КРИПТОНИТ

Стандартизация российских криптографических механизмов в сетях связи 5G/IMT-2020: задачи, перспективы

Грибоедова Екатерина

Руководитель направления стандартизации,
Лаборатория криптографии

Дрынкин Антон

Руководитель направления практической криптографии,
Лаборатория криптографии

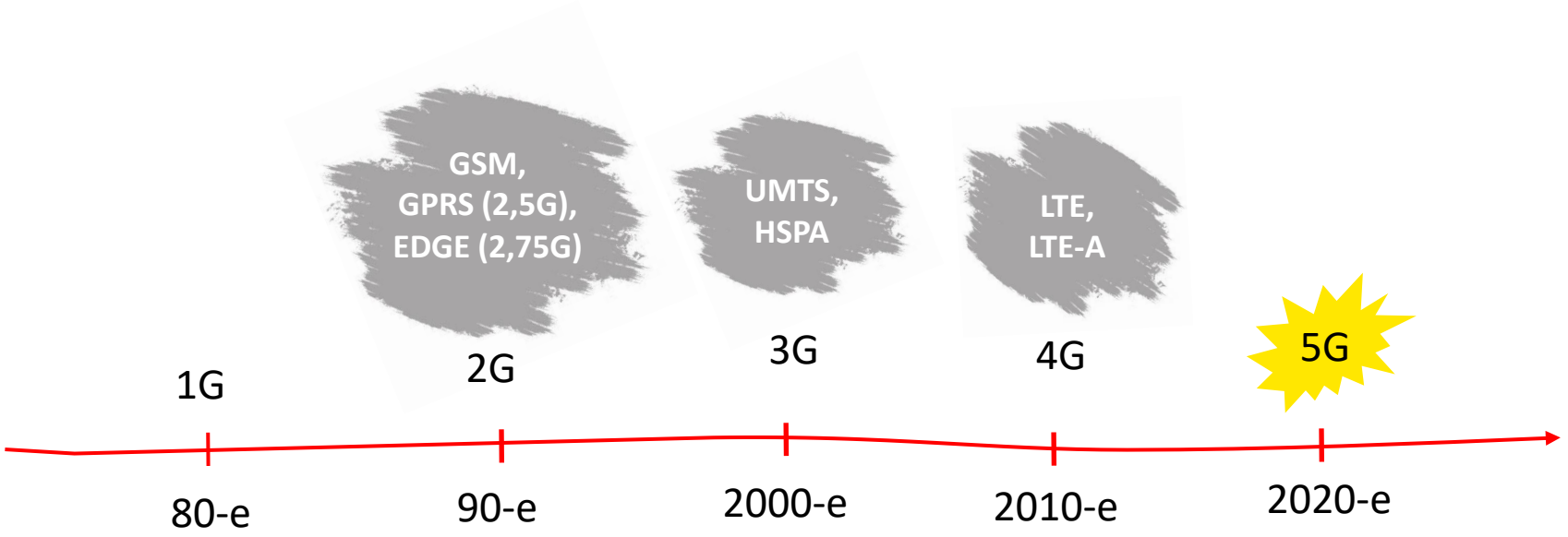
Цифровая экономика

В последние годы в России различные информационные системы активно переводятся на использование отечественных криптографических алгоритмов и протоколов с целью обеспечения их технологической независимости.

В ноябре 2020 года в рамках заседания Президиума Правительственной комиссии по цифровому развитию была утверждена **дорожная карта развития мобильных сетей 5G**.

