

ГРУППА КОМПАНИЙ | СПБ

СРЕДСТВА ДОВЕРЕННОЙ АУТЕНТИФИКАЦИИ В СЕТЯХ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ

Емельянов-Гирс В.М. Заместитель генерального директора по НИР
ООО «Системы практической безопасности»

УГРОЗЫ БЕЗОПАСНОСТИ ДЛЯ АБОНЕНТА СЕТИ ПРТС

ГРУППА КОМПАНИЙ СПБ

1. Нарушение конфиденциальности данных абонента
2. Нарушение целостности данных абонента
3. Потеря доступности услуги для абонента
4. Потеря идентичности (аутентификация нарушителем от лица абонента, «клонирование» и т.д.)
5. Слежение за местоположением

Доверенная аутентификация является базовым механизмом



ДОВЕРЕННАЯ АУТЕНТИФИКАЦИЯ

ГРУППА КОМПАНИЙ СПБ

ДОВЕРЕННАЯ ГЕНЕРАЦИЯ КЛЮЧЕЙ АУТЕНТИФИКАЦИИ (ДОЛГОВРЕМЕННЫХ ОСНОВНЫХ КЛЮЧЕЙ АБОНЕНТОВ, ДОКА)

ПРОЦЕДУРА АУТЕНТИФИКАЦИИ И СОГЛАСОВАНИЯ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ S3G-256

СКЗИ ГЕНЕРАЦИИ КЛЮЧЕЙ (ГК)



Класс КВ

СКЗИ ЦЕНТРА АУТЕНТИФИКАЦИИ (ЦА)



