ГРУППА КОМПАНИЙ СПБ

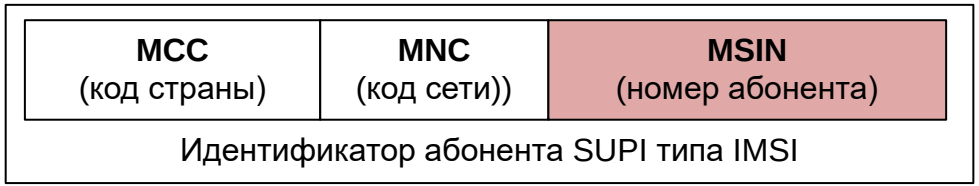
РусКрипто XXVIII

НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

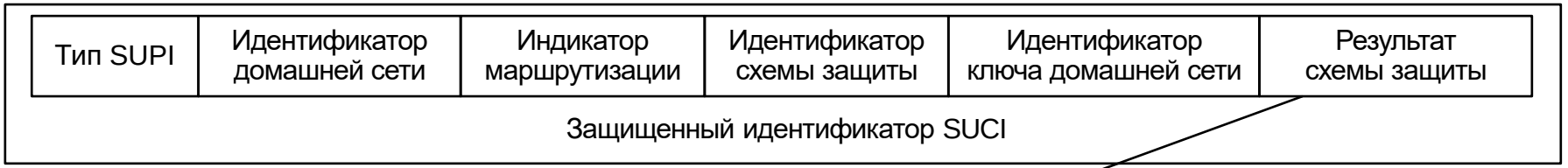
ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ АППАРАТНОГО МОДУЛЯ БЕЗОПАСНОСТИ HSM, ВЫПОЛНЯЮЩЕГО КРИПТОГРАФИЧЕСКИЕ ФУНКЦИИ АУТЕНТИФИКАЦИИ И ИДЕНТИФИКАЦИИ АБОНЕНТОВ, С ОБОРУДОВАНИЕМ ЯДРА СЕТИ ПРТС ПЯТОГО ПОКОЛЕНИЯ

Емельянов-Гирс В.М., Герасимова А.Г., Третникова Е.Н., Устюгов А.А., Андреев А.З.

ЗАЩИТА ПОСТОЯННОГО ИДЕНТИФИКАТОРА АБОНЕНТА



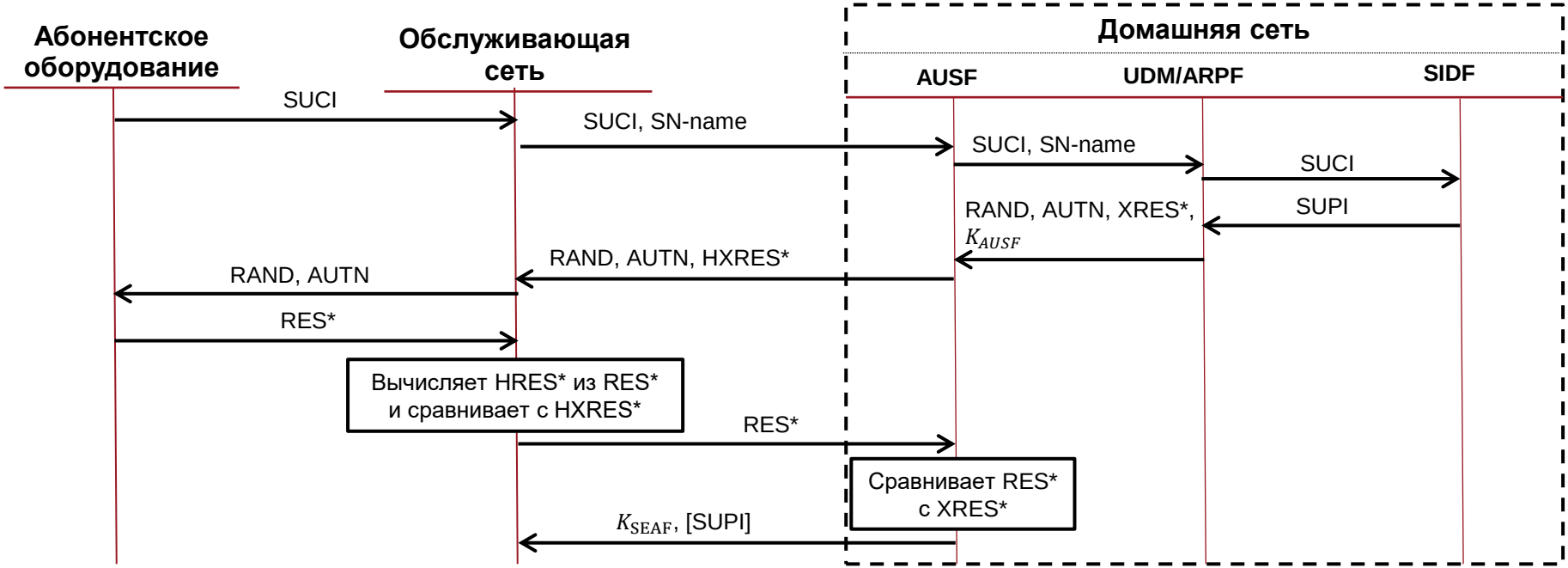
Для защиты идентификатора используется схема гибридного шифрования ECIES*, в результате выполнения которой на стороне абонента формируется поле «Результат схемы защиты», которое становится частью идентификатора SUCI:



