РусКрипто

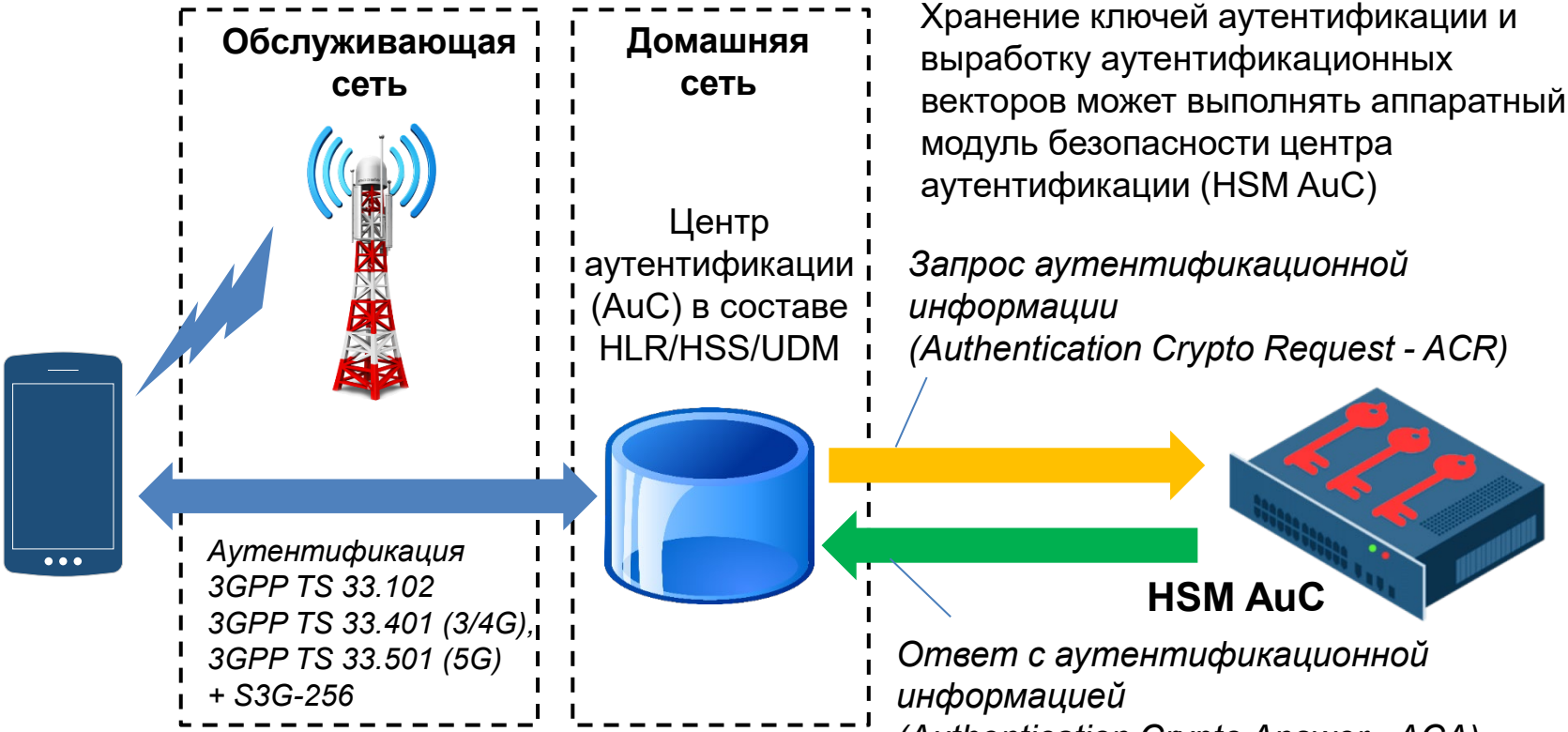
XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

РусКрипто

Аппаратный модуль безопасности центра аутентификации сети подвижной радиотелефонной связи с защитой ключей аутентификации на локальных мастер-ключах

Емельянов Виктор Михайлович, Мареева Елена Владимировна
ООО «Системы практической безопасности»

Аутентификация в сетях подвижной радиотелефонной связи (ПРТС)

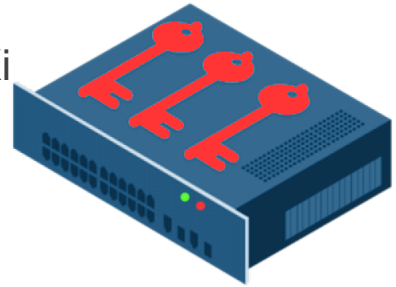


Хранение ключей аутентификации и выработку аутентификационных векторов может выполнять аппаратный модуль безопасности центра аутентификации (HSM AuC)