Класс КВ

ДОВЕРЕННОЕ ПРОИЗВОДСТВО SIM/USIM

ДОВЕРЕННЫЙ МОДУЛЬ ИДЕНТИФИКАЦИИ SIM/USIM

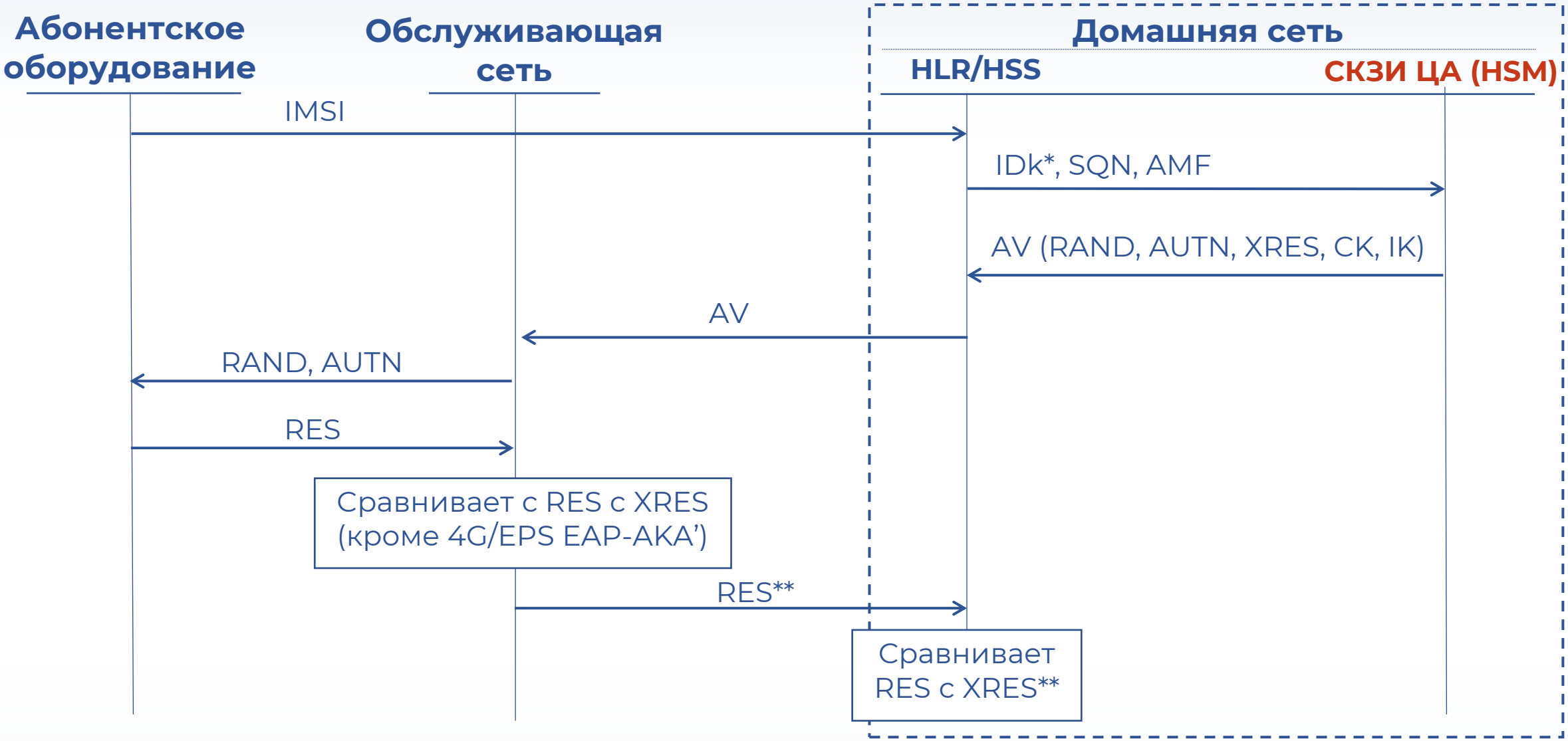


Класс КС3

СКЗИ ДЛЯ ПРОИЗВОДСТВА

Класс КВ

ПОТОК ДАННЫХ В ПРОЦЕДУРЕ АУТЕНТИФИКАЦИИ В СЕТЯХ 3G/4G



* Идентификатор ключа
** Только 4G/EPS EAP-AKA'

ГЕНЕРАЦИЯ И ВВОД ДОКА

ГРУППА КОМПАНИЙ СПБ

01 ДОКА являются криптографическими ключами. Организация, осуществляющая формирование ДОКА должна иметь соответствующую лицензию ФСБ России.

02 Формирование ДОКА может осуществлять Оператор сети ПРТС, Производитель модулей идентификации SIM/USIM или независимая от них внешняя организация. Один оператор связи может использовать в своих интересах несколько внешних центров генерации, либо собственных, либо их комбинацию.

03 Предполагается, что форматы хранения и передачи ДОКА будут едиными для оборудования разных вендоров, что обеспечит их взаимную совместимость

04 Операторы сетей ПРТС для ввода ДОКА в СКЗИ ЦА должны организовать орган криптографической защиты (ОКЗ) или использовать услуги сторонней организации, имеющей такой орган

