Технология eSIM. Проблемы внедрения российских криптографические механизмов в стандарты GSMA: задачи, перспективы

Грибоедова Екатерина

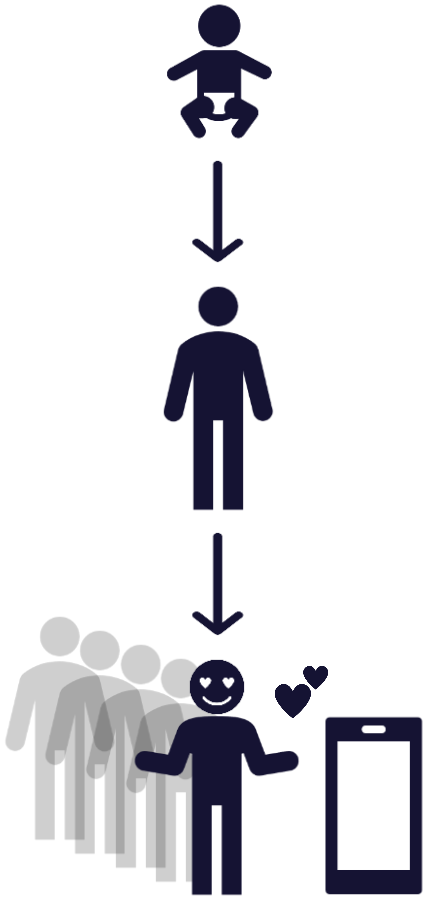
Руководитель направления стандартизации,
Лаборатория криптографии

Рускрипто’2022

КРИПТОНИТ

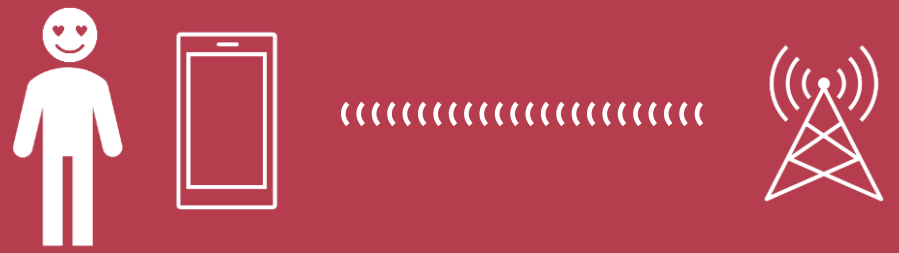
КРИПТОНИТ

Что такое eSIM?

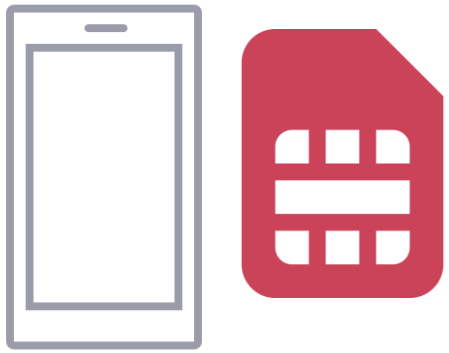


КРИПТОНИТ

5G-AKA



Профиль пользователя

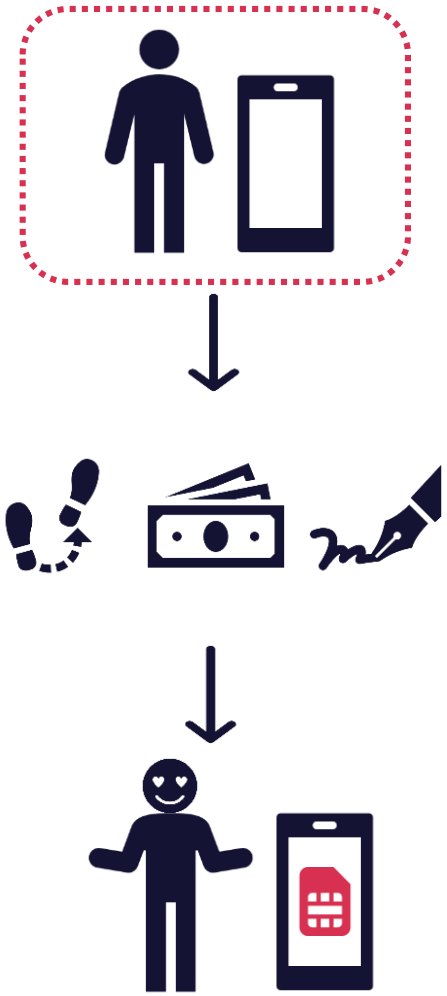


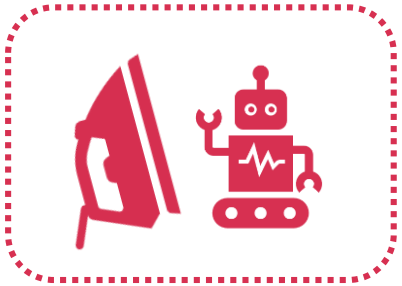
1. Информация о домашней сети (HN)
2. Уникальная информация пользователя (Ключ K, идентификатор SUPI)
3. Криптографический модуль (например, набор функций S3G)

5G-AKA

1 SIM

КРИПТОНИТ





1. Цена и трудозатраты смены сим-карты на сотнях и тысячах единиц техники
2. Трудность смены оператора. Оператор может диктовать цену.
3. Проблемы в логистике и роуминге

2 eSIM

КРИПТОНИТ

eSIM – технология, позволяющая дистанционно загружать настройки (**профили**) абонента для работы в сети операторов связи.

Обычная SIM-карта и SIM-чип не позволяют изменить оператора связи без похода в салон и замены физического носителя. Технология eSIM позволяет **удаленно «перепрошить»** устройство и загрузить туда новый абонентский профиль.

КРИПТОНИТ

Consumer (для пользователя)

устройства с возможностью ввода/вывода информации, управление осуществляет непосредственно пользователь

M2M, IoT

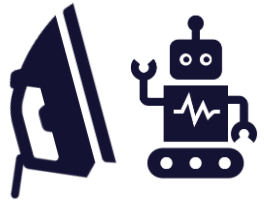
устройства без экрана и средств ввода, управление осуществляется со стороны

КРИПТОНИТ

eSIM

Consumer (для пользователя)

Стандарт SGP.21, SGP.22:
www.gsma.com/esim/esim-specification



M2M, IoT

Стандарт SGP.01, SGP.02:
www.gsma.com/esim/esim-m2m-specifications

С 2021 года Криптонит является членом GSMA.

Развитие технологии eSIM на базе российских криптографических алгоритмов является одной из основных задач в рамках новой РГ КМ ПРТС

Что такое eSIM?

Инфраструктура eSIM

Роль GSMA

КРИПТОНИТ

1. Выработка спецификаций
2. Аккредитация участников
3. Регулирование инфраструктуры PKI