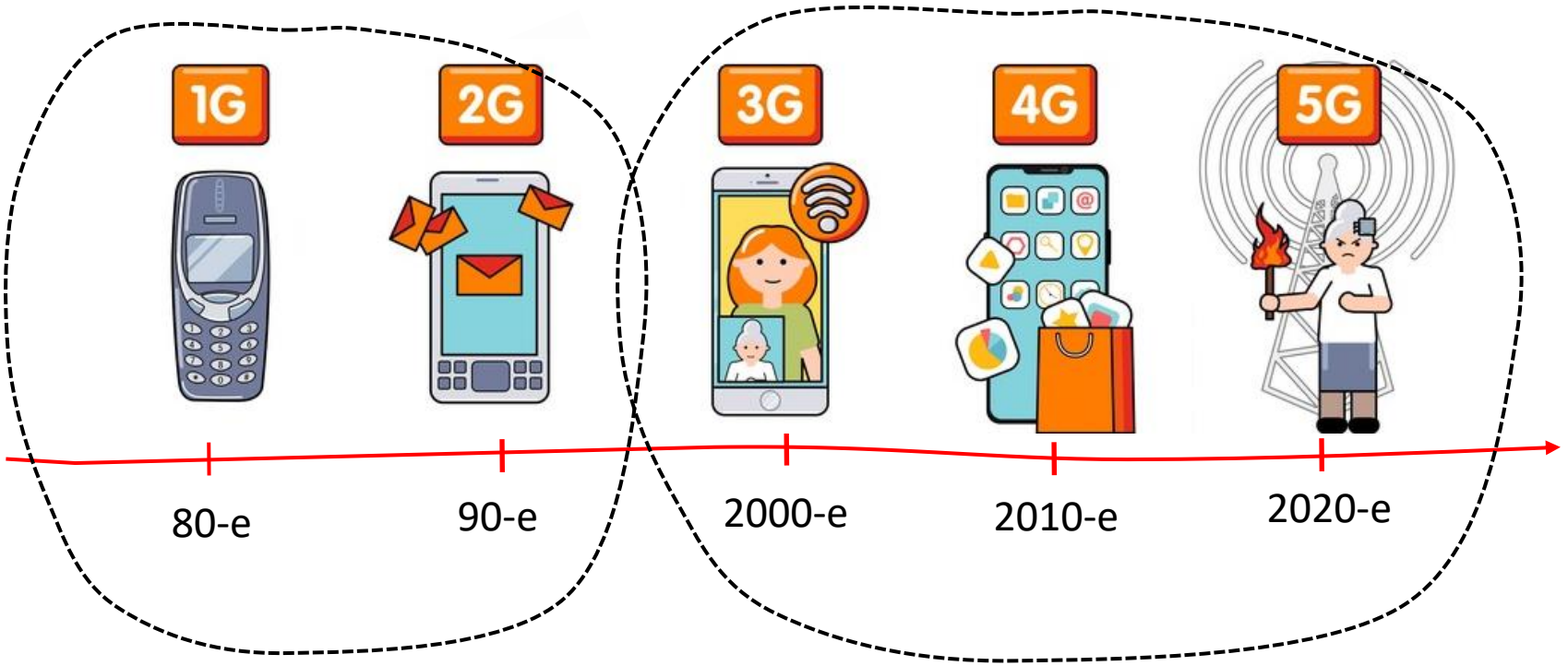
Целью данного проекта является ускорение развертывания телекоммуникационной сети нового поколения на базе отечественного оборудования и алгоритмов.

Поколения сотовой связи



Ключевое отличие 5G — новая сетевая архитектура, где реализация всех основных функций телекоммуникационного оборудования происходит на программном уровне и не требует специализированных аппаратных решений.

Поколения сотовой связи



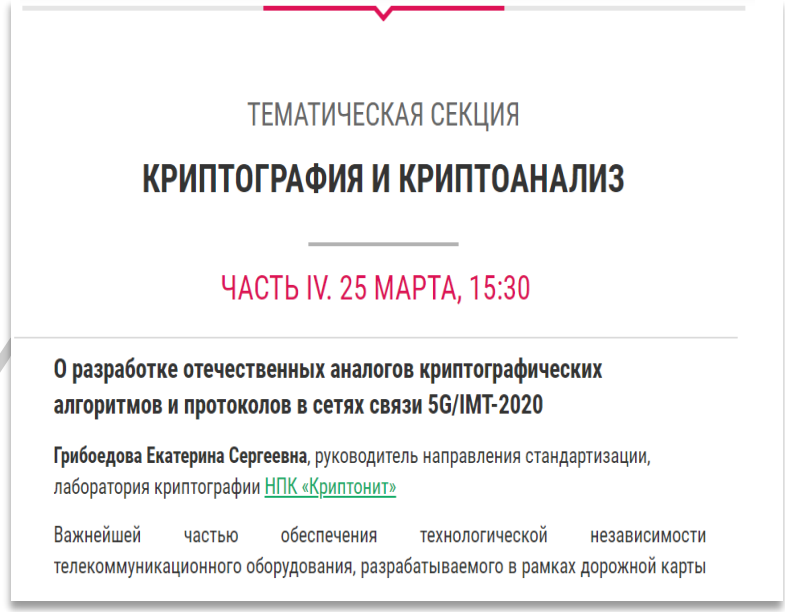
Локальные стандартизирующие организации

3GPP

5G устройство сети

5G 3GPP

5G Росстандарт



ТЕМАТИЧЕСКАЯ СЕКЦИЯ

КРИПТОГРАФИЯ И КРИПТОАНАЛИЗ

ЧАСТЬ IV. 25 МАРТА, 15:30

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

Грибоедова Екатерина Сергеевна, руководитель направления стандартизации, лаборатория криптографии НПК «Криптонит»

Важнейшей частью обеспечения технологической независимости телекоммуникационного оборудования, разрабатываемого в рамках дорожной карты

Структура 3GPP

Структура 3GPP

«THIRD GENERATION PARTNERSHIP PROJECT»

Консорциум, разрабатывающий спецификации для мобильной телефонии. Ассоциация не имеет юридического лица, но является совместной деятельностью следующих стандартизирующих организаций, называемых «**Организациями партнерами**»:

