конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто'2022»

Система доверенной аутентификации абонентов сети подвижной радиосвязи

В.М. Емельянов
Руководитель направления, ООО «СПБ»

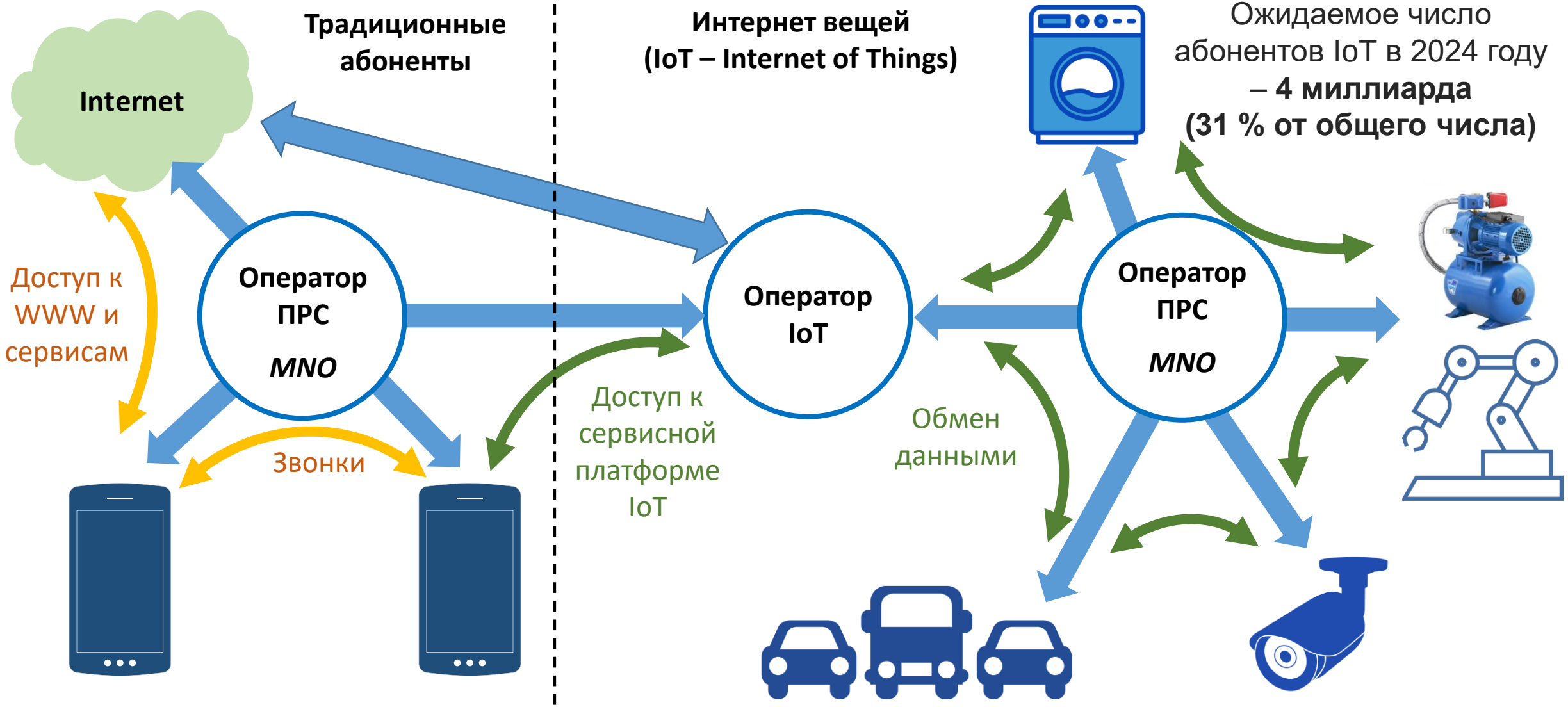
С.В. Александров
Технический директор, ООО «СПБ»