GSMA

КРИПТОНИТ

EUM
производитель eUICC

CI
удостоверяющие центры

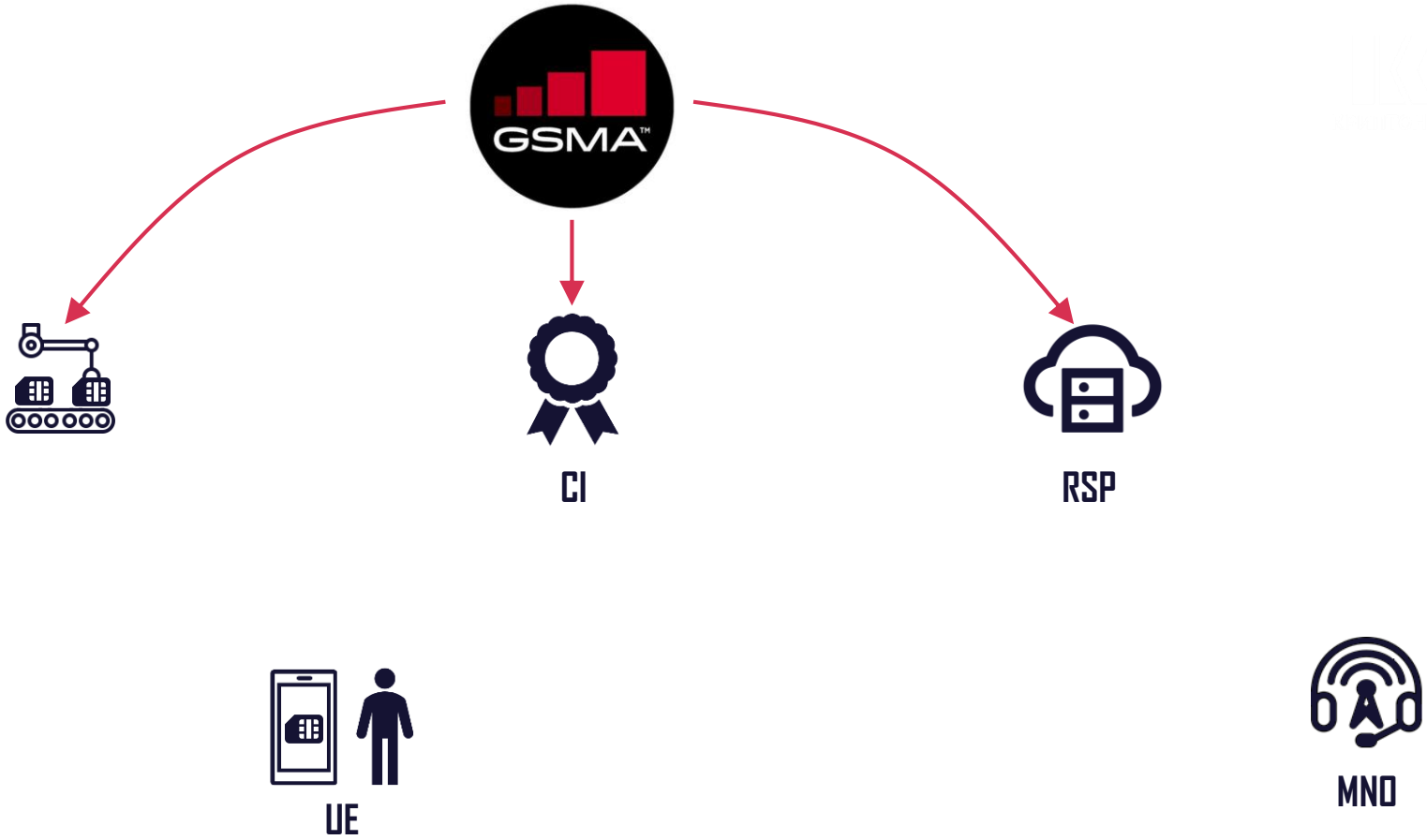
RSP
платформа загрузки профилей

MNO
операторы связи

eSIM
устройства с eSIM

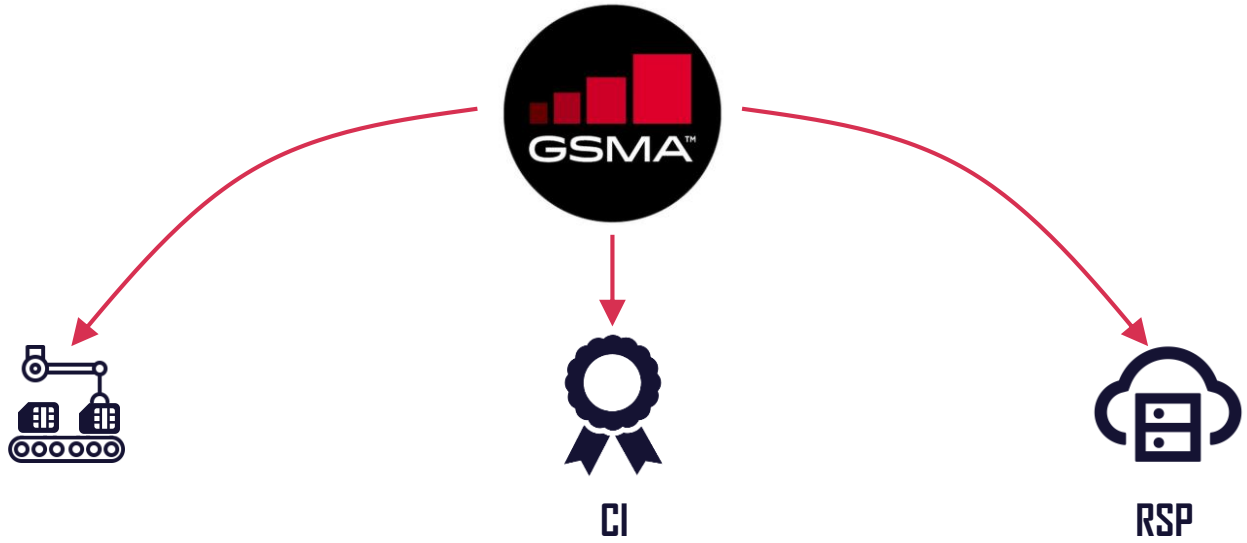
1

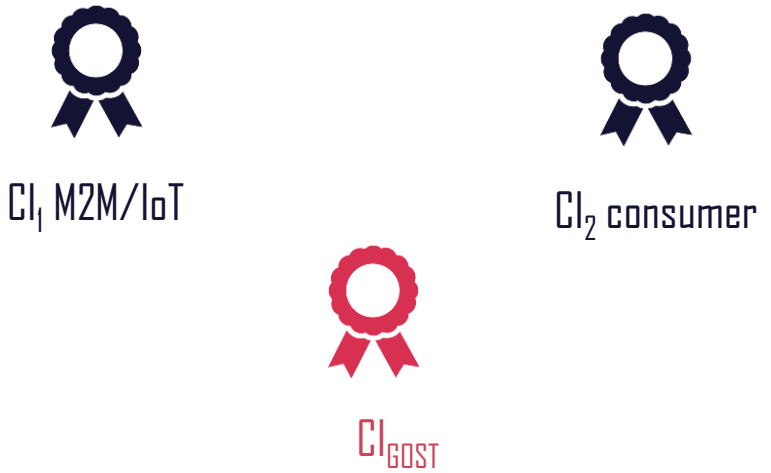
Аккредитация



1

Аккредитация

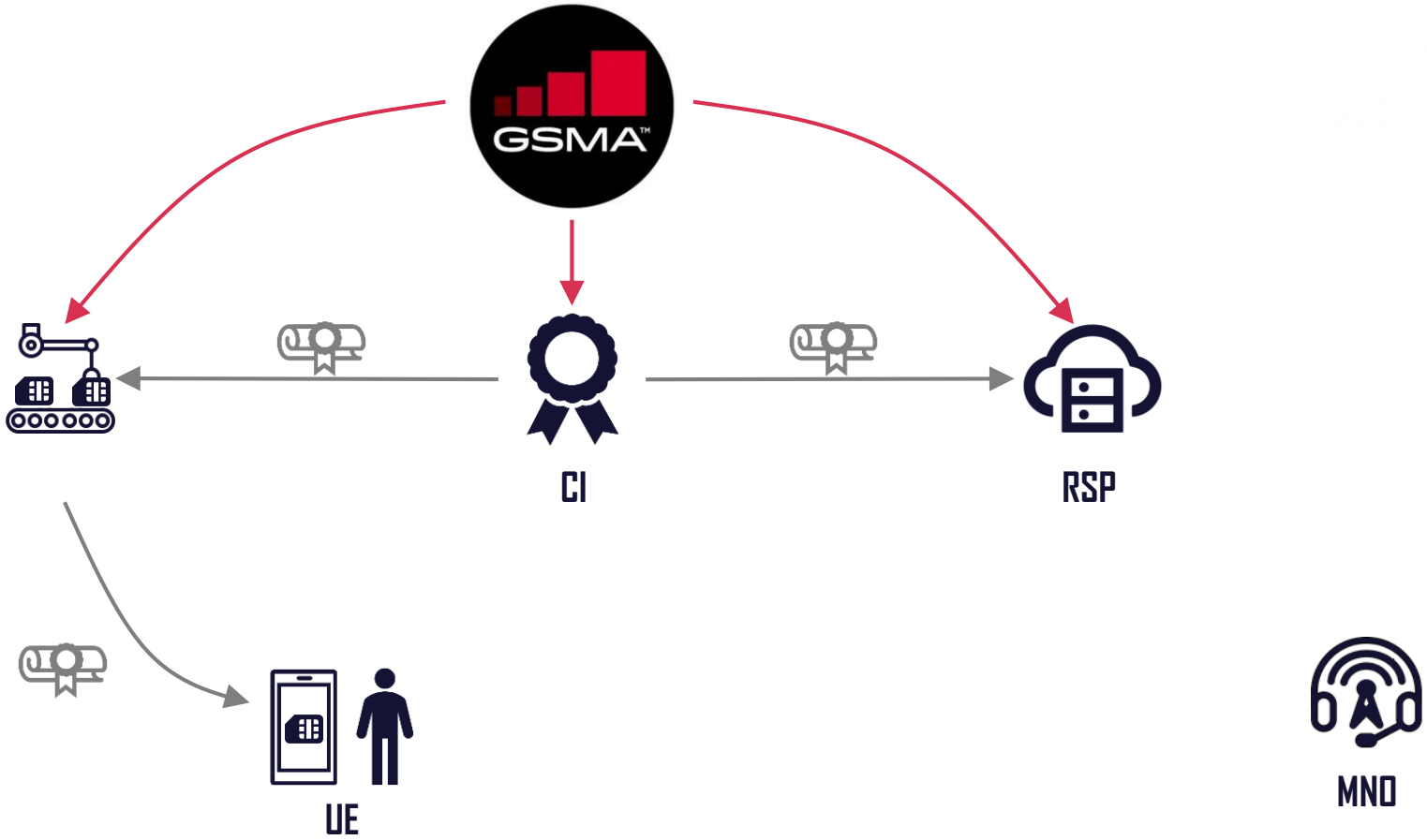




Первая ключевая проблема: необходимость организации CI с поддержкой сертификатов по ГОСТ. Подробнее об этом в докладе “Особенности построения инфраструктуры PKI GSMA” (Александров С.В. и др.).