Запрос аутентификационной информации (Authentication Crypto Request - ACR)

Ответ с аутентификационной информацией (Authentication Crypto Answer - ACA)

Требования к HSM AuC



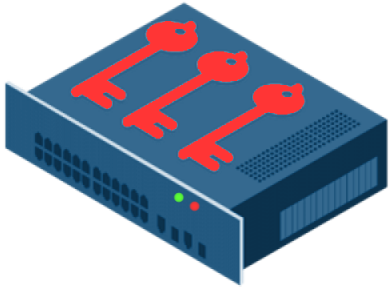
- Надежное хранение ключей аутентификации абонентов Ki в течение срока до 15 лет
- Производительность, достаточная для реализации протокола аутентификации в соответствии со спецификациями 3GPP
- Загрузка новых ключей в течение всего срока эксплуатации без снижения производительности
- Интерфейс сопряжения с HLR/HSS в соответствии с Приказами № 275 и 319 Минцифры (интерфейс сопряжения с UDM в сетях 5G не определен)
- Соответствие требованиям к СКЗИ для класса КА

По оценке «ТМТ Консалтинг», число абонентов сетей ПРТС в РФ по состоянию на ноябрь 2024 года составило 263 млн. (+1,9 % за год)*. Это обуславливает потребность в HSM AuC емкостью не менее 1 миллиона ключей Ki (точный объем хранимой ключевой информации определяется оператором сети ПРТС с учётом емкости HLR/HSS и их количества).

** «Телеком показал мобильность.» Коммерсант. https://www.kommersant.ru/doc/7404420*

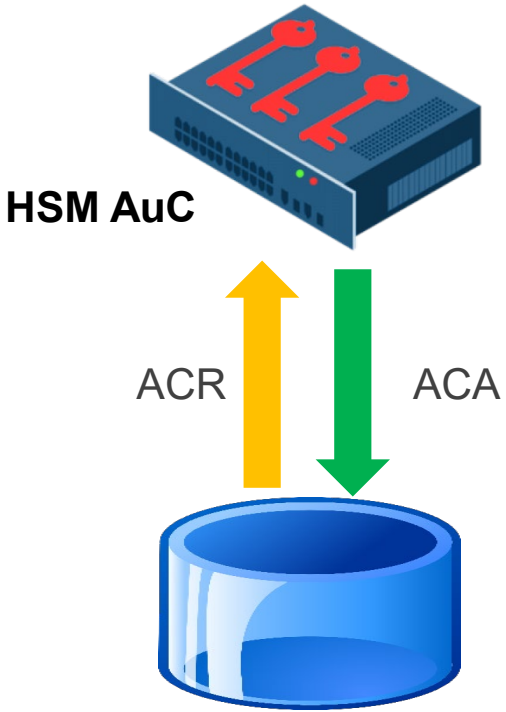
Использование локальных мастер-ключей

- Организация хранения большого объема ключей аутентификации Ki и поиска ключа с учётом обеспечения требований по быстродействию, надежности и безотказности оказываются сложными задачами как в части технической реализации, так и сопутствующих организационных мер

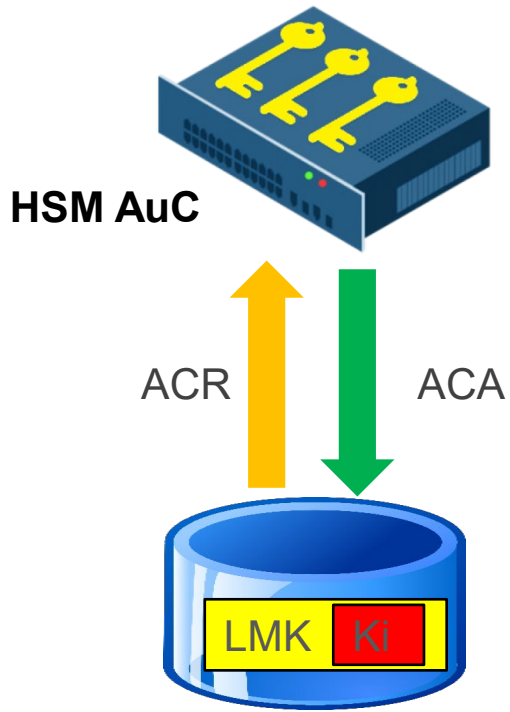


- В HSM платежных систем используется хранение ключей вне самого аппаратного модуля безопасности в виде шифрограмм (так называемых «keyblock»), зашифрованных на локальных мастер-ключах (LMK – Local Master Key)
- Аналогичная технология может быть применена и для HSM AuC