Услуги сотовой связи для традиционных абонентов и IoT

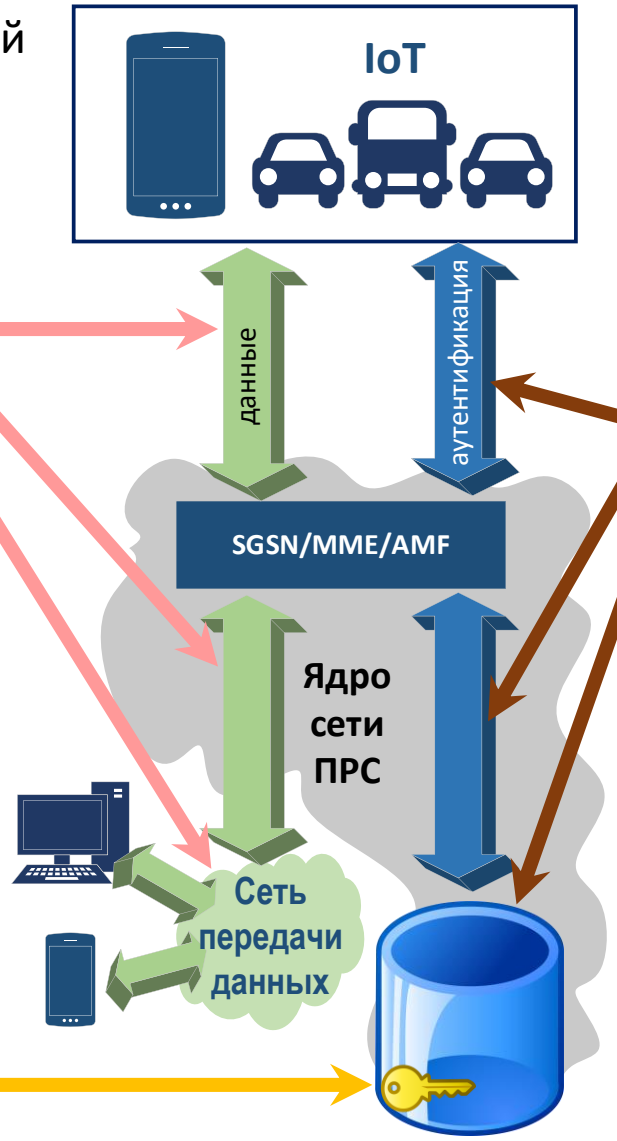
Традиционные абоненты

Интернет вещей (IoT – Internet of Things)

Ожидаемое число абонентов IoT в 2024 году **– 4 миллиарда (31 % от общего числа)**



Угрозы и безопасность



Угрозы пользовательским данным:

1. Нарушение конфиденциальности (перехват)
2. Нарушение целостности (искажение или подмена при передаче)

Угрозы персональным данным:

1. Нарушение конфиденциальности (утечка)
2. Нарушение целостности (искажение)

Следствия:

1. Передача третьим лицам
2. Искажение данных профиля в целях мошенничества или отказа в обслуживании
3. Подготовка сценариев действий от лица абонента

Угрозы служебным данным:

1. Раскрытие местоположения абонента через получение его постоянных идентификаторов
2. Раскрытие ключа аутентификации и ключей шифрования
3. Отказ в облуживании

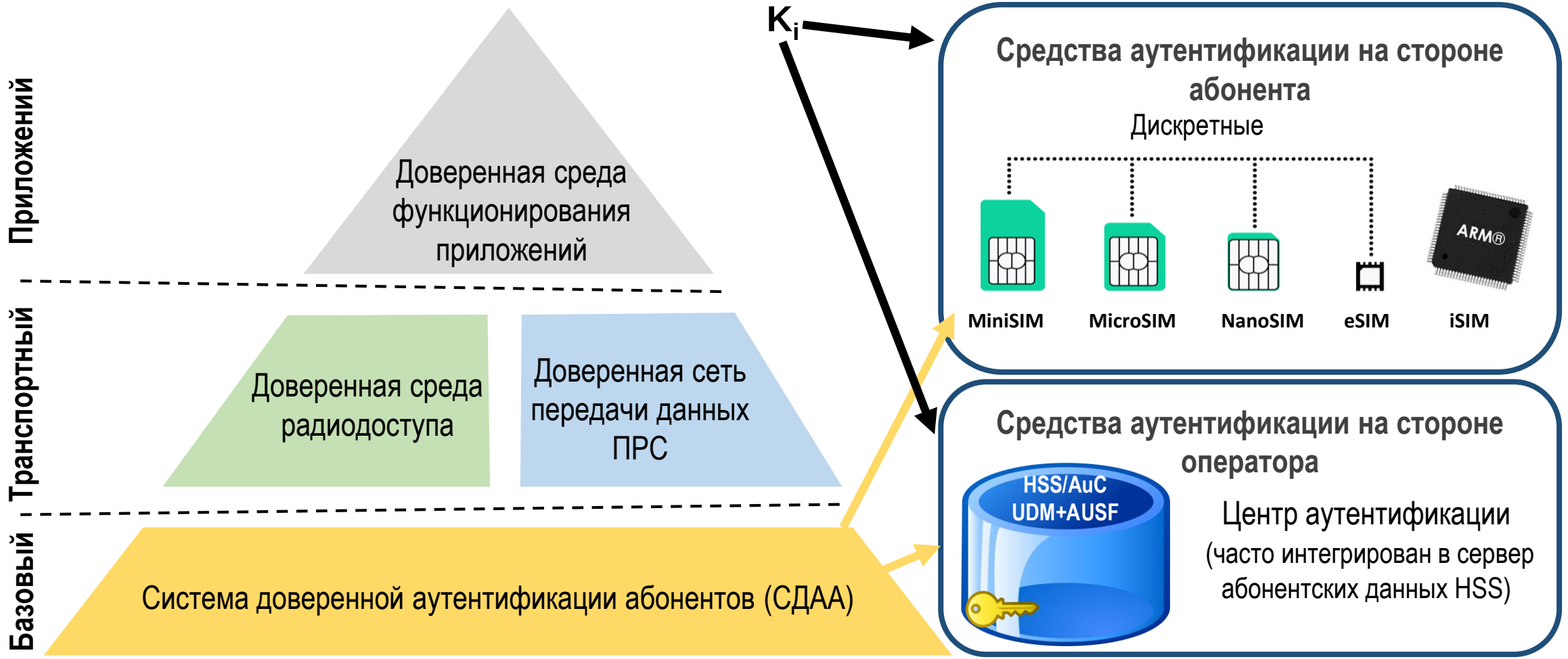
Следствия:

1. Слежение за перемещениями абонента
2. Перехват трафика или подмена абонентского терминала в сети