2

PKI: выдача сертификатов

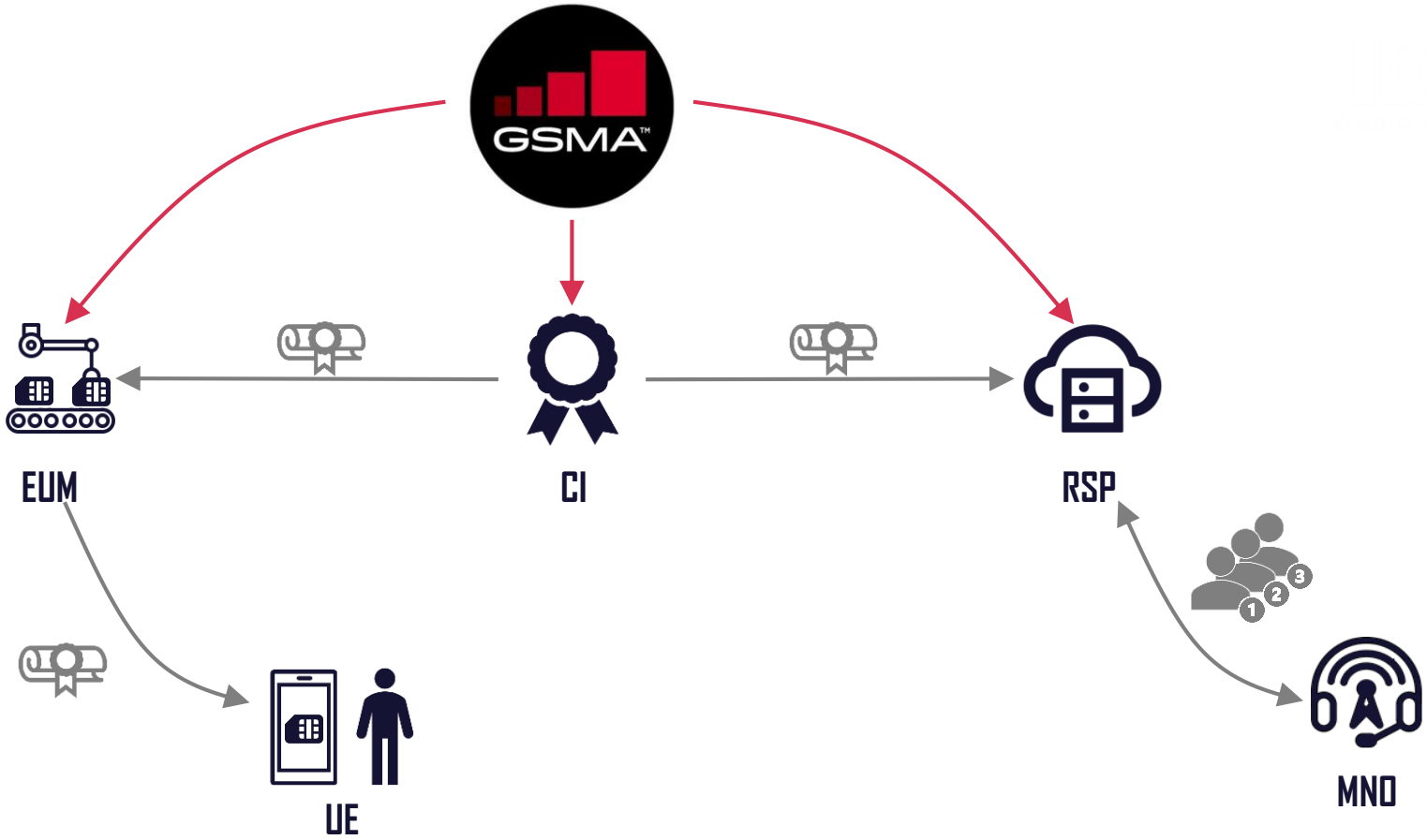


Удостоверяющие центры должны поддерживать использование по крайней мере одного алгоритма, сертифицированного в GSMA (сейчас это только ECDSA).

В очередной версии спецификаций (ориентировочно май 2022 года) появится возможность опционального добавления произвольных алгоритмов подписи.

3

Генерация профилей

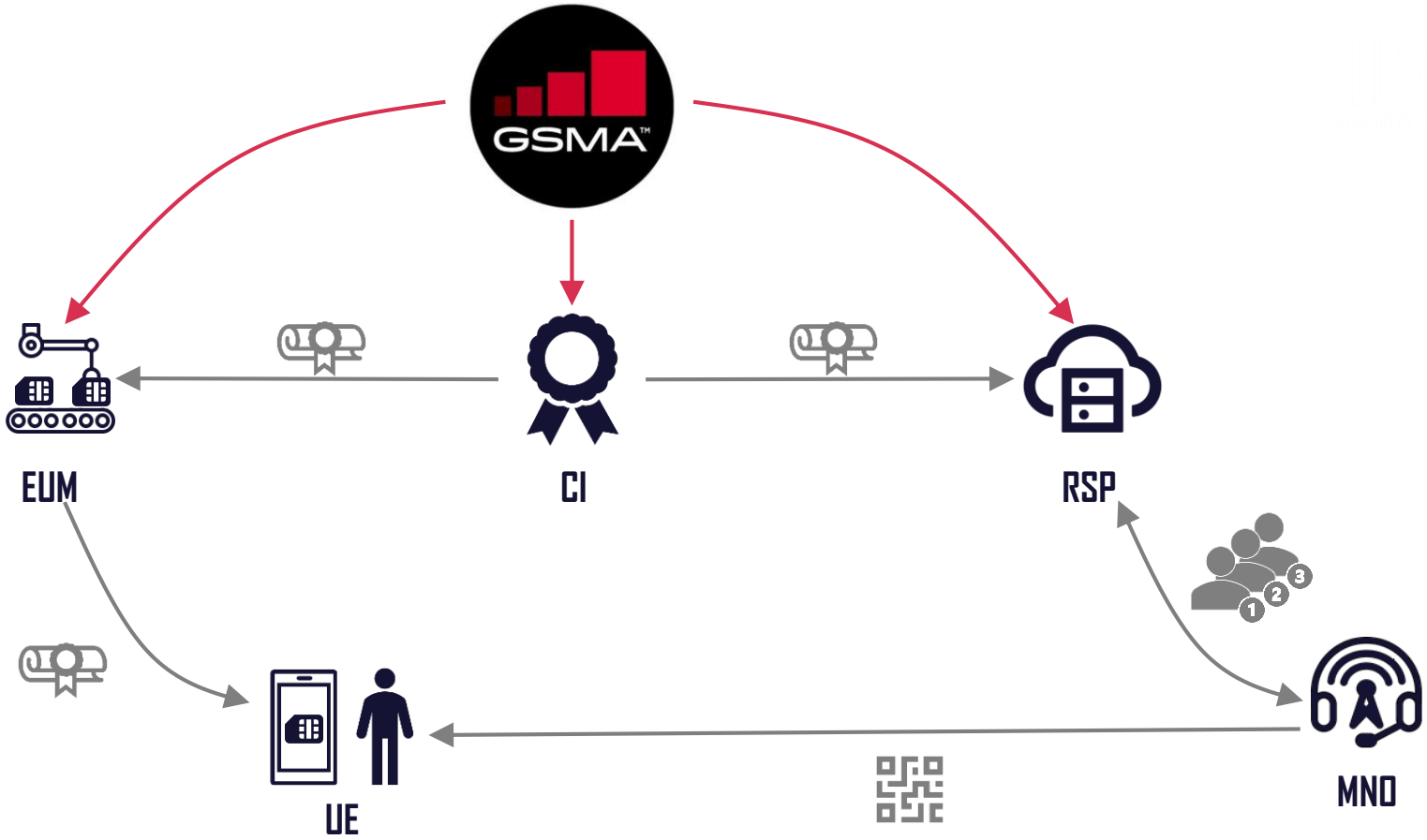


Одна из сторон (RSP/MNO) генерирует учетные данные пользователя (в т.ч. SUPI, K) и передает его второй стороне.

RSP записывает учетные данные в профиль пользователя Uprofile .

4

Activation Code



Activation Code (например, в формате QR-кода) генерируется оператором для конкретного пользователя и содержит ссылку на скачивание профиля в RSP.

Получив QR-код, пользователь переходит по ссылке и устанавливает соединение с RSP.