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

Структура 3GPP

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

- НПК “Криптонит”
- Nexign
- Intel Russia

КРИПТОНИТ nexign intel

Структура 3GPP

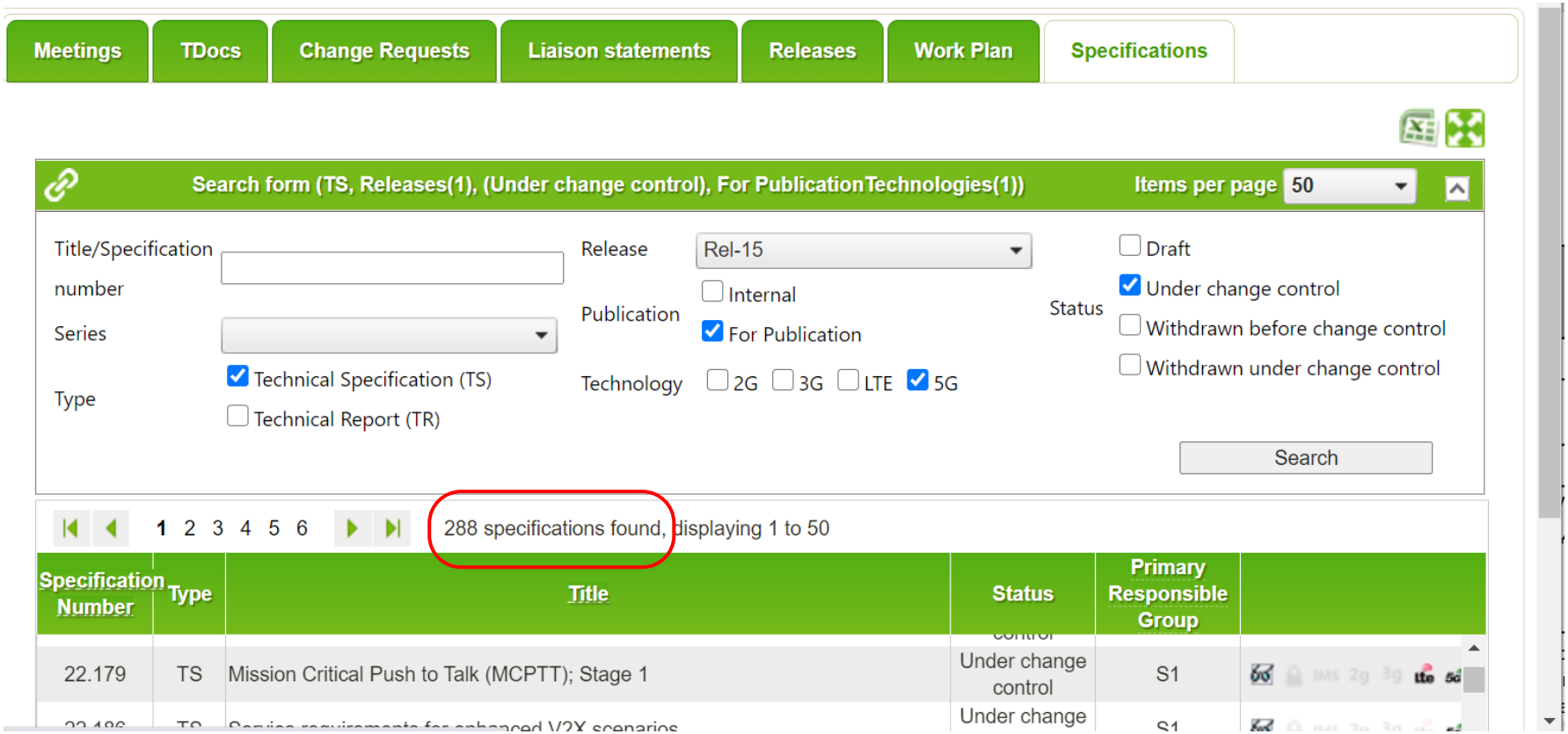
Задачей 3GPP является разработка технических спецификаций, в то время как присвоение им статуса рекомендаций или стандартов является задачей «организаций партеров».