Угрозы аутентичности абонента:

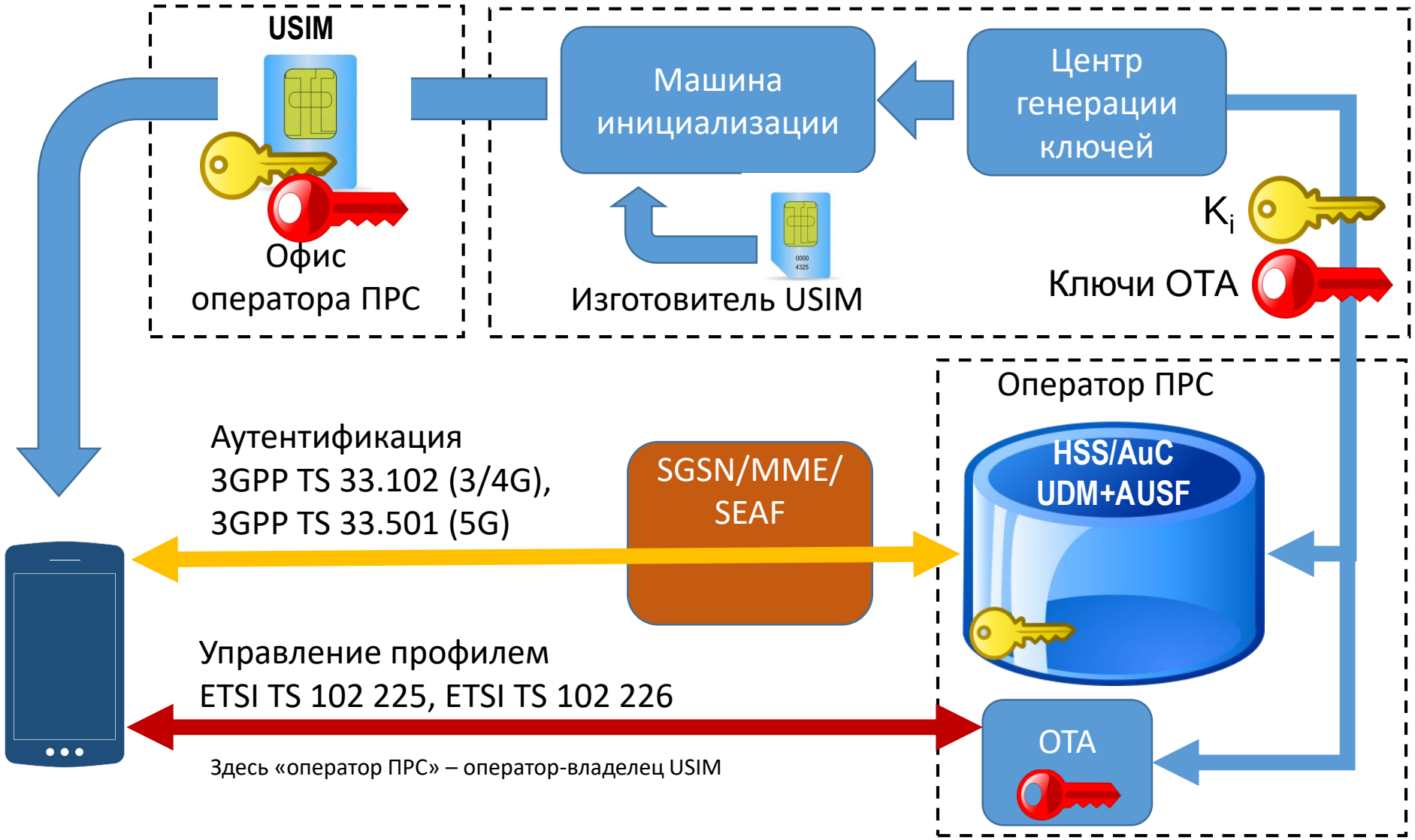
1. Аутентификация нарушителя от лица абонента в платежных системах
2. Аутентификация нарушителя в от лица абонента в государственных информационных системах
3. «Клонирование» абонентского терминала для иных действий от лица абонента (в т.ч. терроризма)

Уровни безопасности и система доверенной аутентификации



В сетях 3G/4G/5G все используемые ключи шифрования и имитозащиты порождаются от ключа аутентификации (и ключа K_i). СДАА – основа повышения безопасности сетей ПРС