4

Activation Code

4.1 Activation Code

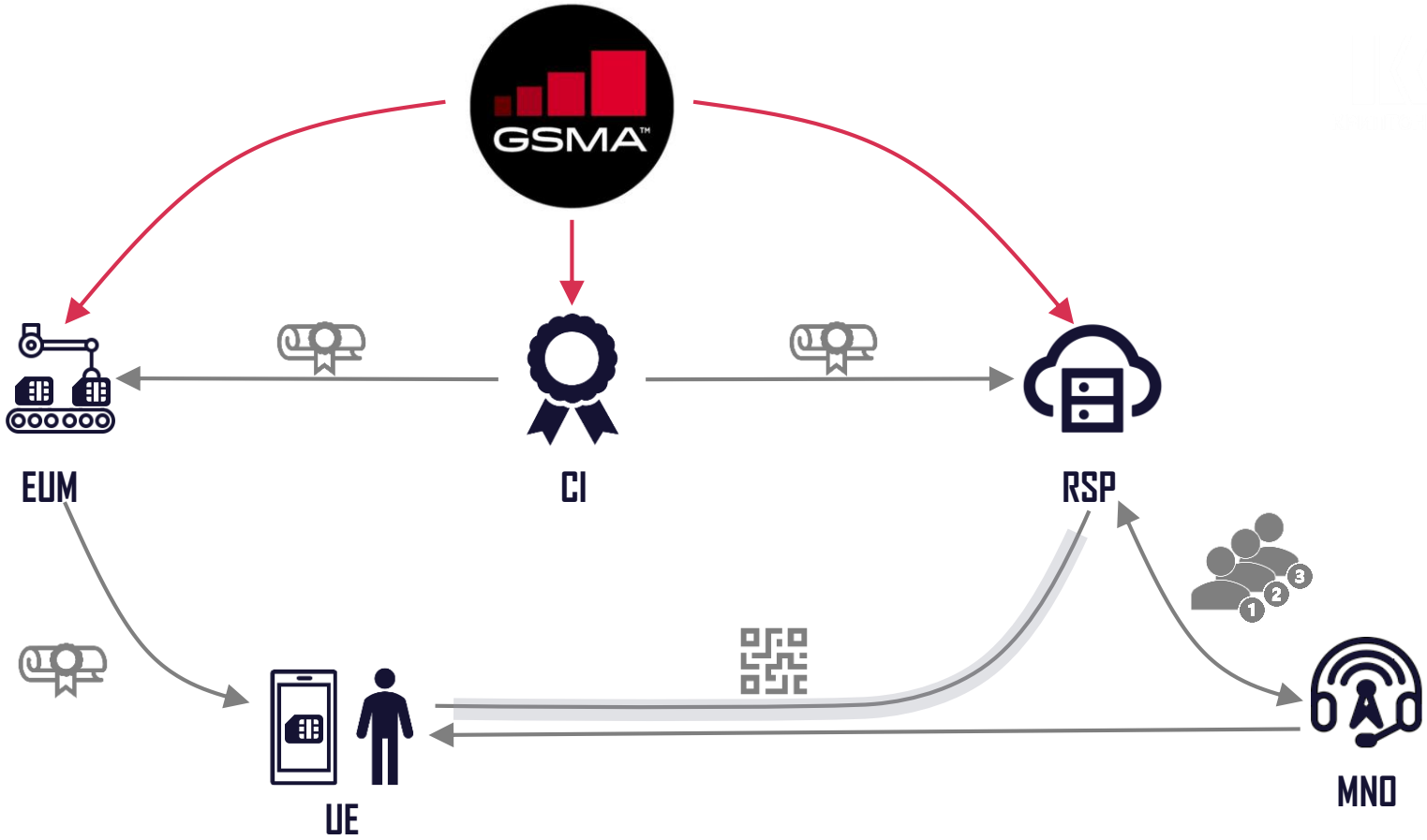
The Activation Code SHALL be coded to be the concatenation of the following strings listed in the following table:

Name	Description	MOC
AC_Format	Format of the Activation Code. SHALL be set to "1" for this Format of the Activation Code and any subsequent backward compatible Format	M
Delimiter	SHALL be set to "$"	M
SM-DP+ Address	FQDN (Fully Qualified Domain Name) of the SM-DP+ (e.g., SMDP.GSMA.COM) restricted to the Alphanumeric mode character set defined in table 5 of ISO/IEC 18004 [15] excluding '$'	M
Delimiter	SHALL be set to "$"	M
AC_Token	MatchingID as described in section (4.1.1)	M
Delimiter	SHALL be present and set to "$" if any of the following optional parameters is present	C
SM-DP+ OID	SM-DP+ OID in the CERT.DPauth.ECDSA	O
Delimiter	SHALL be present and set to "$" if any of the following optional parameters is present	C
Confirmation Code Required Flag	SHALL be present and set to "1" if Confirmation Code is required; otherwise it SHALL be absent	O

PIN

4

Activation Code



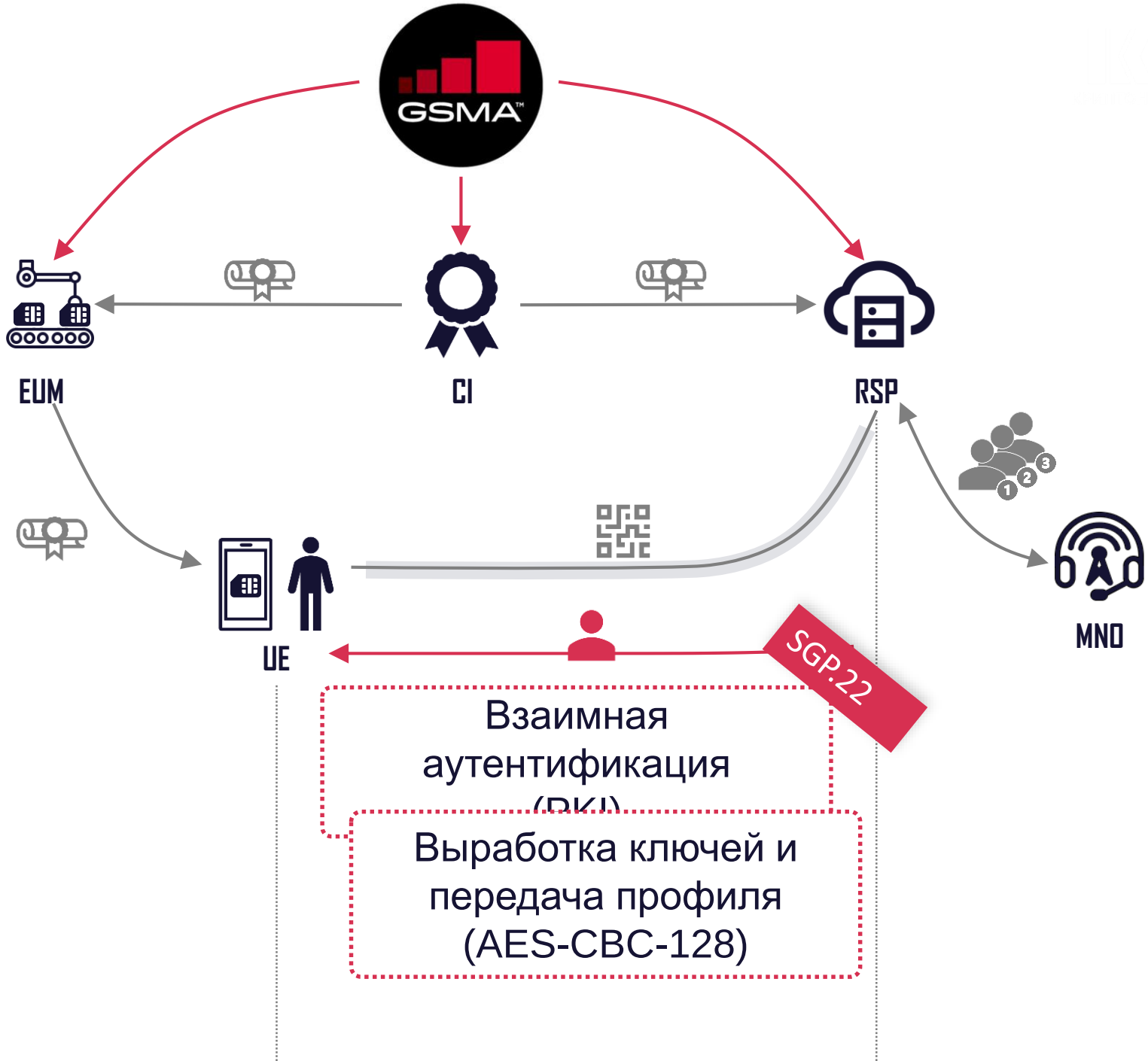
Соединение с RSP устанавливается по каналу, защищенному TLS. GSMA допускает опциональный выбор используемых криптонаборов (что хорошо).