Структура 3GPP

Стандарты 3GPP структурированы **релизами**

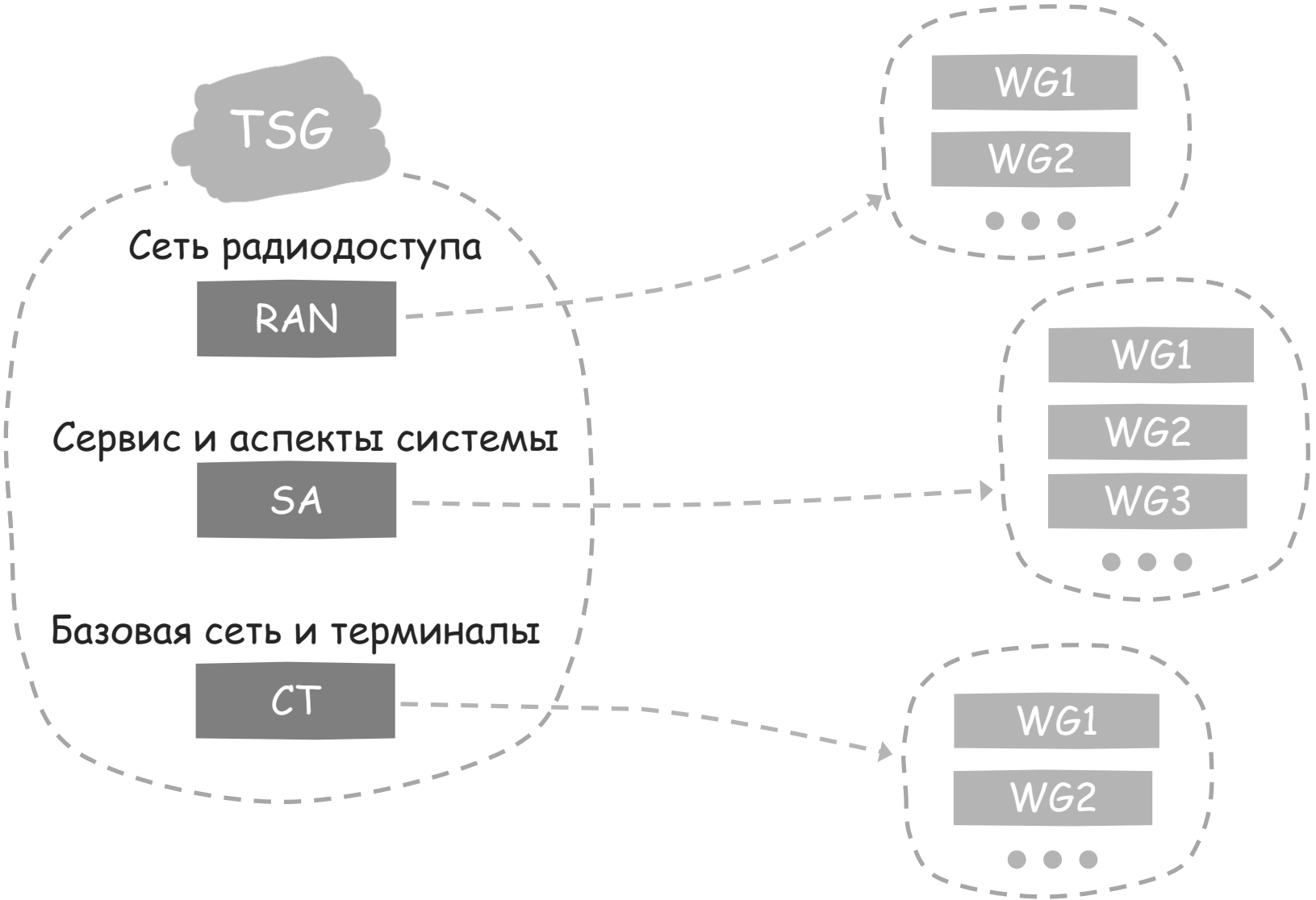
Структура 3GPP

Все документы 3GPP находятся в открытом доступе на ресурсе: https://portal.3gpp.org/