Состоит из:
- Q_{eph} – точка ЭК;
- C – зашифрованный **MSIN**;
- T – имитовставка для шифртекста.

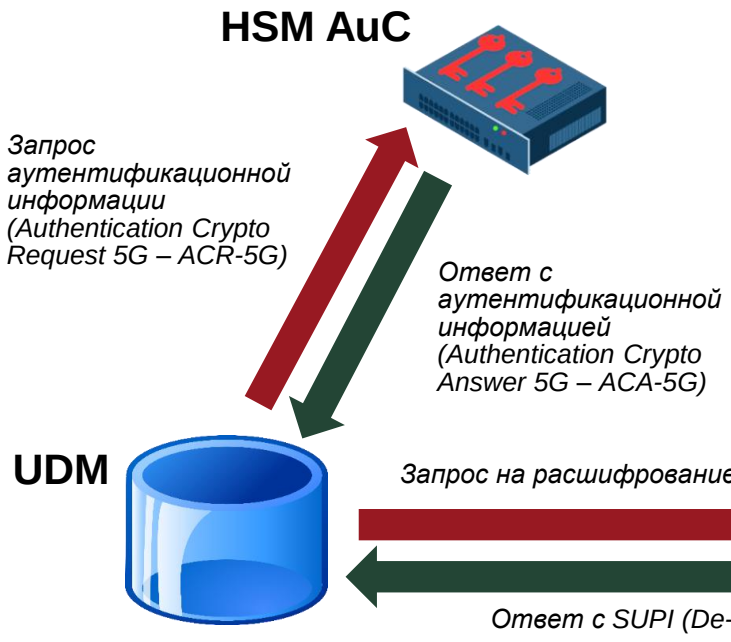
* Проект методической рекомендации ТК 26 «Использование российских криптографических алгоритмов в схеме защиты постоянного идентификатора абонента сетей подвижной радиотелефонной связи (ECIES)»

ПОТОК ДАННЫХ В ПРОЦЕДУРЕ АУТЕНТИФИКАЦИИ 5G-AKA-GOST*



* Проект методической рекомендации ТК 26 «Протокол аутентифицированной выработки общего ключа в сетях подвижной радиотелефонной связи»

ИСПОЛЬЗОВАНИЕ HSM ПРИ АУТЕНТИФИКАЦИИ



Опубликован проект приказа Минцифры России «Об утверждении Требований к применению оборудования коммутации стандарта 5G/IMT-2020, используемого при оказании услуг передачи данных и телефонного соединения»*, который определяет необходимость использования двух СКЗИ:

- аппаратный модуль безопасности SIDF (HSM-SIDF) для расшифрования SUPI из SUCI;
- аппаратный модуль безопасности центра аутентификации (HSM AuC) для хранения ключей аутентификации и выработки аутентификационных векторов.

* https://regulation.gov.ru/projects/162149/

ЗАПРОС НА ПОЛУЧЕНИЕ ПОСТОЯННОГО ИДЕНТИФИКАТОРА SUPI

Запрос на получение идентификатора SUPI к HSM-SIDF (DCR):

Поле	Содержание
Code	Код сообщения UDM. Длина: 48 битов.
SUCI	Закрытый идентификатор подписки SUCI. Длина: 53 байта.