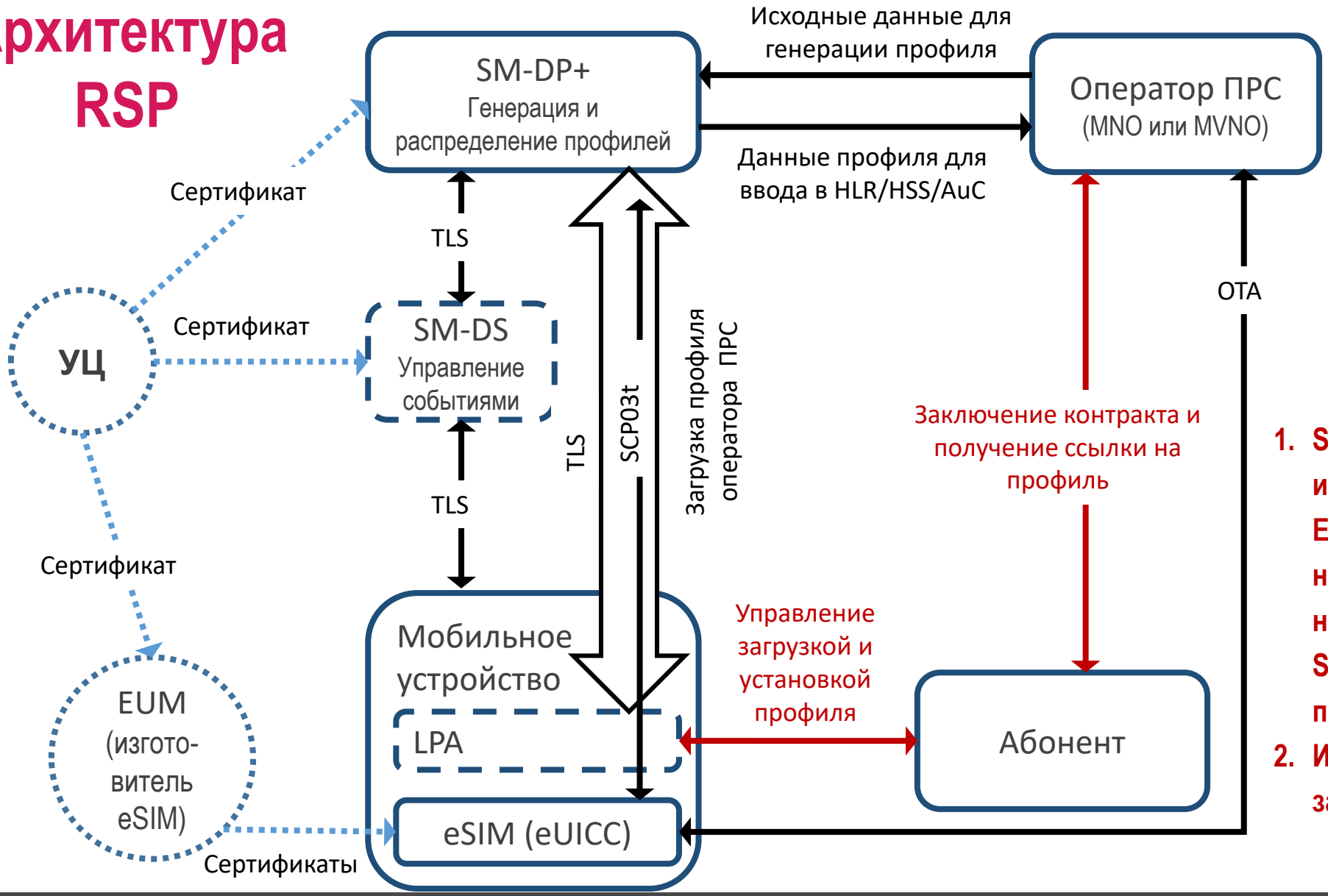
Распределение ключей и аутентификация в сети ПРС



Проблемы:

1. Должна быть обеспечена защита K_i и ключей OTA в USIM и HSS
2. Должна быть исключена утечка ключей на этапах производства и ввода данных в HSS
3. Должна быть обеспечена невозможность получения ключа K_i на основе порожденных от него ключей в ядре сети и сети радиодоступа
4. HSS должен быть подконтролен и располагаться на территории РФ.
5. OTA-платформа должна быть подконтрольна и располагаться на территории РФ