ЗАКАЗ ДОКА

ГРУППА КОМПАНИЙ СПБ

Центр генерации ДОКА

СКЗИ ГК
Класс КВ



K+IDk

СКЗИ для производства
Класс КВ



Производитель SIM/USIM

K+IDk

K+IDk

IMSI+IDk

Заявка на генерацию ДОКА







Резервное хранилище

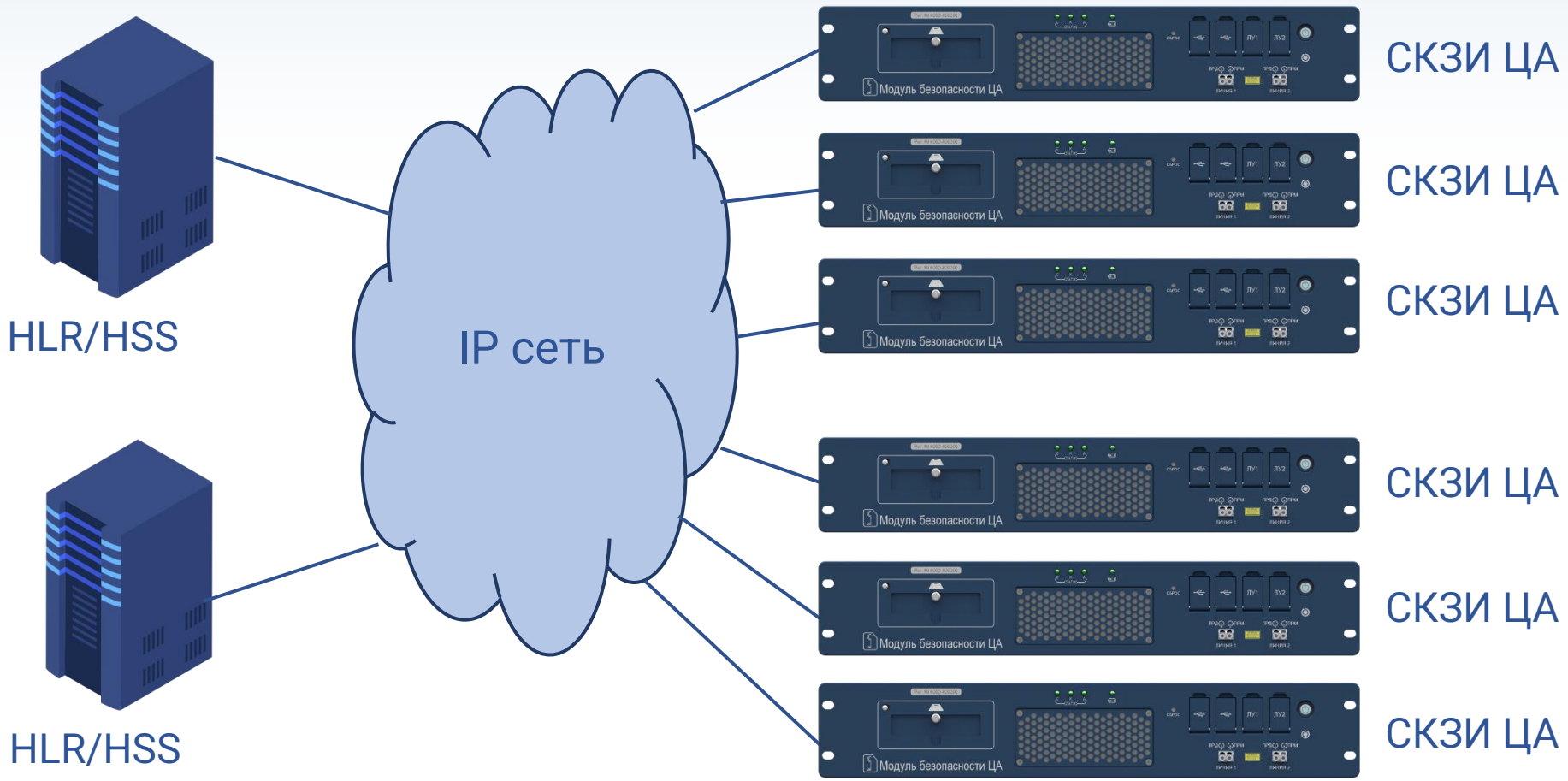
СКЗИ ЦА
Класс КВ

HLR/HSS

IMSI

Оператор сети ПРТС

СОПРЯЖЕНИЕ СКЗИ ЦА С HLR/HSS



01 Между HLR/HSS и СКЗИ ЦА интерфейс на основе UDP в соответствии с приказами Минкомсвязи № 160 от 26.06.2011 (с учётом приказа № 275 от 13.06.2018) и Минцифры № 319 от 25.06.2018.

02 Несколько СКЗИ ЦА могут использоваться как для резервирования, так и наращивания абонентской емкости.

ПЕРЕНОС ДОКА В ДРУГОЕ СКЗИ ЦА

ГРУППА КОМПАНИЙ СПБ

Центр генерации ДОКА

СКЗИ ГК
Класс КВ



K+IDk

K+IDk

Заявка на изготовление КД для другого СКЗИ + ключи



Резервное хранилище



СКЗИ ЦА
Класс КВ

Оператор сети ПРТС

01 Идентификатор ключа не меняется.

02 Резервный комплект расходуется - его необходимо обновить

РЕШЕНИЯ ГК «СПБ» ДЛЯ ДОВЕРЕННОЙ АУТЕНТИФИКАЦИИ

ГРУППА КОМПАНИЙ СПБ



МБ ЦА. СКЗИ центра аутентификации. Класс КВ.
Емкость: 10 000 000 ДОКА.
Производительность: не менее 20 000 запросов ACR/RCR (аутентификация и ресинхронизация) в секунду.
Сетевые интерфейсы: 2x1000Base-LX для подключения к HLR/HSS, 2x1000Base-LX для подключения терминала управления.
Управление: локальное, с использованием веб-интерфейса.



МБ ГК. СКЗИ для генерации ключей. Класс КВ.
Тип носителя для записи ДОКА: USB-накопитель.
Сетевые интерфейсы: 2x1000Base-LX для подключения терминала управления.
Управление: локальное, с использованием веб-интерфейса.

01 Модуль безопасности центра аутентификации сети 5G

- Генерация вектора аутентификации с использованием S3G-256 и S3G-5G
- Вычисление аутентификационной информации при ресинхронизации
- Функция SIDF: экспорт постоянного идентификатора SUPI из защищенного с помощью схемы ECIES идентификатора SUCI по запросу от UDM/UDR
- Вычисление $RAND_{UE}$ для алгоритма S3G-5G
- Соответствие требованиям к СКЗИ для класса не ниже КВ
- Надежное хранение ДОКА объемом до 10 млн.
- Надежное хранение ключевых пар домашней сети
- Производительность 20-50 тыс. запросов на аутентификацию в секунду (уточняется с учетом требований операторов связи)
- Интерфейс сопряжения с UDM в соответствии приказом Минцифры

МБ ЦА для сетей 5G – продукт эволюционного развития МБ ЦА для сетей 2-4G

02 Модуль безопасности для OTA-платформы

- Защищенное управление профилем USIM с использованием протокола СЕКУНДА
- Надежное хранение ключей дистанционного управления объемом до 10 млн.
- Соответствие требованиям к СКЗИ для класса КС3 или КВ (уточняется)



ООО «СПБ» (входит в Группу компаний «СПБ»)

г. Санкт-Петербург, ул. Политехническая, д. 22АБ

info@systempb.ru
+7 (812) 468-15-61

www.systempb.ru | www.skzi.ru | @GKSPB_skzi