После установки соединения запускается протокол защищенной передачи данных профиля пользователя на eUICC, в процессе которого выполняется аутентификация сторон и выработки ключевого материала.

5

Передача профиля

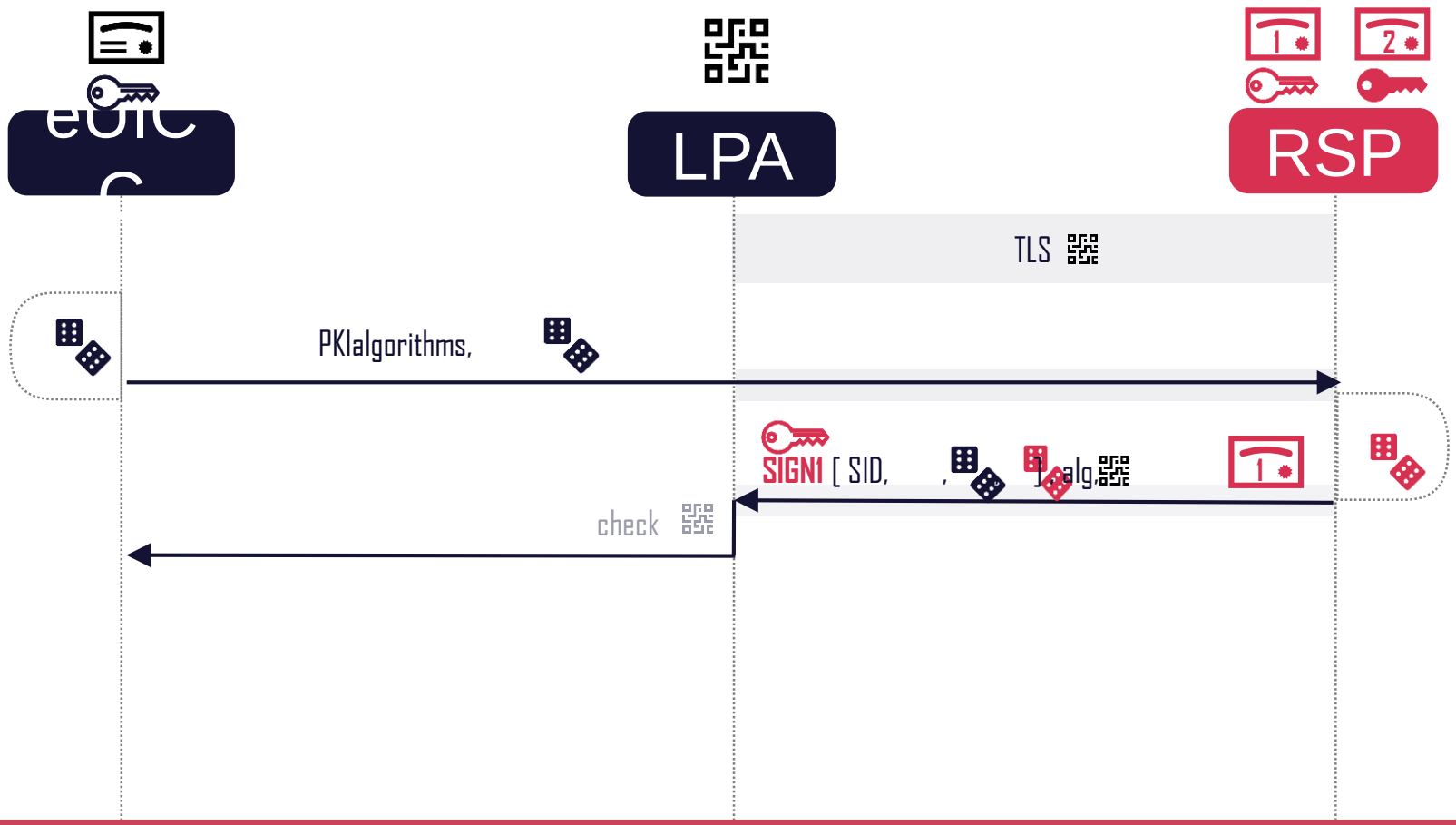
???