Архитектура RSP

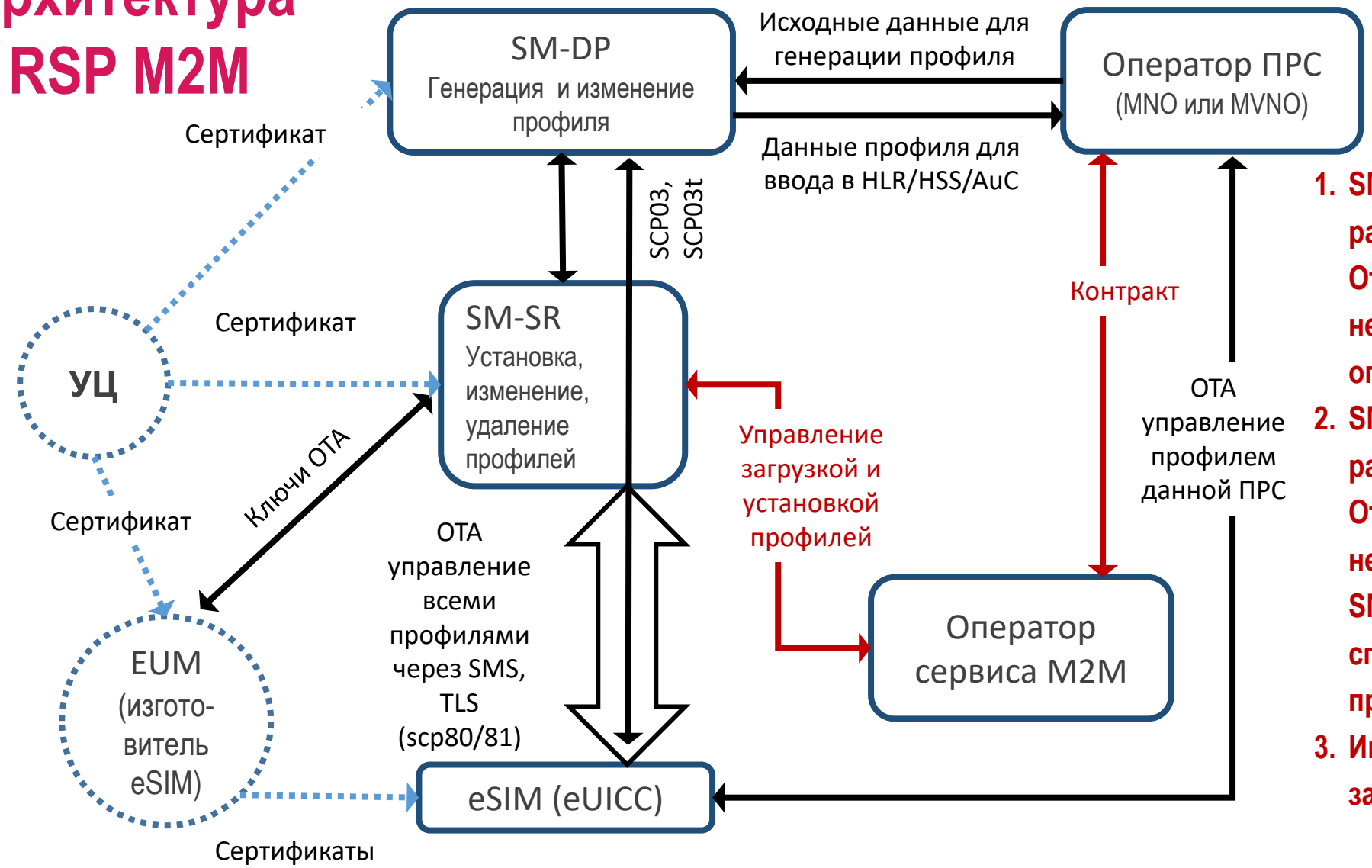


Открытое распределение ключей используется для обеспечения взаимной аутентификации eSIM/iSIM, SM-DP+ и SM-DS в целях загрузки профилей и установления TLS-соединений

Проблемы:

1. **SM-DP+ должен быть подконтролен и располагаться на территории РФ. Его отключение делает невозможной загрузку профилей новых абонентов. Также SM-DP+ является оператором персональных данных**
2. **Имеется риск отзыва сертификатов зарубежного УЦ**

Архитектура RSP M2M



Проблемы:

1. **SM-DP должен быть подконтролен и располагаться на территории РФ. Отключение SM-DP делает невозможной загрузку профилей операторов, которых он обслуживает**
2. **SM-SR должен быть подконтролен и располагаться на территории РФ. Отключение SM-SR делает невозможным управление eSIM/iSIM. SM-SR, управляемый нарушителем, способен реализовывать практически любые угрозы**
3. **Имеется риск отзыва сертификатов зарубежного УЦ**

Атаки и методы защиты

Цели атаки

- Ki абонента
- Передаваемая информация
- Постоянные идентификаторы (SUPI, IMSI, MSISDN)
- Другие данные профиля (регистрация, услуги и т.д.)
- Отказ в обслуживании

Дополнительно для технологии eSIM:

- Секретные ключи PKI
- Цифровой абонентский профиль
- Подложный SM-DP/SM-DP+

Объекты атаки

- USIM
- Изготовитель USIM
- Сеть радиодоступа
- HSS/AuC/UDM
- Другие элементы ядра сети ПРС
- OTA-платформа

Дополнительно для технологии eSIM:

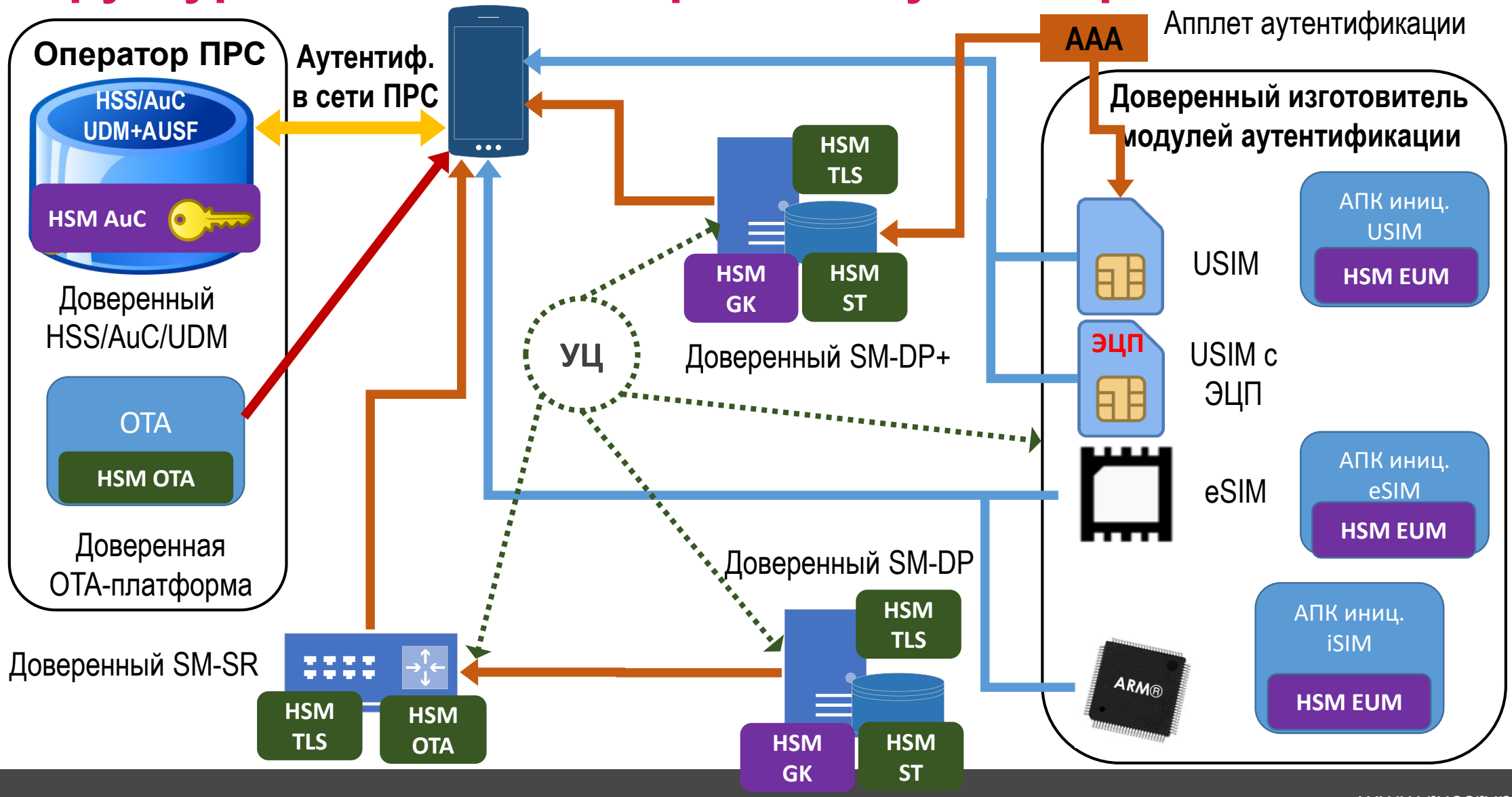
- eSIM/iSIM
- Изгтовитель eSIM/iSIM
- SM-DP/SM-DP+
- SM-SR
- Абонентский терминал
- Ссылка на скачивание
- Маршрутизаторы и DNS-серверы
- Удостоверяющий центр (УЦ)

Средства противодействия

- Отечественная криптография
- Сертифицированные СКЗИ для ключевых элементов (HSM)
- Сертифицированные СКЗИ для каналов связи
- Доверенные модули USIM/eSIM/iSIM, изготовленные доверенным производителем
- Доверенный HSS/AuC/UDM
- Доверенная OTA-платформа
- Доверенные SM-DP/SM-DP+ и SM-SR
- Размещение ключевых элементов на территории РФ
- Продуманные политики безопасности
- Отечественный УЦ

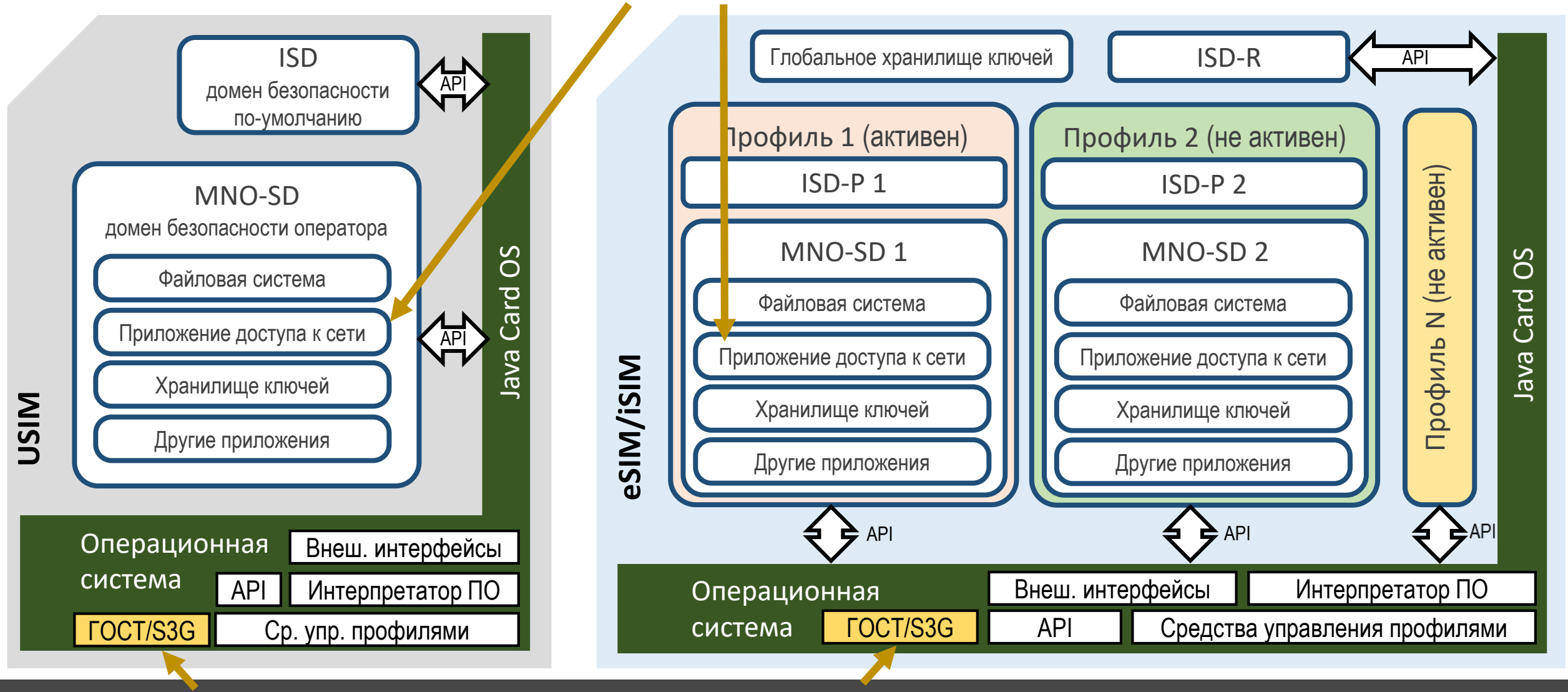
Способы атак – использование уязвимостей криптографии, НДВ, внутренний нарушитель, отзыв сертификатов УЦ

