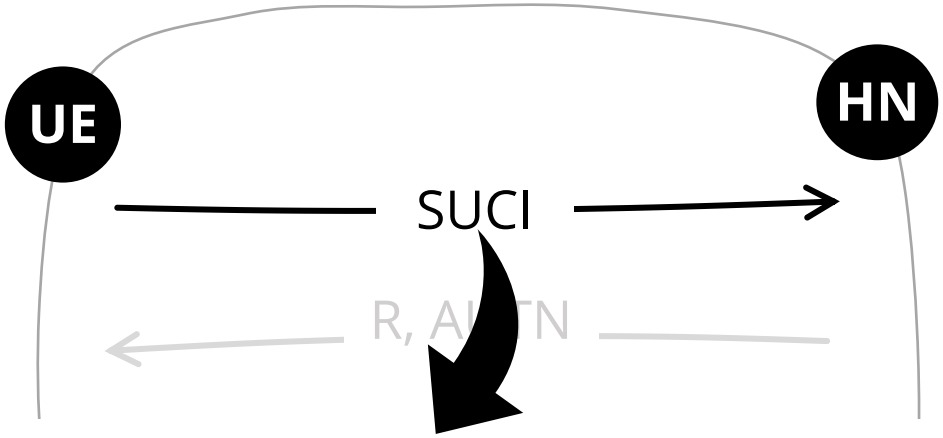
(RES, CAUSE, AUTS)


UE ≟ UE’
UE
HN
R, AUTN
AKA
UE’
A
R, AUTN
UE’
A
R, AUTN
UE = UE’:
(|| || AUTS)
UE ≠ UE’:
(|| ||)
(|| || AUTS)
(|| ||)

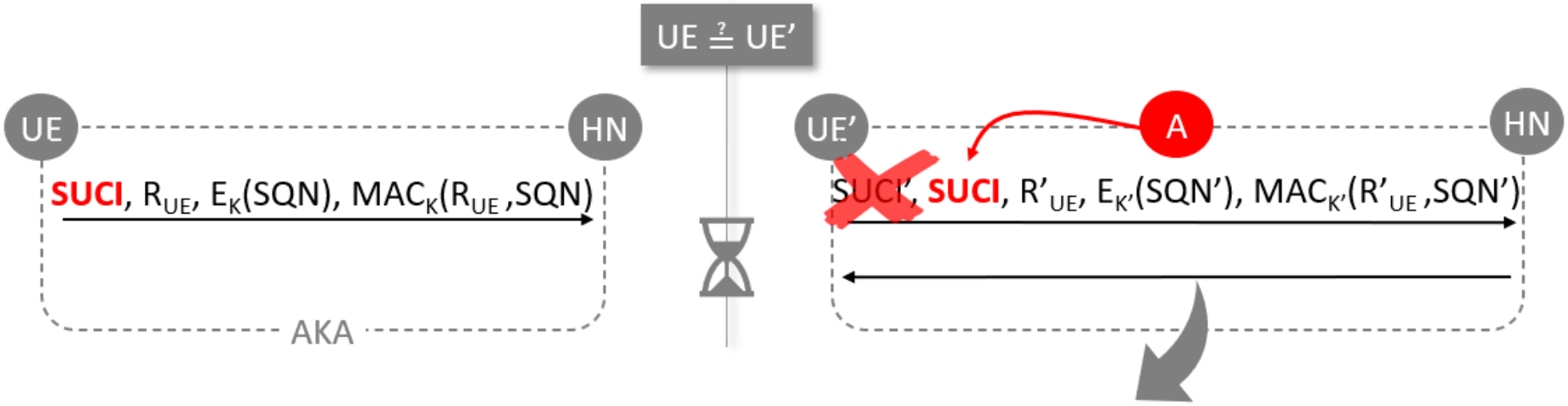
Solution #2.4


UE ≟ UE'
UE
HN
R, AUTN
AKA
UE'
HN
R, AUTN
A
UE = UE':
AUTS1 (RANDSQN)
UE'
HN
AMFSync, RANDSync, AUTNSync
UE
HN
R2, AUTN2
UE ≠ UE':
UE'
HN
R3, AUTN3