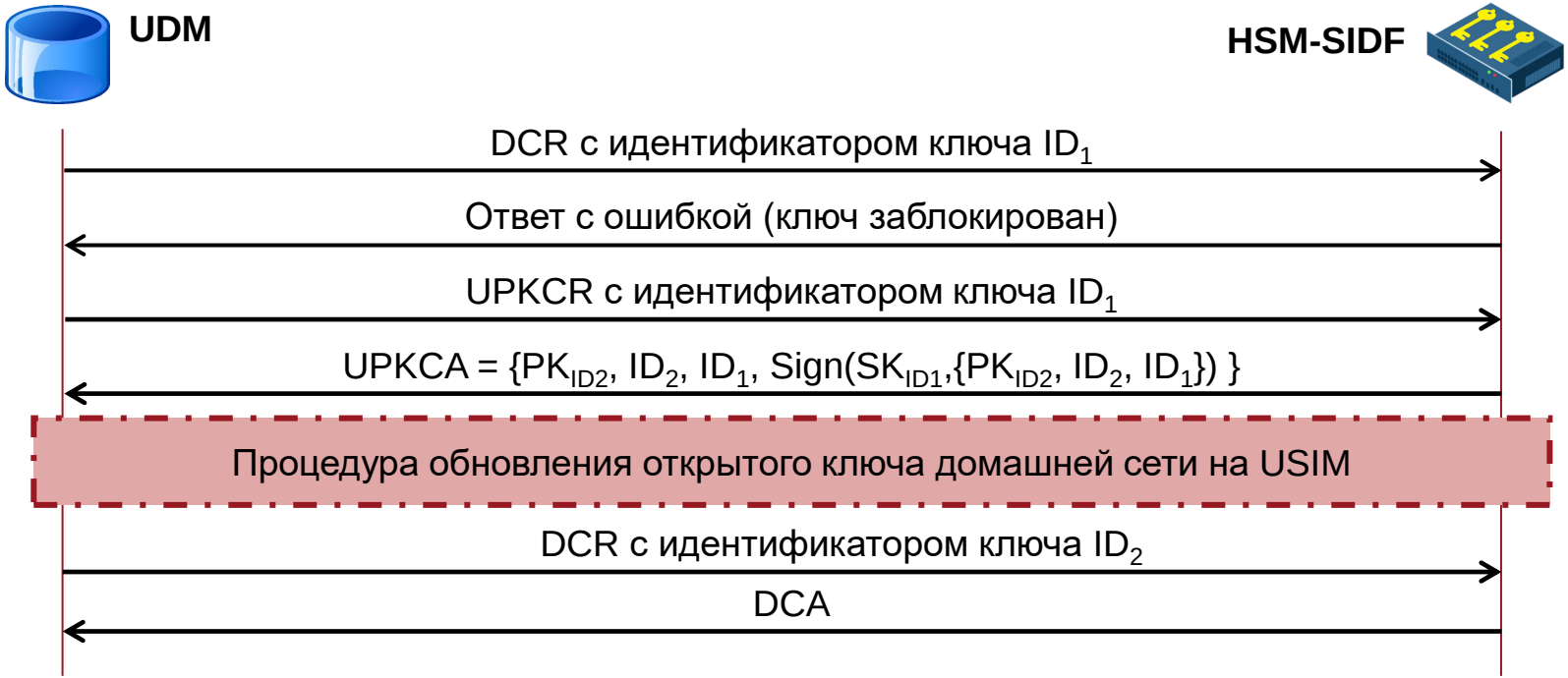
Повышение производительности HSM-SIDF возможно за счет:

- Использования ЭК с идентификатором **id-tc26 - gost-3410-2012-256-paramSetA в скрученной форме Эдвардса;**
- **Отказа от сокращенной передачи** эфемерной точки Q_{eph}, что увеличит размер SUCI, но ускорит обработку, поскольку не нужно будет восстанавливать y-координату

Ответ на запрос (DCA):

Поле	Содержание
Code	Код сообщения HSM-SIDF. Длина: 48 бит.
SUPI	Постоянный идентификатор абонента SUPI. Длина: 5 байт.
$RAND_{UE}$	Случайное значение из схемы защиты SUCI. Длина: 264 бит.
Q_{eph}	Точка ЭК из схемы защиты SUCI. Длина: 512 бит.
FUPK	Указатель обновления публичного ключа домашней сети. Длина: 8 бит.