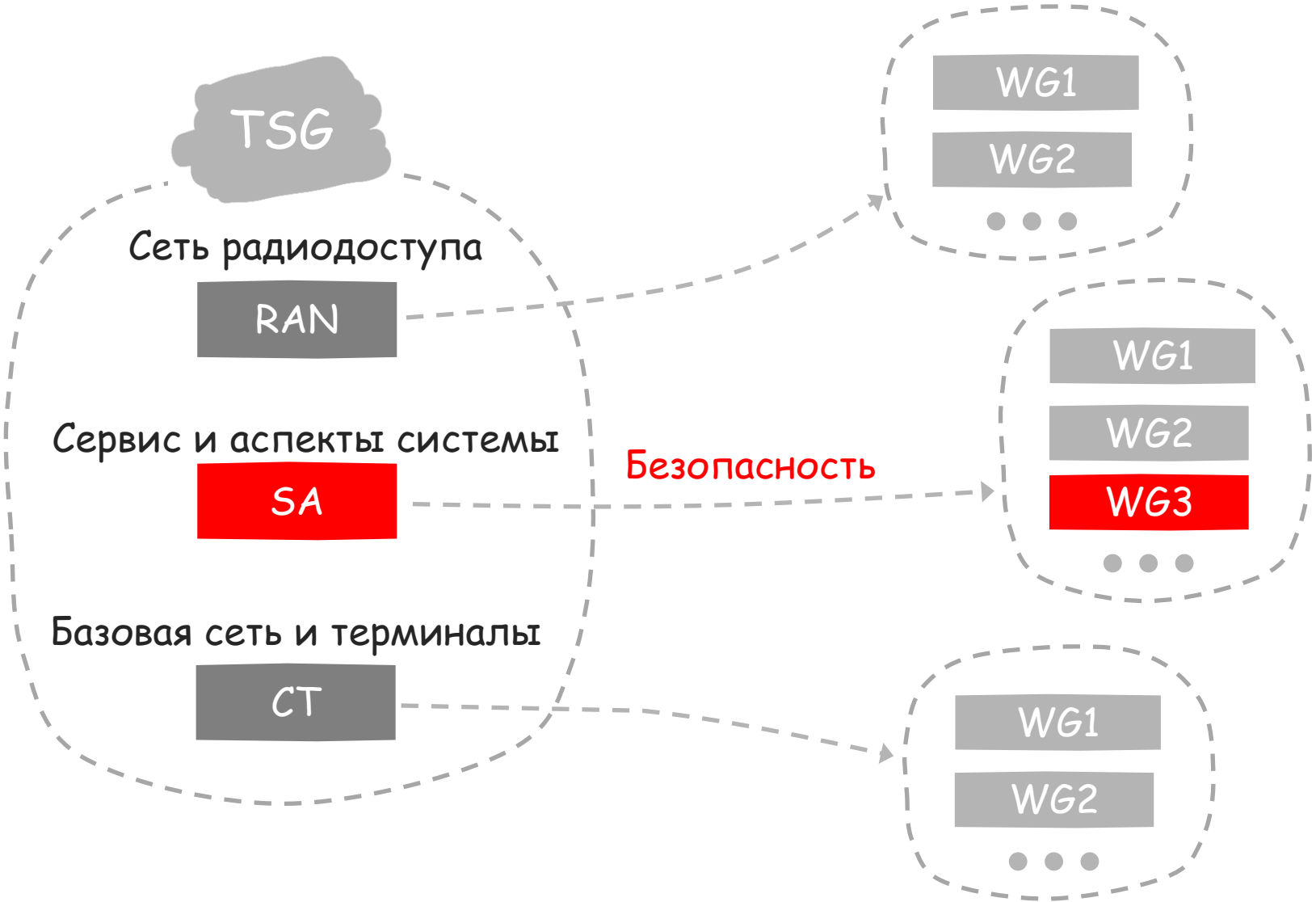
Структура 3GPP

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



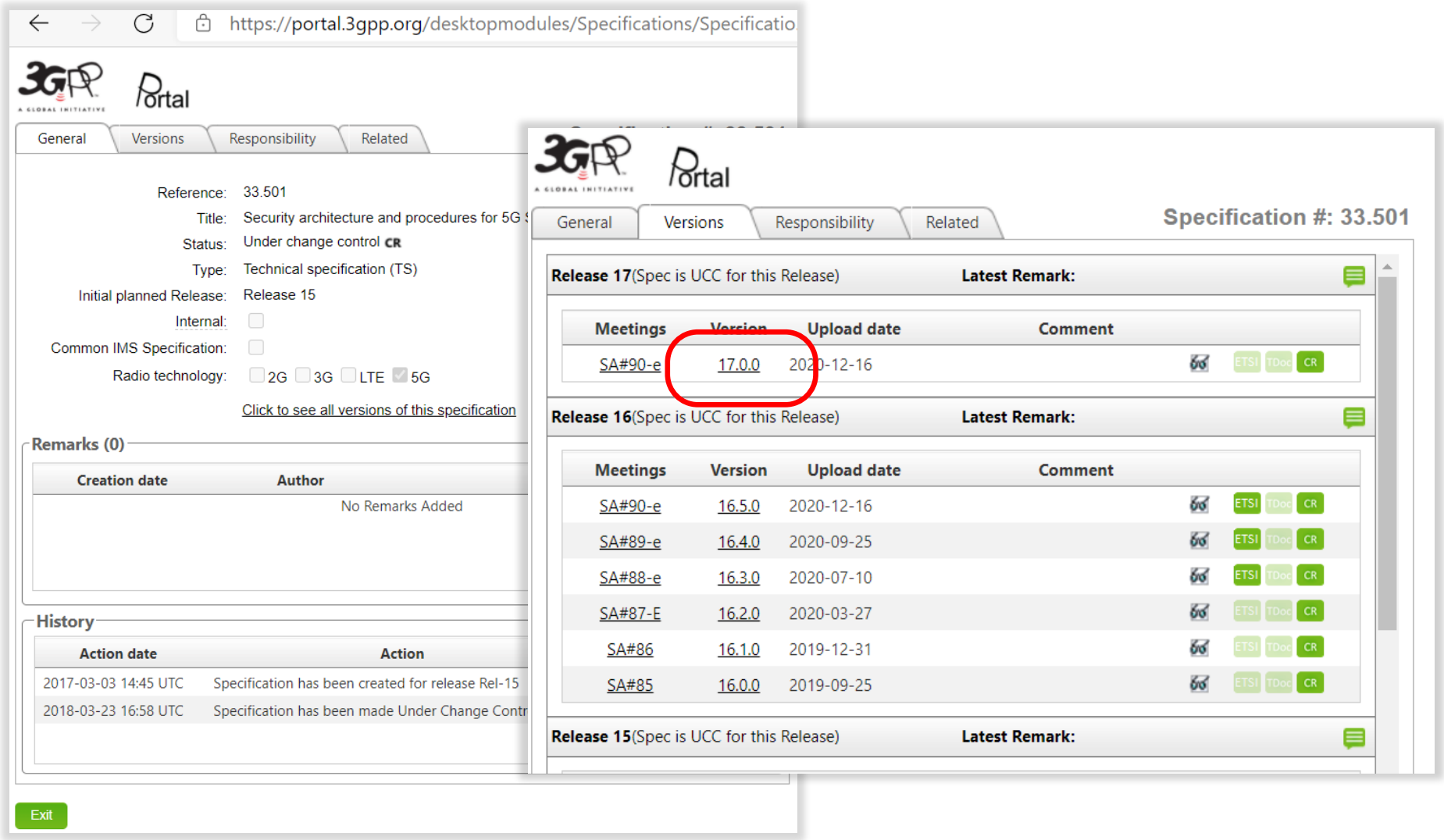