Solution #3.1

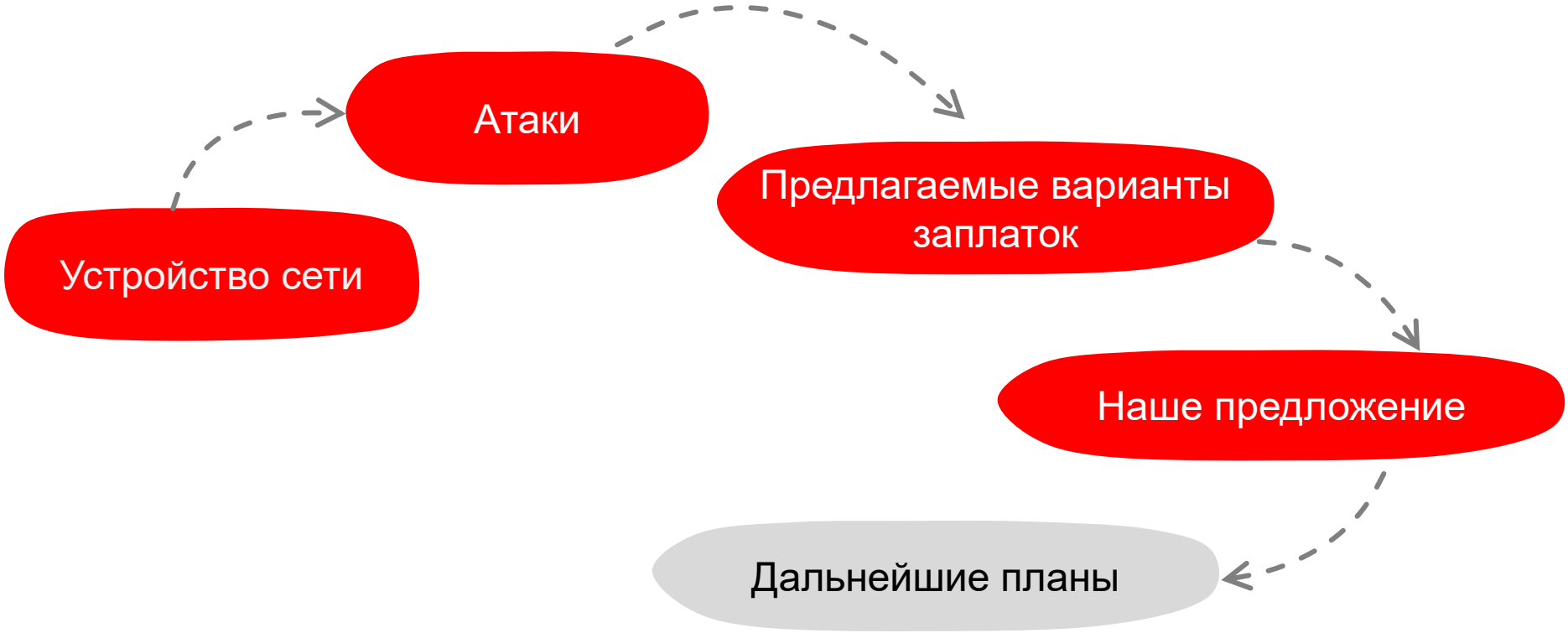


SUCI, $\mathbf{R_{UE}}$, E_K ($\mathbf{SQN_{UE}}$), MAC_K ($\mathbf{R_{UE}}$, $\mathbf{SQN_{UE}}$)