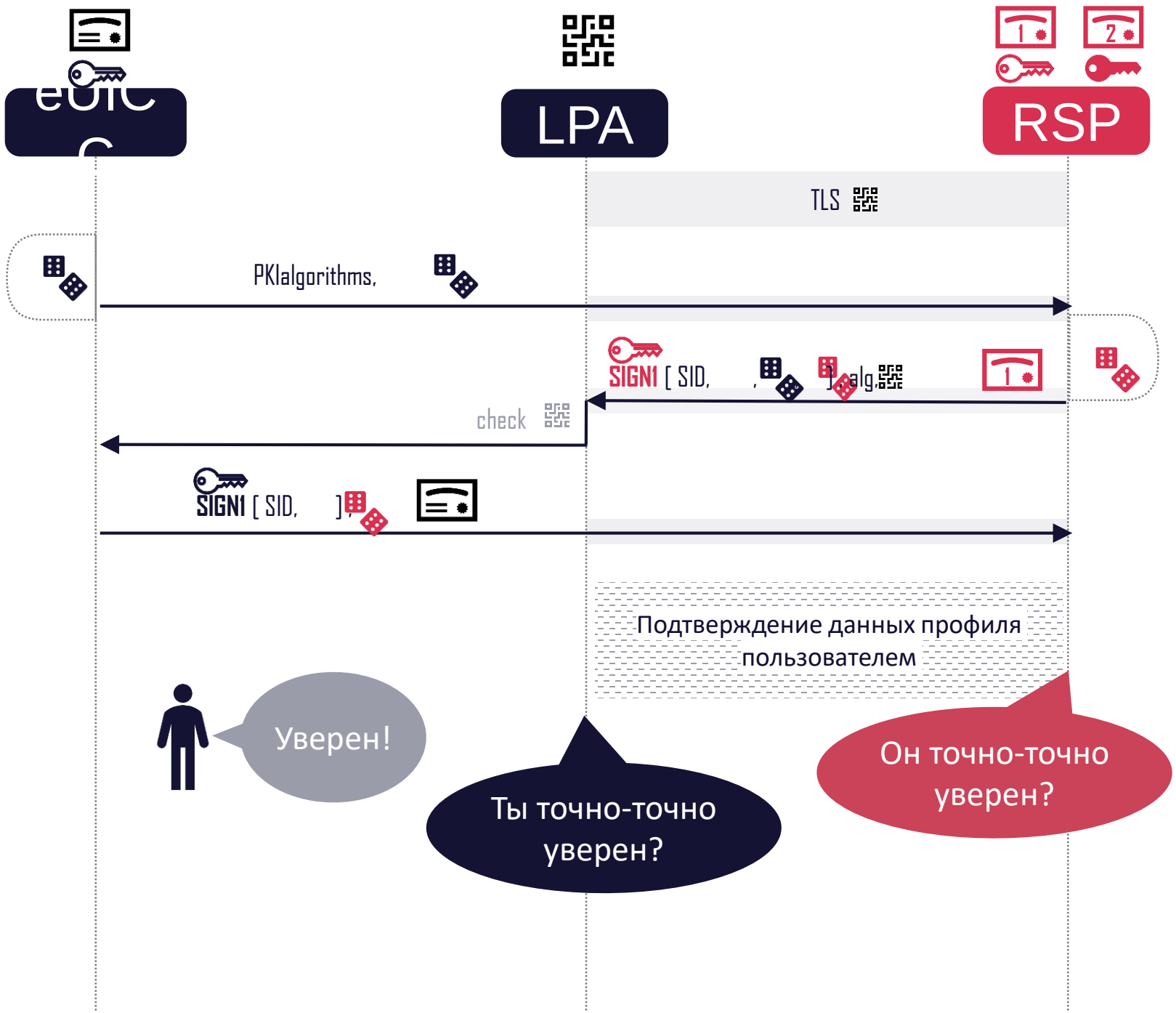
КРИПТОНИТ

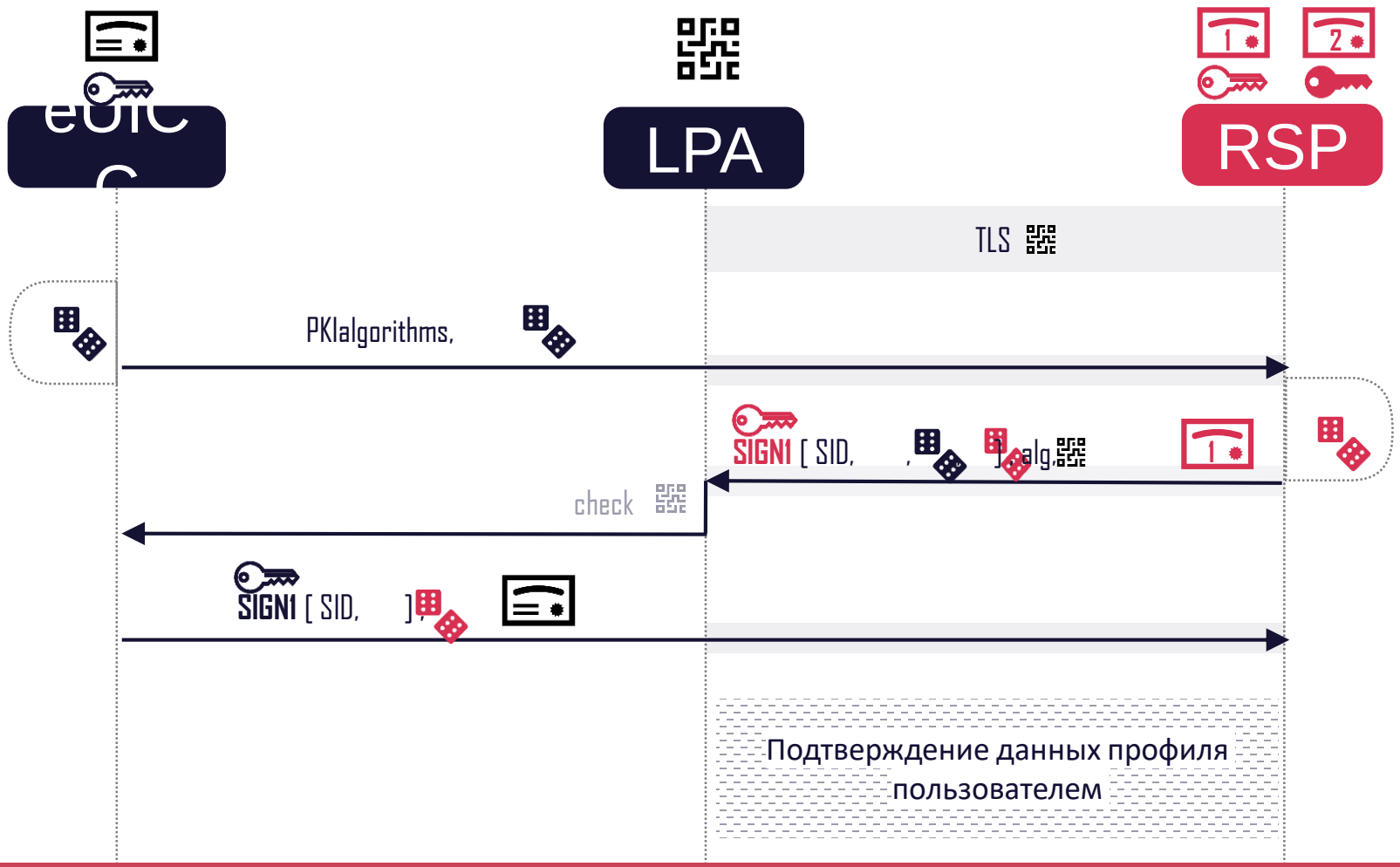
- Что такое eSIM?
- Инфраструктура eSIM
- Передача профиля. Consumer


eUIC
C
LPA
Системное приложение в телефоне
RSP

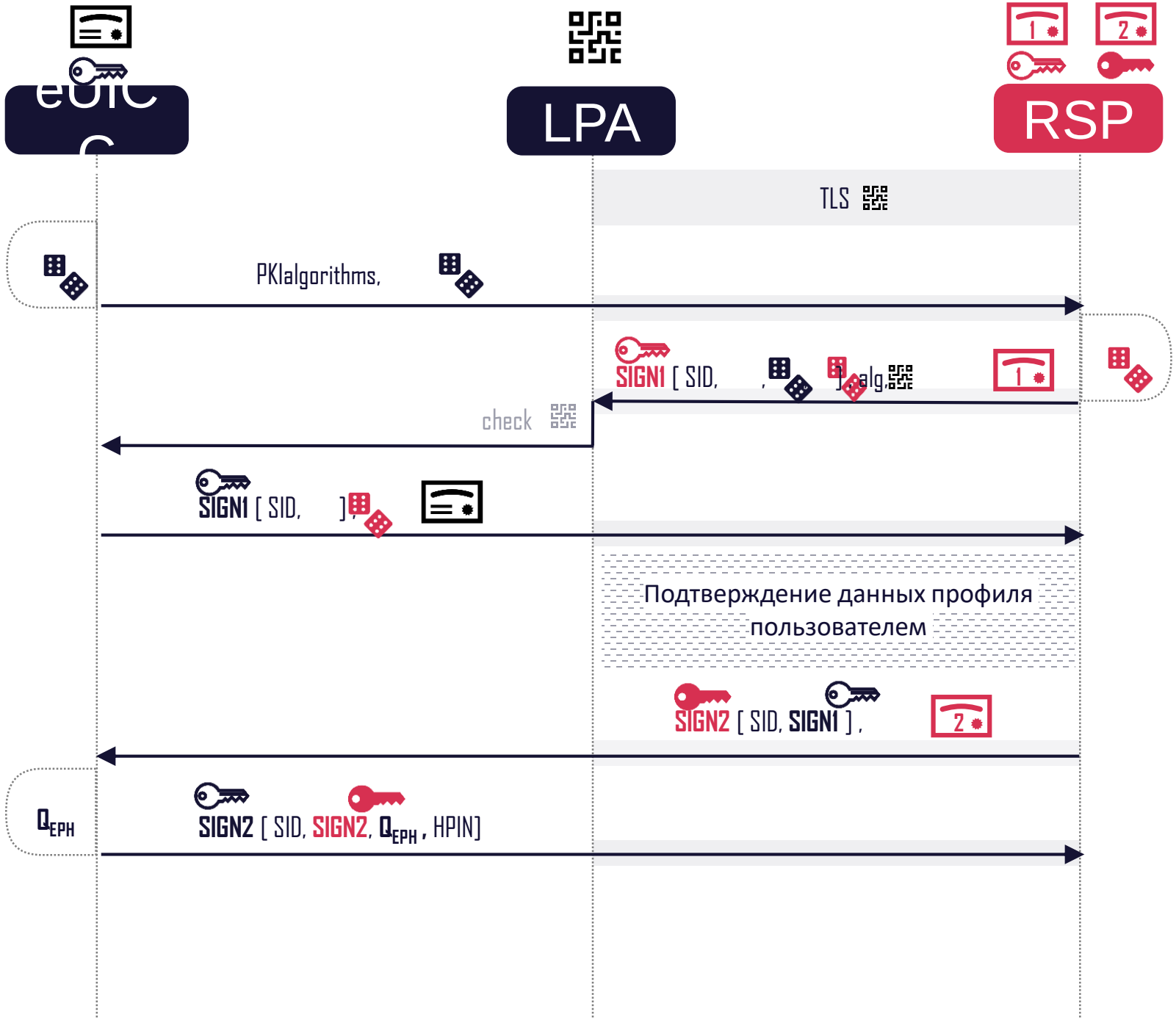


Поле alg не защищается подписью: потенциальная возможность для downgrade-атак.