Структура системы доверенной аутентификации абонентов



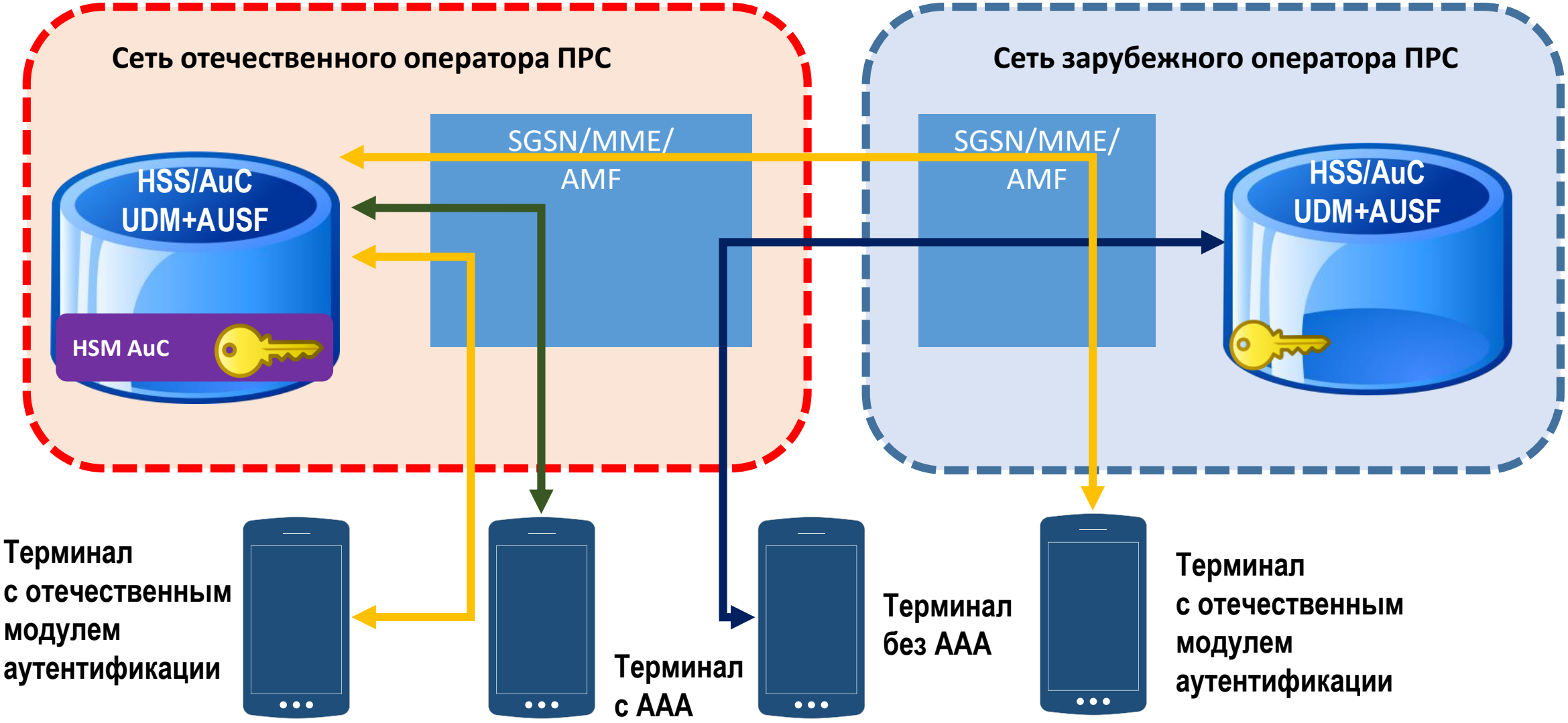
Архитектура SIM

Встраивание апплета аутентификации абонента (AAA) для возможности регистрации в сети абонентских терминалов с иностранными модулями