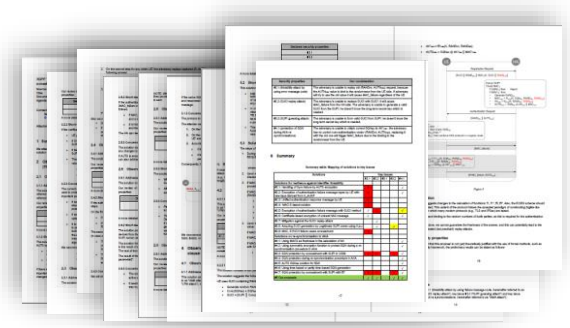


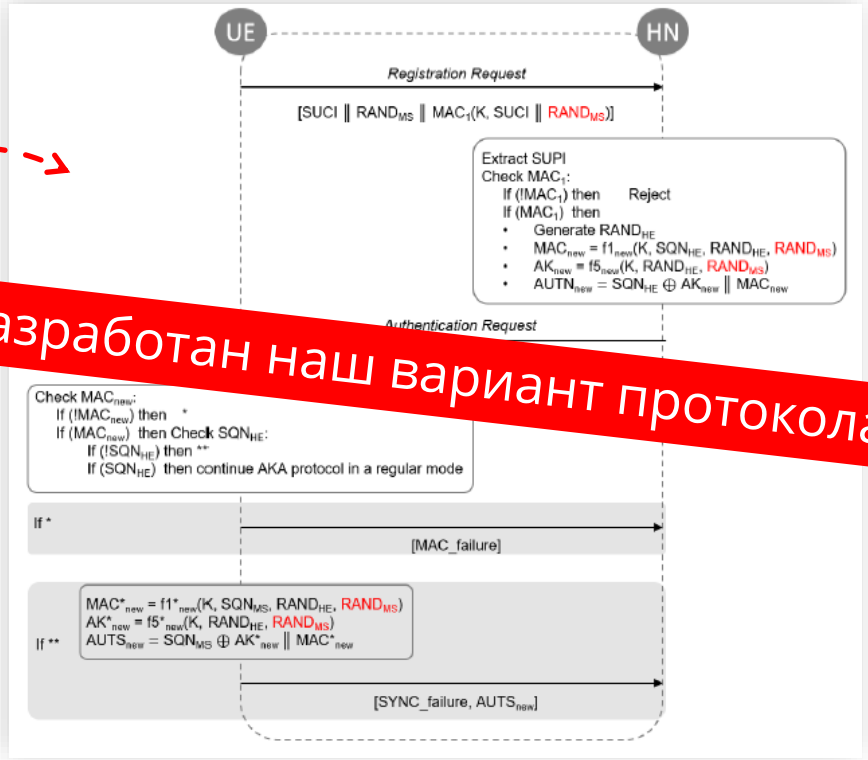
UE = UE': *Authentication Request*

UE ≠ UE': *Registration Reject*

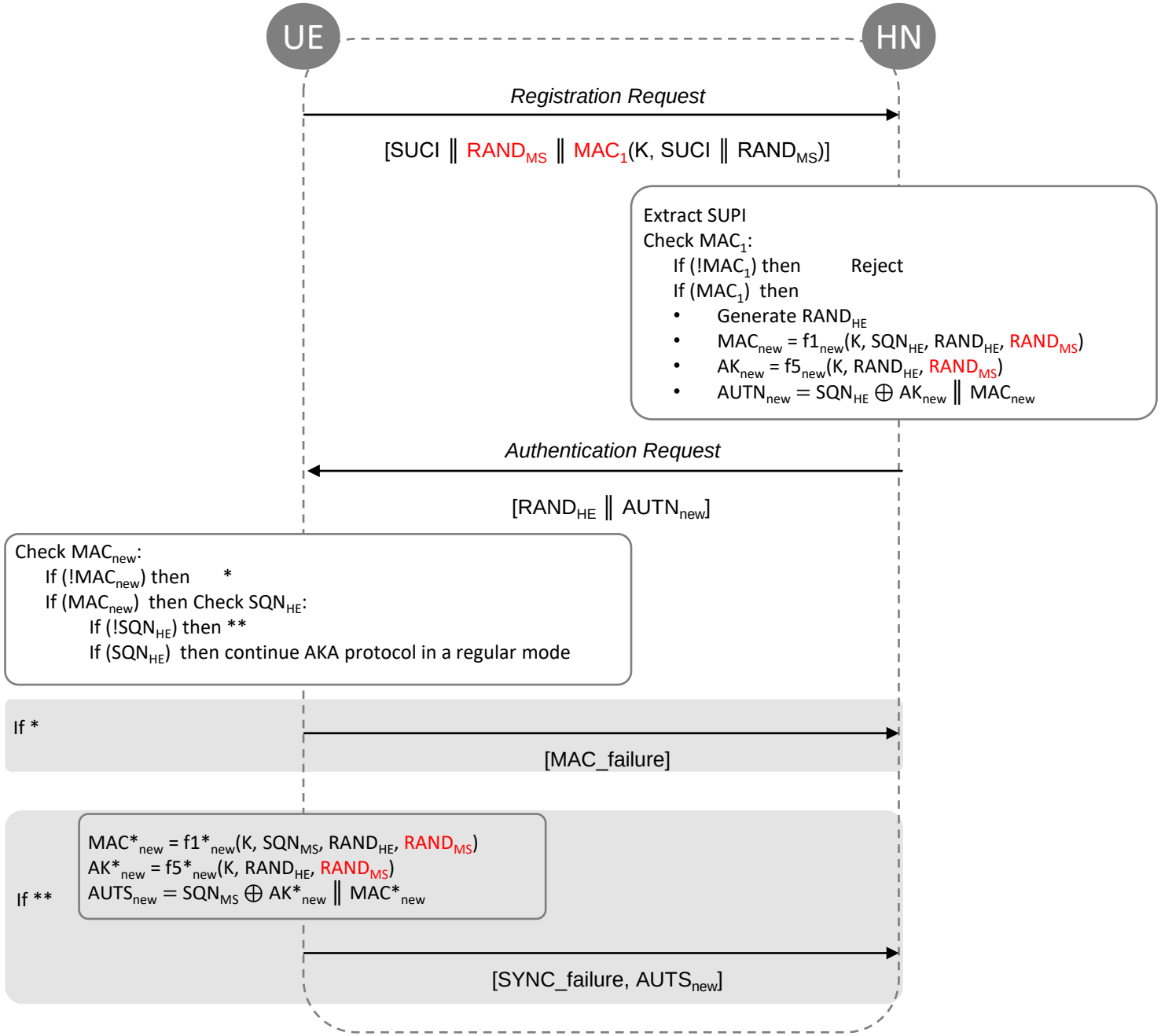