Структура 3GPP

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




3GPP
TS 33.501

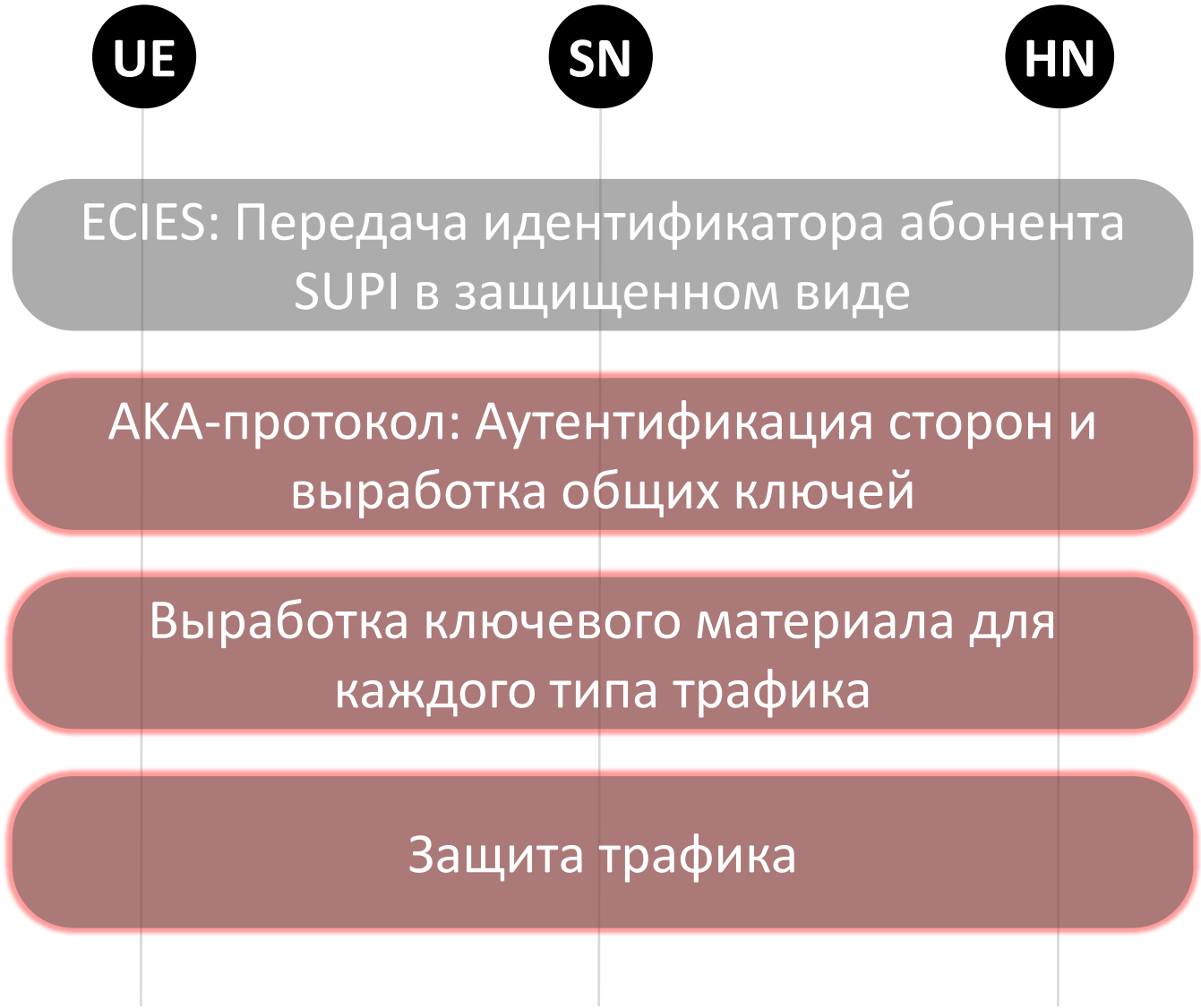
TS 33.501:


https://portal.3gpp.org/desktopmodules/Specifications/Specificatio
Portal
General
Versions
Responsibility
Related
Reference: 33.501
Title: Security architecture and procedures for 5G
Status: Under change control CR
Type: Technical specification (TS)
Initial planned Release: Release 15
Internal:
Common IMS Specification:
Radio technology: 2G 3G LTE 5G
Click to see all versions of this specification
Remarks (0)
Creation date
Author
No Remarks Added
History
Action date
Action
2017-03-03 14:45 UTC
Specification has been created for release Rel-15
2018-03-23 16:58 UTC
Specification has been made Under Change Contr
Exit
Portal
General
Versions
Responsibility
Related
Specification #: 33.501
Release 17(Spec is UCC for this Release)
Latest Remark:
Meetings
Version
Upload date
Comment
SA#90-e
17.0.0
2020-12-16
Release 16(Spec is UCC for this Release)
Latest Remark:
Meetings
Version
Upload date
Comment
SA#90-e
16.5.0
2020-12-16
SA#89-e
16.4.0
2020-09-25
SA#88-e
16.3.0
2020-07-10
SA#87-E
16.2.0
2020-03-27
SA#86
16.1.0
2019-12-31
SA#85
16.0.0
2019-09-25
Release 15(Spec is UCC for this Release)
Latest Remark:

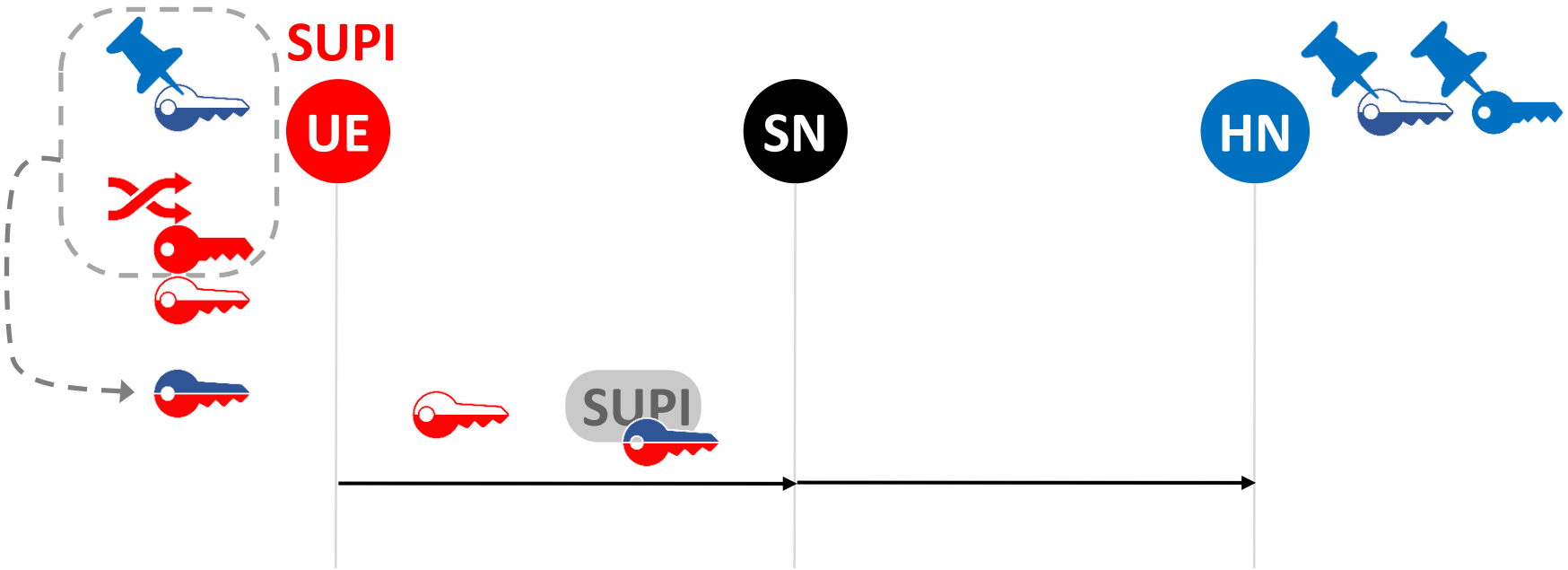
Внедрение отечественной криптографии

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

Внедрение отечественной криптографии



Внедрение отечественной криптографии



✓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.