ЗАПРОС НА ОБНОВЛЕНИЕ ОТКРЫТОГО КЛЮЧА ДОМАШНЕЙ СЕТИ (UPKCR)



ВАРИАНТЫ ВВОДА КЛЮЧЕВОЙ ИНФОРМАЦИИ В HSM

HSM сам генерирует новую ключевую пару	В HSM вводится только ключевая пара	В HSM вводится ключевая пара и подпись
«+» генерация и обновление в пределах контролируемой зоны эксплуатации HSM	«+» не требуется реализация в HSM функции генерации ключей	«+» не требуется реализация в HSM функций генерации ключей, а также формирования подписи «+» не требуется дополнительный учет нагрузки на закрытый ключ
«?» - подпись вычисляется единожды после смены		
«-» нужен механизм передачи ключевой пары в связанный HSM для синхронизации и резервирования «-» необходимость выполнения требований к СКЗИ с функцией генерации ключей «-» необходимость реализации функций формирования и проверки подписи	«-» зависимость от внешней инфраструктуры «-» необходимость реализации функций формирования и проверки подписи	«-» зависимость от внешней инфраструктуры

ИНТЕРФЕЙС ВЗАИМОДЕЙСТВИЯ UDM И HSM AUC

Запрос Authentication Crypto Request 5G:

Поле	Содержание
Code	Код запроса. Длина: 48 бит.
Kid	Идентификатор ключа абонента. Длина: 128 бит.
AMF	Элемент AMF (Authentication management field), устанавливающийся операторами связи. Длина: 16 бит.
SQN	Счетчик числа аутентификаций. Длина: 48 бит.
$RAND_{UE}$	Случайное значение из схемы защиты SUCI. Длина: 264 бит

$$RAND_{UE} = str_{256}(X^{eph}) \| a(Y^{eph}),$$
где $a(Y^{eph}) = Y^{eph} \bmod 2 \in \{0x00, 0x01\}$,
X^{eph} и Y^{eph} —координаты точки Q_{eph} из результата схемы защиты SUCI

Ответ Authentication Crypto Answer 5G:

Поле	Содержание
Code	Код ответа на запрос. Длина: 48 бит
AV	Вектор аутентификации, состоящий из: • RAND (128 бит); • XRES (64 бит); • CK (128 бит); • IK(128 бит); • SQN/(SQN⊕AK) (48 бит); • AMF (16 бит); • MAC (64 бит) Длина: 576 бит.

ИНТЕРФЕЙС ВЗАИМОДЕЙСТВИЯ UDM И HSM AUC

Запрос Resynchronization Crypto Request 5G:

Поле	Содержание
Code	Код запроса. Длина: 48 бит.
Kid	Идентификатор ключа абонента. Длина: 128 бит.
RAND	Случайное значение, используемое при генерации вектора аутентификации. Длина: 128 бит.
$RAND_{UE}$	Случайное значение из схемы защиты SUCI. Длина: 264 бит
Conc (SQN_{MS})	Сокрытый счетчик числа аутентификаций абонента. Длина: 48 бит.

Ответ Resynchronization Crypto Answer 5G:

Поле	Содержание
Code	Код ответа на запрос. Длина: 48 бит
XMACS	Вычисленная имитовставка для счетчика аутентификаций абонента. Длина: 64 бит
SQN_{MS}	Счетчик числа аутентификаций абонента. Длина: 48 бит.

Отличия интерфейса взаимодействия UDM и HSM AuC от интерфейса взаимодействия HLR/HSS и HSM AuC несущественные. Алгоритм S3G-5G также с точки зрения HSM AuC мало отличается от алгоритма S3G-256.

HSM AUC ДЛЯ СЕТЕЙ 5G

- Генерация вектора аутентификации с использованием алгоритмов S3G-256 и S3G-5G
- Вычисление аутентификационной информации при ресинхронизации
- Соответствие требованиям к СКЗИ для класса не ниже КВ
- Надежное хранение долговременных основных ключей абонентов (ДОКА) объемом до 10 млн.
- Производительность 20-50 тыс. запросов на аутентификацию в секунду (уточняется с учетом требований операторов связи)
- Интерфейс сопряжения с UDM в соответствии приказом Минцифры