Атаки
Устройство сети
Предлагаемые варианты заплаток
Наше предложение
Дальнейшие планы

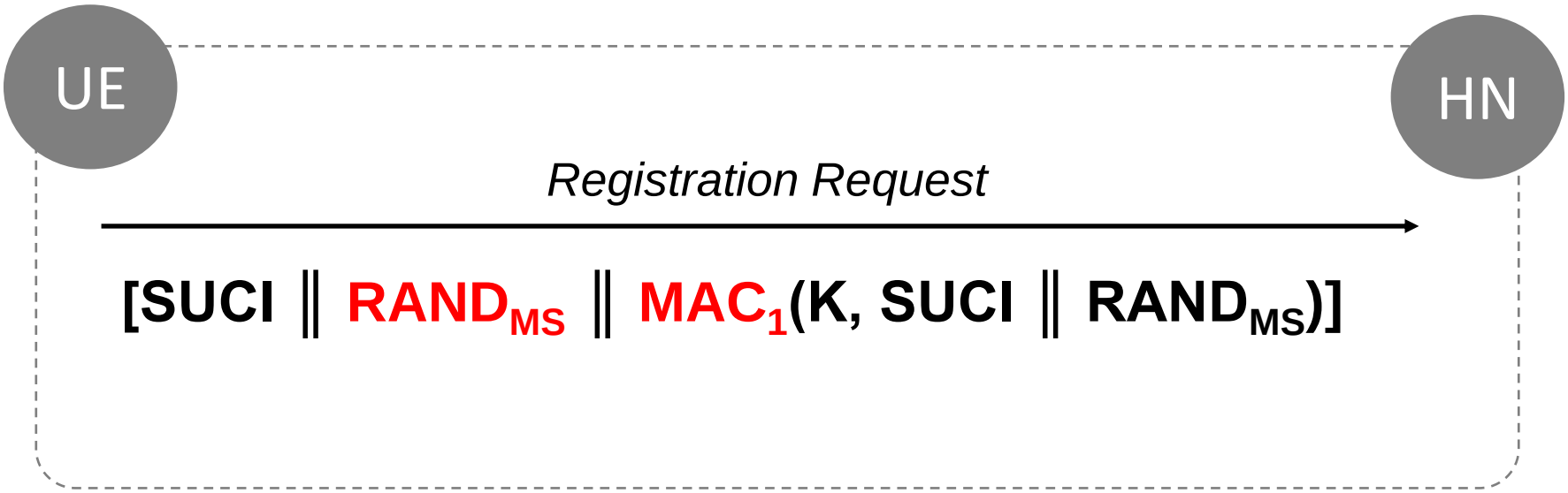
Подготовлен solution proposal к документу TR 33.846