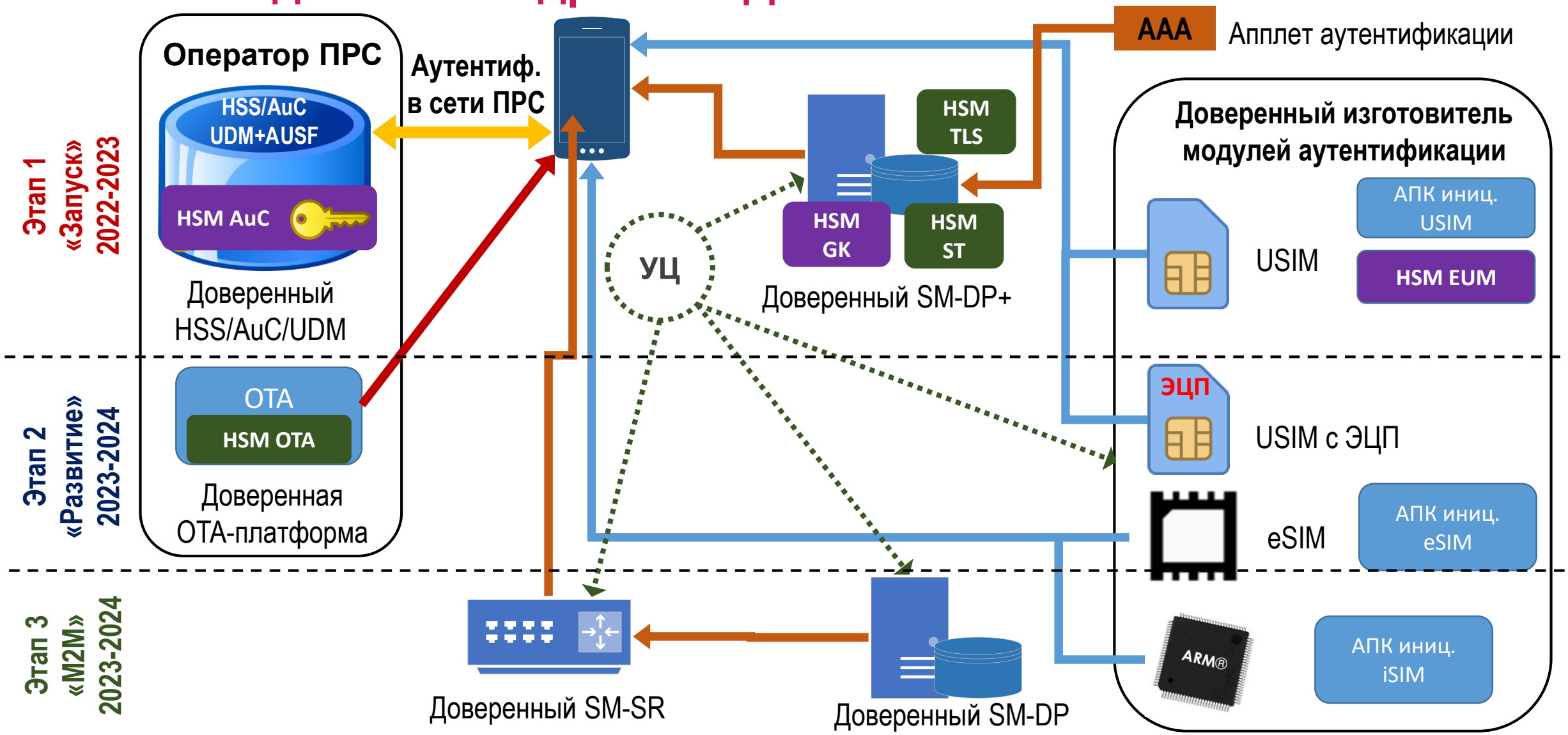


Встраивание отечественных криптографических алгоритмов в доверенные модули

Доверенная аутентификация в домашней сети и в роуминге



Этапы создания и внедрения СДАА



Макет СДАА

Макет HSM AuC

200 000 векторов аутентификации в секунду (S3G-128)
Питание 220 В/50 Гц
Габариты: 19” 2U

10GE

Интерфейс в соответствии с приказами № 275, 319 Минцифры

HSS

Протестированы:
1) SUMMA Networks NextGen
2) Ericsson
3) Protei HLR/HSS

Оператор ПРС

OTA-платформа

Макет сервера генерации профилей и HSM GK

Профиль
AAA

Терминал с eSIM

Терминал с USIM

AAA

АРМ

AAA
Макет апплета аутентификации

Сеть радиодоступа
2G GSM
3G UMTS
4G LTE

Результаты испытаний макета СДАА

Параметр/характеристика	Значение
Производительность макета HSM AuC при формировании векторов аутентификации S3G	225753 запросов/с
Установка апплета аутентификации абонента (AAA), реализующего S3G, в USIM	Успешно
Регистрация в сети оператора абонентского терминала с USIM	Успешно
Предоставление услуг для абонентского терминала с USIM	Голосовые вызовы, передача данных, SMS
Интеграция AAA, реализующего S3G, в профиль абонента, загружаемый в eSIM	Успешно
Регистрация в сети оператора абонентского терминала с eSIM	Успешно
Предоставление услуг для абонентского терминала с eSIM	Голосовые вызовы, передача данных, SMS
Среднее время выполнения команды аутентификации в eSIM с использованием российского алгоритма S3G	1,2 с

Вопросы

???

Контактная информация

Электронная почта:

emelyanov@systempb.ru

Телефон:

+7 812 468-15-61

Сайт:

www.systempb.ru

skzi.ru