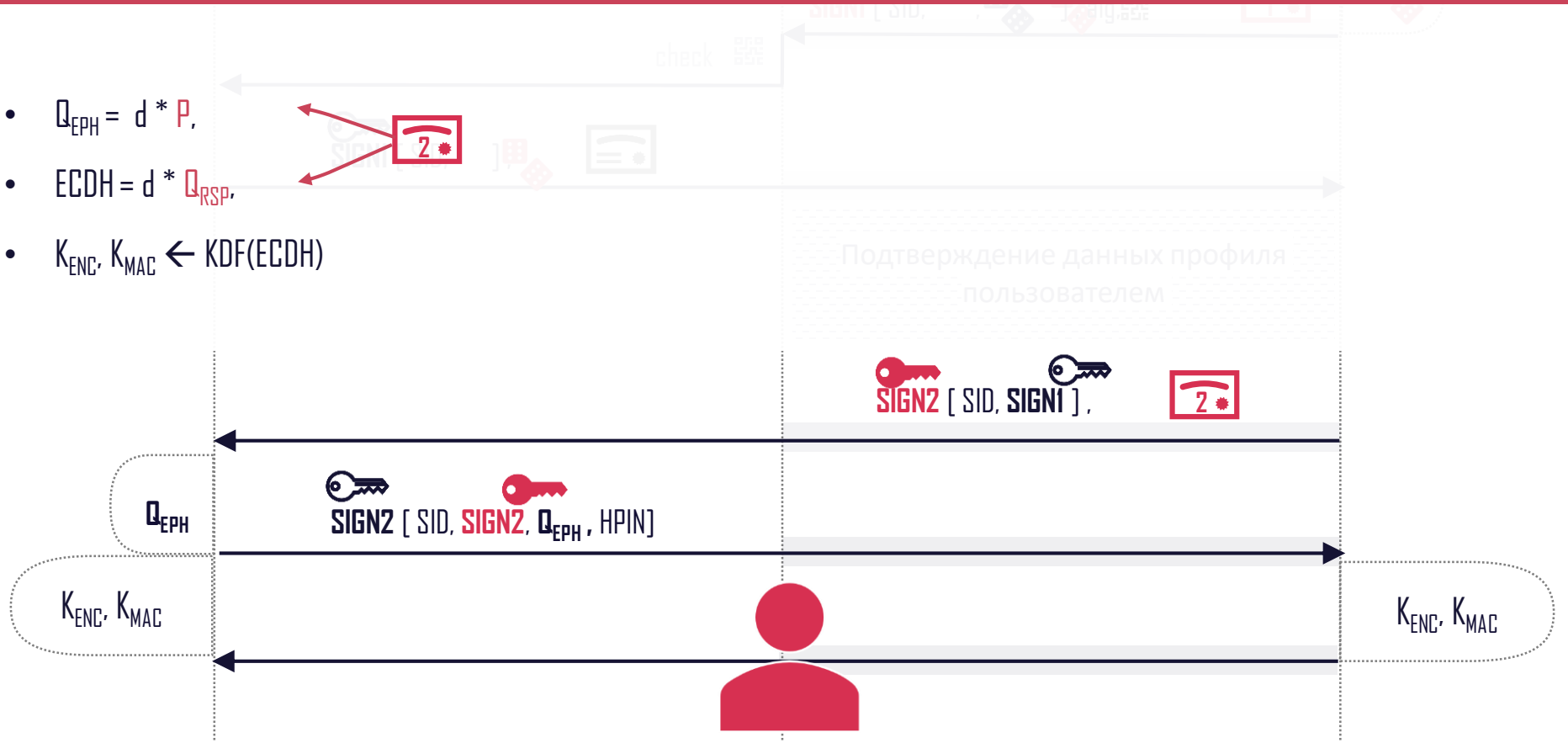

eUICC
LPA
RSP
TLS
PKIalgorithms,
SIGN1 [SID,
alg,
check
SIGN1 [SID,
Подтверждение данных профиля пользователем
Уверен!
Ты точно-точно уверен?
Он точно-точно уверен?

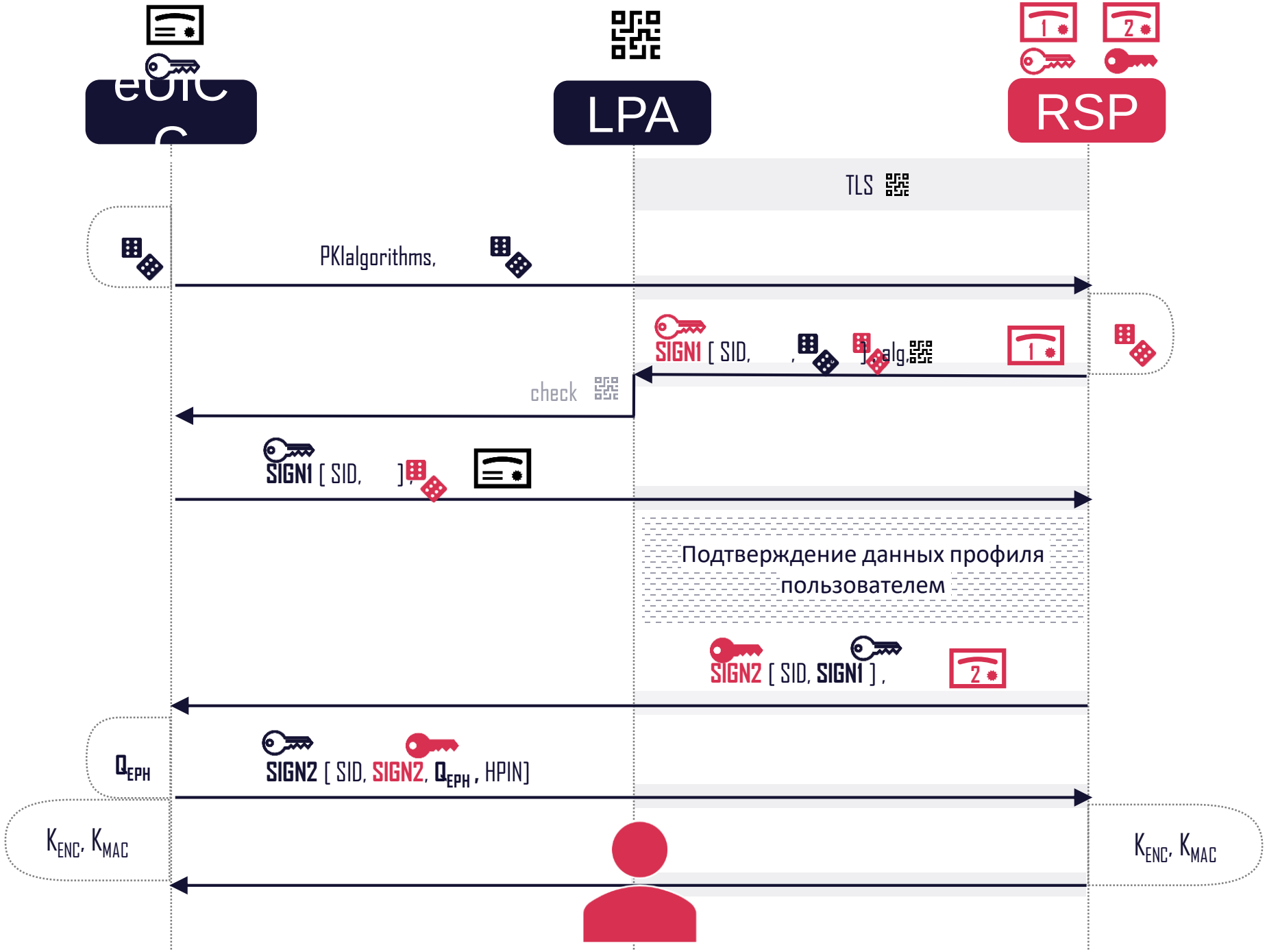


Вопрос доверенности узла LPA влияет на возможность проведения MiTM-атак (подмена информации в коде активации и при подтверждении действий пользователя), поэтому требует отдельного изучения.


eUICC
LPA
RSP
TLS
PKIalgorithms,
SIGN1 [SID,
alg,
check
SIGN1 [SID,
]
Подтверждение данных профиля пользователем
SIGN2 [SID, SIGN1] ,
QEPH
SIGN2 [SID, SIGN2, QEPH , HPIN]

- Использование одного и того же ключа сертификата в двух криптографических операциях: при формировании подписи и при генерации ECDH-значения. Возможная альтернатива – неявная аутентификация (eSIM-M2M, TLS 1.2 на базе российских криптонаборов).
- Использование полустатического Диффи-Хеллмана. Возможные альтернативы – VKO, использование полностью эфемерного Диффи-Хеллмана.
- Зашитый AES




eUICC
LPA
RSP
TLS
PKIalgorithms,
SIGN1 [SID,
alg,
check
SIGN1 [SID,
]
Подтверждение данных профиля пользователем
SIGN2 [SID, SIGN1] ,
QEPH
SIGN2 [SID, SIGN2, QEPH , HPIN]
KENC, KMAC
KENC, KMAC