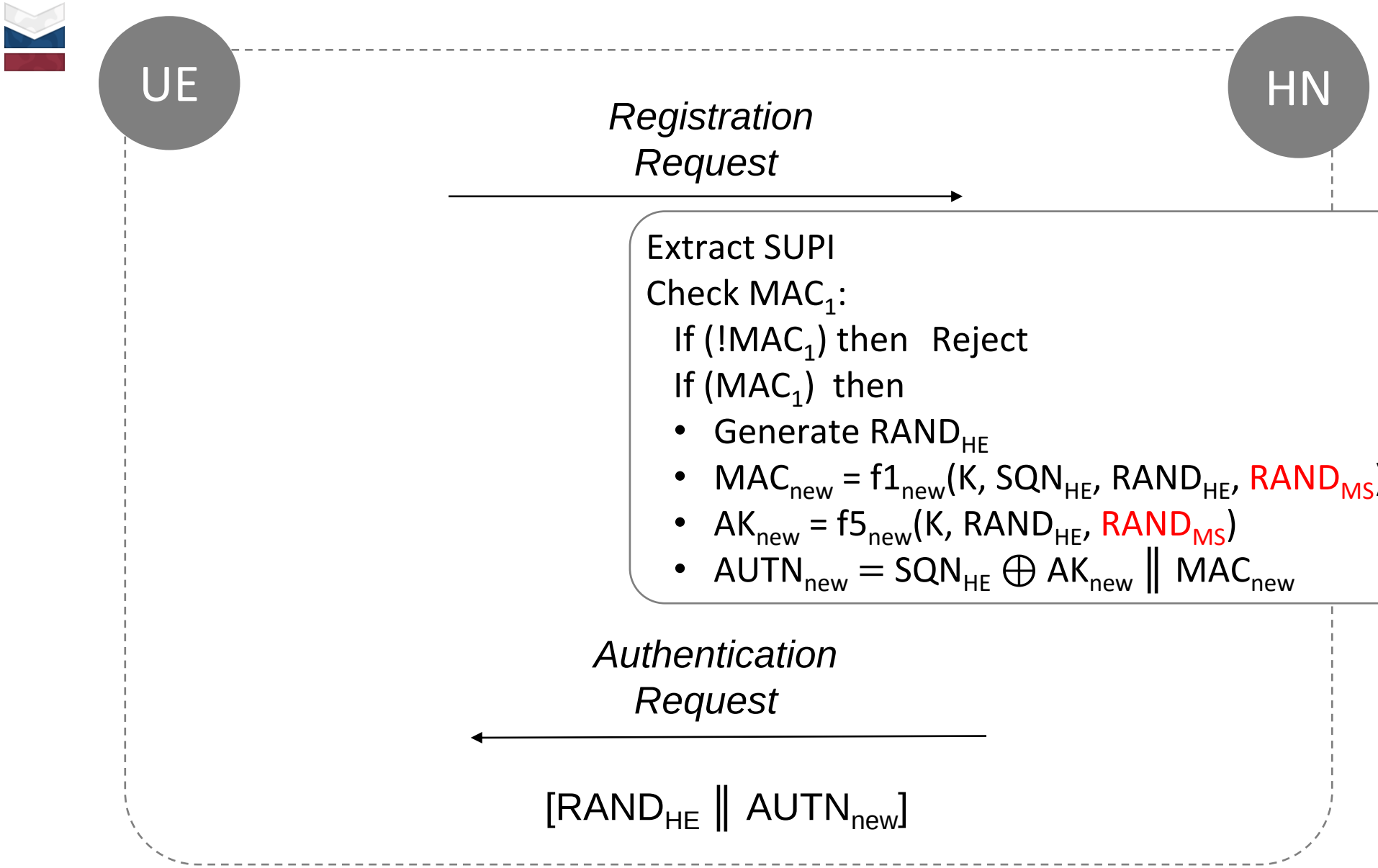


Разработан наш вариант протокола


UE
HN
Registration Request
[SUCI ‖ RAND_MS ‖ MAC_1(K, SUCI ‖ RAND_MS)]
Extract SUPI
Check MAC_1:
If (!MAC_1) then Reject
If (MAC_1) then
• Generate RAND_HE
• MAC_new = f1_new(K, SQN_HE, RAND_HE, RAND_MS)
• AK_new = f5_new(K, RAND_HE, RAND_MS)
• AUTN_new = SQN_HE ⊕ AK_new ‖ MAC_new
Authentication Request
[RAND_HE ‖ AUTN_new]
Check MAC_new:
If (!MAC_new) then *
If (MAC_new) then Check SQN_HE:
If (!SQN_HE) then **
If (SQN_HE) then continue AKA protocol in a regular mode
If *