3GPP

Подготовлен Draft CR
change_to_TS_33501_new_ECIES_profile

- ✓ Эллиптическая кривая: id-tc26-gost-3410-2012-256-paramSetA
- ✓ KDF: PRF_IPSEC_PRFPLUS_GOSTR3411_2012_256
- ✓ Хэш-функция: GOST R 34.11-2012, 256-bit output
- ✓ Алгоритм вычисления имитовставки: «Кузнечик» в режиме CMAC
- ✓ Алгоритм шифрования: «Кузнечик» в режиме CTR

Росстандарт

Оформляется аналогичный проект рекомендаций по стандартизации

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

3GPP

Подготовлен Draft TS *draft_TS_S3G*

- ✓ Описывает набор функций f1,…,f5* на базе российской хэш функции ГОСТ Р 34.11-2012

Росстандарт

Полностью аналогичный документ на русском языке **уже стандартизован:**

- ✓ рекомендации по стандартизации Р 1323565.1.003-2017, описывающие набор функций S3G

Запланирован перевыпуск данного стандарта (ошибки в контрольных примерах, изменение длины одного из параметров)

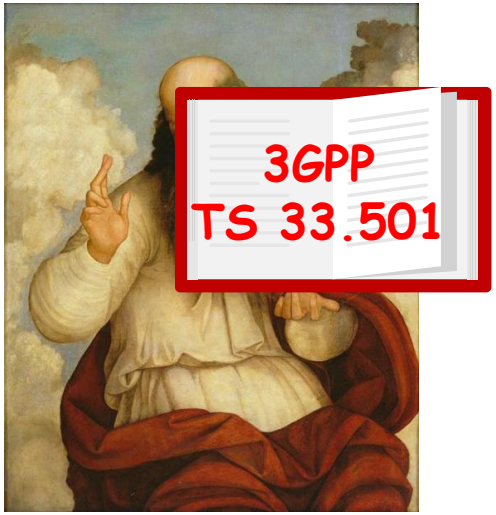
Огромный ряд проблем и вопросов в отношении функционирования всего остального протокола 5G-AKA (EAP-AKA’)

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

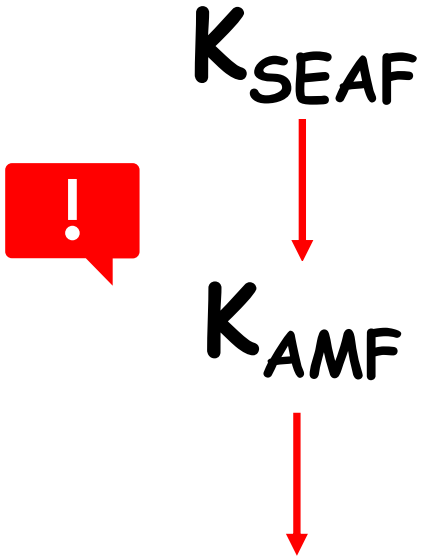
- ☺ Избавлен от ряда лишних вычислений
- ☹ Не предусматривает опциональности в выборе криптографических примитивов
- ☹ Описан в TS 3GPP

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


UE
SN
HN
ECIES: Передача идентификатора абонента SUPI в защищенном виде
AKA-протокол: Аутентификация сторон и выработка общих ключей
K_{SEAF}
Выработка ключевого материала для каждого типа трафика
Защита трафика
3

3GPP KDF с фиксированным SHA-256



В результате данного этапа для каждого типа трафика вырабатывается своя пара ключей

K_{ENC}, K_{MAC}

3GPP	Росстандарт
?	?

Необходимо добиваться опциональности в 3GPP

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

3GPP

Подготовлен Draft TS
Confidentiality and integrity Algorithms “NEA7” & “NIA7”

- ✓ Алгоритм вычисления имитовставки: «Кузнечик» в режиме CMAC
- ✓ Алгоритм шифрования: «Кузнечик» в режиме CTR

Росстандарт

Оформляется аналогичный проект рекомендаций по стандартизации

Есть ряд криптографических проблем, не связанных со спецификой работы конкретного блочного шифра

Выводы

Проблемы:

- ✓ Зашитые зарубежные алгоритмы
- ✓ Устаревшие принципы построения криптографических протоколов, наличие большого числа уязвимостей
- ✓ Огромный объём документации, как следствие сложность проведения независимого аудита безопасности за приемлемое время.

Планы на 2021 год:

- ✓ Налаживание активного участия в работах 3GPP
- ✓ Инициирование рассмотрения подготовленных драфтов документов
- ✓ Выполнение работ в рамках дорожной карты по 5G
- ✓ Разработка проектов рекомендаций по стандартизации

Вопросы:

- ✓ Организация рабочей группы для разработки проектов документов в ТК 26

В работе над докладом принимали участие

Грибоедова Екатерина

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

Дрынкин Антон

Руководитель направления практической криптографии,
Лаборатория криптографии
a.drynkin@kryptonite.ru

Давыдов Степан

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