Передача профиля. Consumer

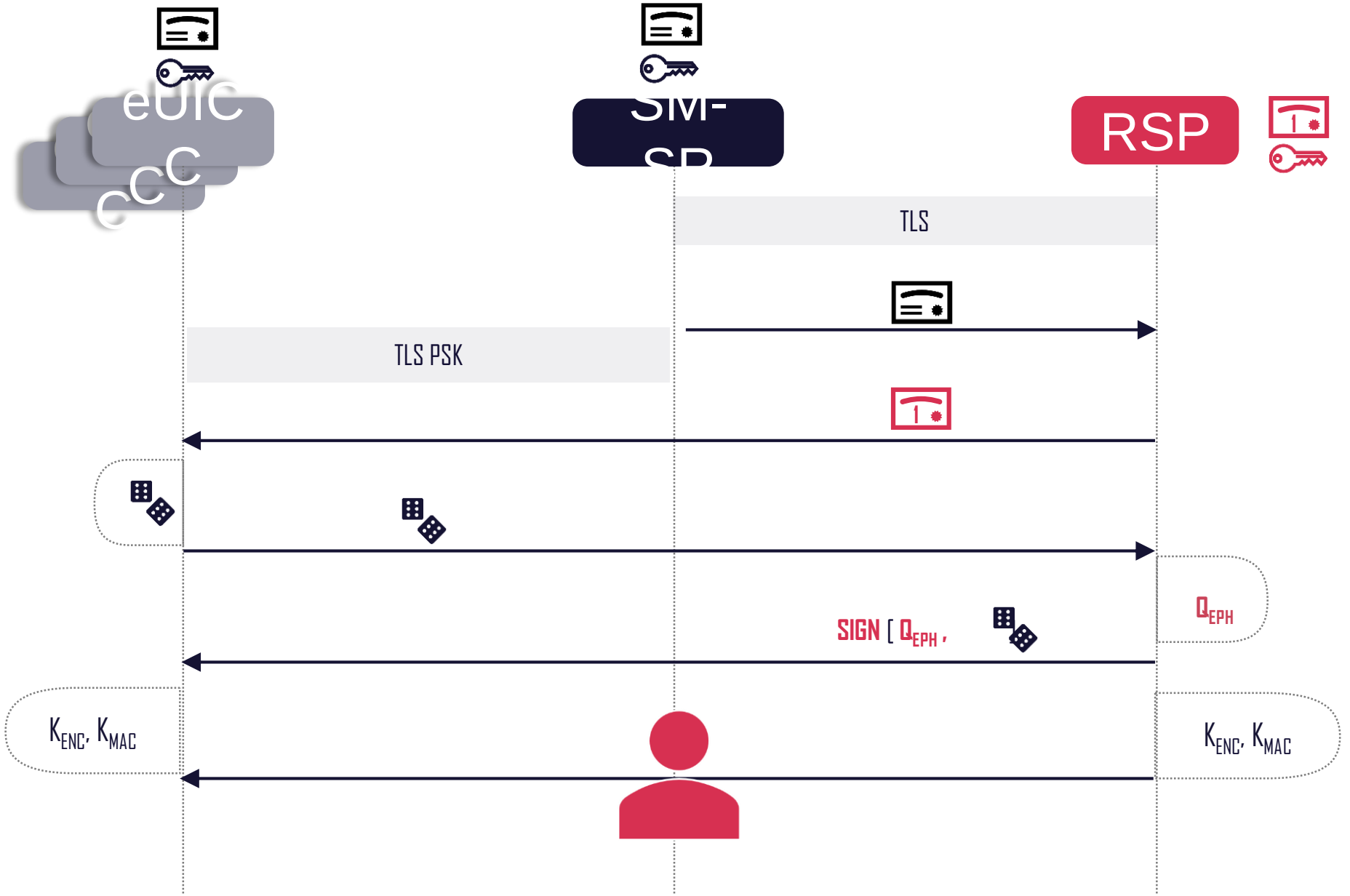
КРИПТОНИТ

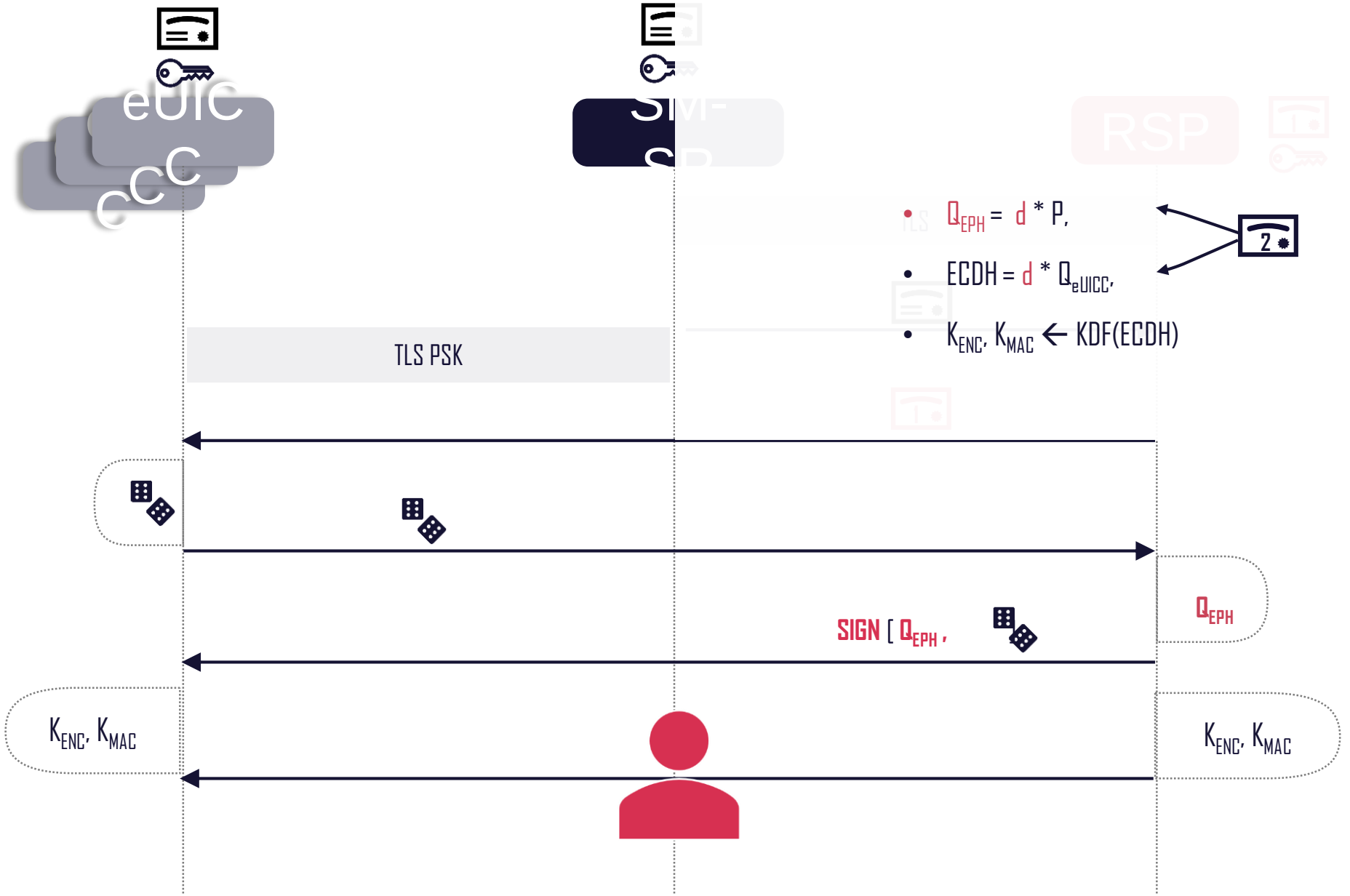
Поскольку в GSMA (как и в 3GPP) не используются классические AKE-протоколы семейства SigMa (TLS 1.3, IPSec), в текущей версии протокола могут быть следующие потенциально слабые места:

- Поле alg не защищается подписью: потенциальная возможность для downgrade-атак.
- Вопрос доверенности узла LPA влияет на возможность проведения MiTM-атак (подмена информации в коде активации и при подтверждении действий пользователя), поэтому требует отдельного изучения.
- Использование одного и того же ключа сертификата в двух криптографических операциях: при формировании подписи и при генерации ECDH-значения. Возможная альтернатива – неявная аутентификация (eSIM-M2M, TLS 1.2 на базе российских криптонаборов).
- Использование полустатического Диффи-Хеллмана. Возможные альтернативы – VKO, использование полностью эфемерного Диффи-Хеллмана.

КРИПТОНИТ

- Что такое eSIM?
- Инфраструктура eSIM
- Передача профиля. Consumer
- **Передача профиля. M2M**


eUICC
SM-SR
RSP
TLS
TLS PSK
SIGN [Q_{EPH} ,
Q_{EPH}
K_{ENC}, K_{MAC}
K_{ENC}, K_{MAC}


eUICC
SM-SR
RSP
• $Q_{EPH} = d * P$,
• ECDH = $d * Q_{eUICC}$,
• K_{ENC}, K_{MAC} ← KDF(ECDH)
TLS PSK
Q_{EPH}
SIGN [Q_{EPH} ,
K_{ENC}, K_{MAC}
K_{ENC}, K_{MAC}

Передача профиля. M2M

КРИПТОНИТ

Первые выводы:

- Неявная аутентификация со стороны eUICC (в отличие от режима Consumer).
- Использование полустатического Диффи-Хеллмана. Возможные альтернативы – VKO, использование полностью эфемерного Диффи-Хеллмана.
- Отсутствие случайности со стороны RSP (возможно всё ок за счет Q_{EPH}).
- Пересылка сертификата отделена от пересылки подписи (потенциально лишняя пересылка).

Ближайшие планы

КРИПТОНИТ

ТК 26

Установочное заседание ТК 26, фиксирование плана работ

Взаимодействие с GSMA

PKI с поддержкой GOST,

Криптографический анализ протоколов,

Внесение новых предложений

...

Авторы доклада:

Грибоедова Екатерина

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

Самохвалов Роман

Специалист-исследователь,
Лаборатория телекоммуникаций
r.samokhvalov@kryptonite.ru

Давыдов Степан

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

Царегородцев Кирилл

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

Спасибо за внимание! ☺