[MAC_failure]
If **
MAC*_new = f1*_new(K, SQN_MS, RAND_HE, RAND_MS)
AK*_new = f5*_new(K, RAND_HE, RAND_MS)
AUTS_new = SQN_MS ⊕ AK*_new ‖ MAC*_new
[SYNC_failure, AUTS_new]



1. Добавляем случайность со стороны UE
2. Добавляем вычисление MAC на общем секретном ключе для защиты от атак, при которых противник генерирует SUCI самостоятельно
3. Запрос регистрации привязан к текущему сеансу посредством вычисления MAC от $RAND_{MS}$

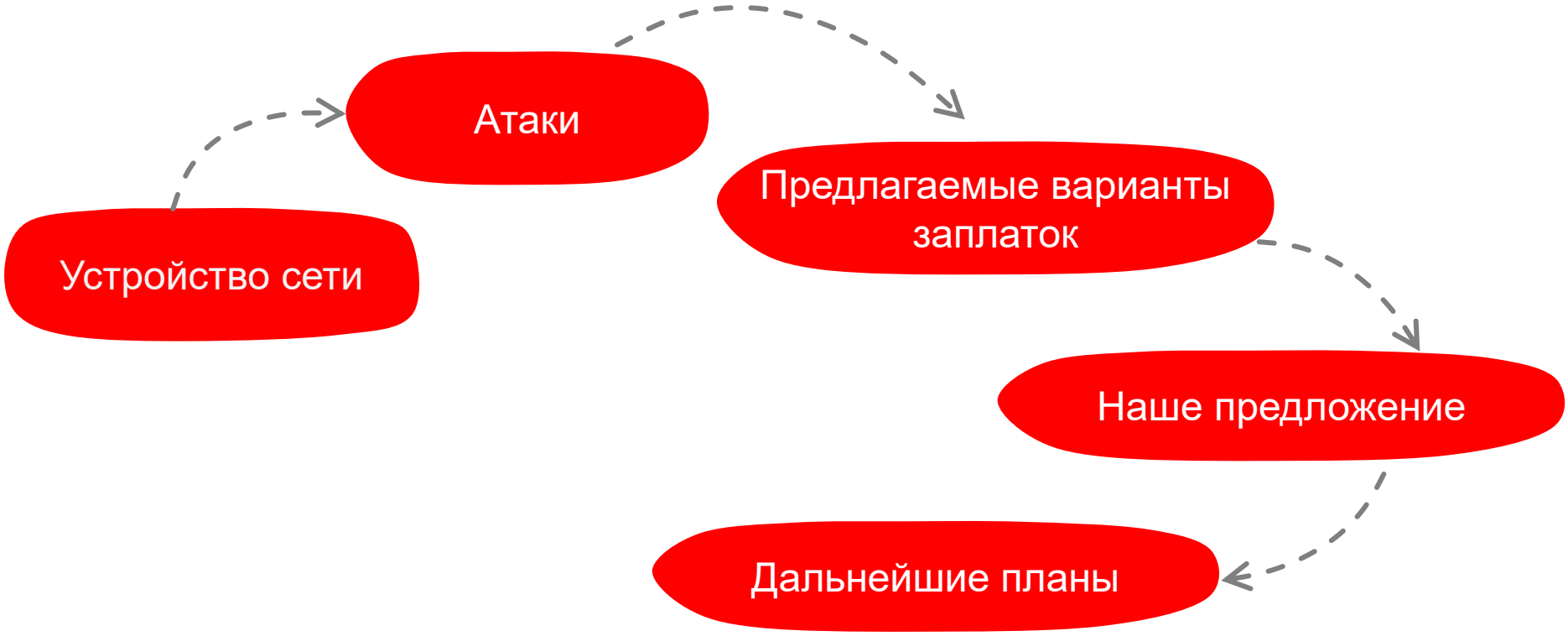


Привязка сообщений к случайности со стороны UE предотвращает возможность replay-атак