HSM AuC для сетей 5G – продукт эволюционного развития HSM AuC для сетей 2-4G

HSM-SIDF ДЛЯ СЕТЕЙ 5G

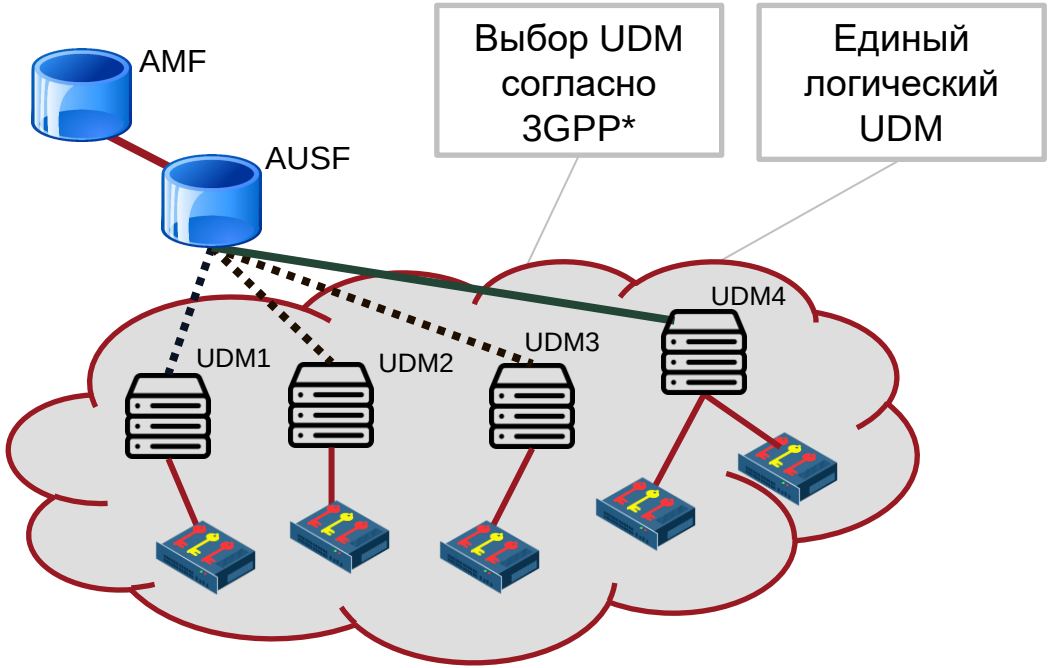
Назначение HSM-SIDF:

- Экспорт постоянного идентификатора SUPI из защищенного идентификатора SUCI по запросу от UDM
- Обновление открытых ключей домашней сети
- Вычисление $RAND_{UE}$ для алгоритма S3G-5G

Требования к HSM-SIDF:

- Соответствие требованиям к СКЗИ для класса не ниже КВ
- Надежное хранение ключевых пар домашней сети
- Производительность, достаточная для реализации схемы ECIES, с учетом требований операторов связи
- Интерфейс сопряжения с UDM в соответствии с проектом приказа Минцифры

СОВМЕЩЕНИЕ ФУНКЦИОНАЛА HSM-SIDF И HSM AUC В ЕДИНОМ УСТРОЙСТВЕ



PROS

Процедура аутентификации согласно 5G-AKA-GOST требует использования как HSM AuC, так и HSM-SIDF. Оба устройства взаимодействуют с UDM. Дополнение HSM AuC функциями HSM-SIDF выглядит логичным и архитектурно верным решением

CONS

Баланс производительности по функциям расчета векторов аутентификации и расшифрования SUCI в едином устройстве может быть неоптимальным

* 3GPP TS 23.501 «System architecture for the 5G System», п.6.3.8

ВЫВОДЫ

- Ввод ключевой информации в HSM-SIDF требует дальнейшего обсуждения. При формировании записи об обновлении открытого ключа, целесообразно формировать подпись для записи единоразово при получении новой ключевой пары
- Необходимо учитывать особенность S3G-5G в интерфейсе взаимодействия HSM AuC и UDM
- Процедура аутентификации 5G-AKA-GOST требует использования как HSM AuC, так и HSM-SIDF, причем, дополнение HSM AuC функциями HSM-SIDF выглядит архитектурно верным решением
- Необходимо уточнить требования операторов связи к производительности функций расчета векторов аутентификации и расшифрований SUCI. Баланс производительности по функциям в едином устройстве может оказаться неоптимальным

Спасибо за внимание!

РусКрипто XXVIII научно-практическая конференция

ГРУППА КОМПАНИЙ СПБ

Емельянов-Гирс В.М., Герасимова А.Г., Третникова Е.Н., Устюгов А.А., Андреев А.З.

info@systempb.ru

+7 (812) 468-15-61 www.systempb.ru | www.skzi.ru | @GKSPB_skzi