Наши предложения	Требуемое изменение	Аналоги в TR 33.846
Добавление случайности со стороны пользователя в функции сокрытия счетчика и контроля целостности	**Обновить алгоритм S3G**. Добавить в функции f1, f1*, f5, f5* новый параметр $RAND_{MS}$ – случайное число со стороны пользователя *(small changes)*	Solution #4.1 (TR 33.846 п. 6.4.1) – добавляют в функцию f5* новый параметр – MAC-S *(small changes)*
Контроль целостности отправляемого пользователем сообщения с зашифрованным идентификатором SUPI	**Обновить алгоритм S3G**. Добавить новую функцию f6, которая вычисляет MAC_1 на долгосрочном ключе K от выходных параметров схемы ECIES. MAC_1 = f6 (K, $RAND_{MS}$, SUCI) *(small changes)*	Solution #4.2 (TR 33.846 п. 6.4.2) – добавляют новую функцию f6, реализующую алгоритм симметричного шифрования *(major changes)*
Обеспечение пересылки случайного значения $RAND_{MS}$ и кода контроля целостности MAC_1 со стороны пользователя вместе с выходными данными схемы ECIES	**Добавить параметры в схему ECIES.** Добавить в пересылаемые параметры значения $RAND_{MS}$ и MAC_1 *(small changes)*	Solution #4.5 (TR 33.846 п. 6.4.5) – вместе с SUCI пересылают AUTS и $RAND_{MS.}$ *(small changes)* В пересылаемых параметрах схемы есть поле “any other parameters”, в которое можно добавить данные объемом до 3000 десятичных знаков (TR 33.846 п. 6.2.7.2)

Summary table: Mapping of solutions to key issues

Solutions	Key Issues				
	#2.1	#2.2	#3.1	#3.2	#4.1
Solutions for resilience against identifier linkability					
#2.1: Handling of Sync failure by AUTS encryption	x				✓
#2.2: Encryption of authentication failure message types by UE with new keys derived from K_AUSF	x				✓
#2.3: Unified authentication response message by UE	x				
#2.4: MAC-S based solution	x				
#2.5: Encryption of authentication failure message with SUCI method	✓	x			✓
#2.6: Certificate based encryption of unicast NAS message	✓				✓
#2.7: Mitigation against the SUCI replay attack		✓			
#2.8: Assuring SUCI generation by Legitimate SUPI owner using K_{SUCI}		✓		✓	
#2.9: MAC, SYNCH failure cause concealment	x				
#2.10: Solution to Key Issue #2.2: SUCI replay		✓ !			
#2.11: Mitigate the SUCI replay based on UE's public key		✓ !			
Solutions for availability aspects of SUCI usage					
#3.1: Mitigation of SUPI guessing and SUCI replay attack using long term key		x		✓	✓
#3.2: Adding Check Value behind SUPI to mitigate the SUPI guessing attacks				✓	
#3.3: Mitigation of SUPI guessing attack				✓	
Solutions on re-synchronisation in AKA					
#4.1: Using MACS as freshness in the calculation of AK					✓
#4.2: Using symmetric encryption function to protect SQN during a re-synchronisation procedure in AKA					✓
#4.3: SQN protection by concealment with SUPI in USIM	x	x		x	✓
#4.4: SQN protection during re-synchronisation procedure in AKA					✓
#4.5: AUTS SQN_{MS} solution for 5GS					✓
#4.6: Using time-based or partly time-based SQN generation					✓
#4.7: SQN protection by concealment with SUPI with f5*	x	x		x	✓
#5 Our proposals	✓	✓		✓	✓


Атаки
Предлагаемые варианты заплаток
Наше предложение
Дальнейшие планы
Устройство сети

Авторы доклада:

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