Хранение всего объема ключей аутентификации Ki в HSM AuC



Защита ключей аутентификации с использованием LMK



HSM AuC хранит LMK, число которых меньше, чем Ki

Ki хранятся в виде шифрограмм в HLR/HSS/UDM

ACR - Authentication Crypto Request

ACA - Authentication Crypto Answer

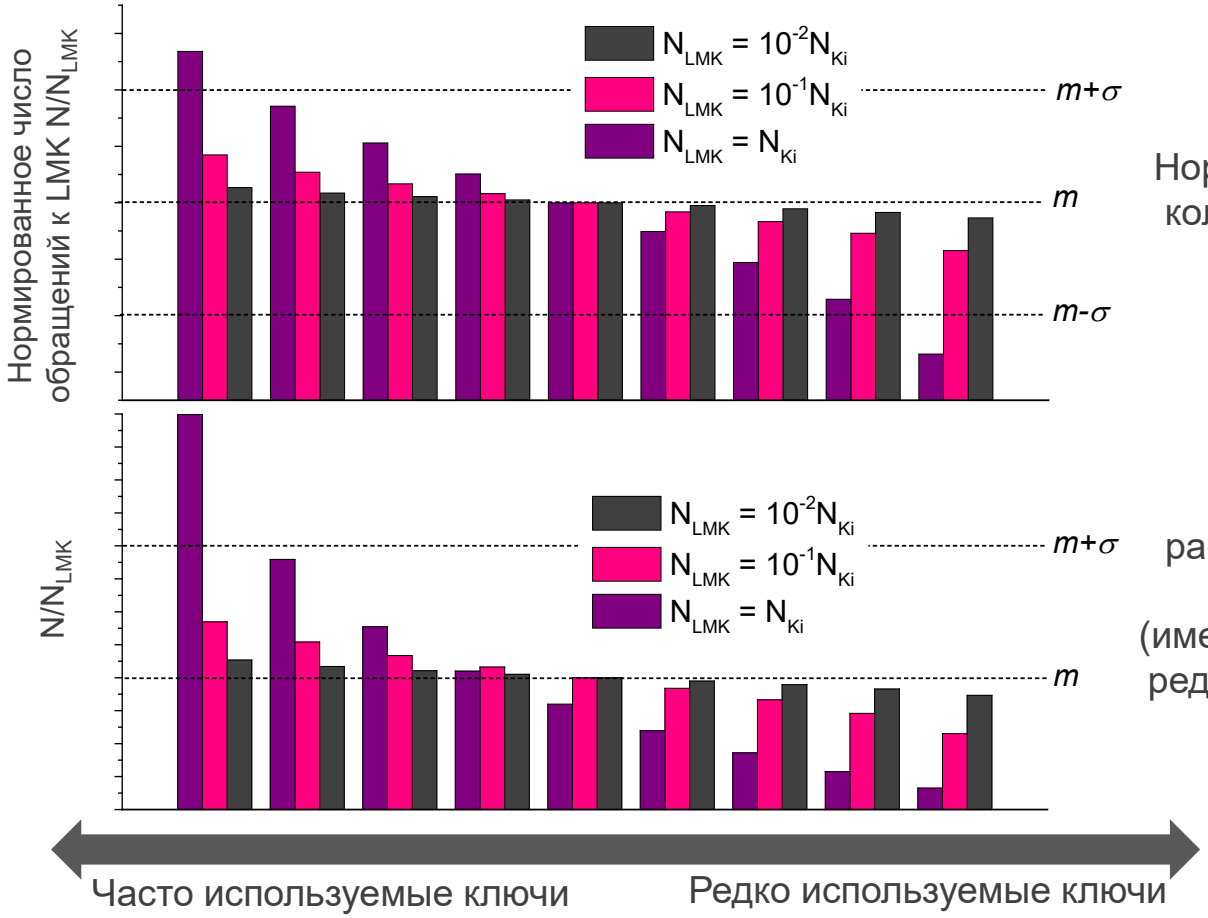
Актуальные проблемы использования LMK

Количество LMK должно определяться с учётом следующих факторов:

- Объем Ki в несколько миллионов уже сам по себе создает значительную нагрузку на LMK
- В процессе функционирования HSM AuC получает большое число запросов на выработку векторов аутентификации (более 100 тыс. на один Ki за его период использования). При этом в HLR/HSS/UDM должна обновляться определенная метаинформация, привязанная к Ki и также подлежащая защите на LMK. Также необходимо учитывать ПЭМИН
- Число LMK и организация хранения Ki на них должны обеспечивать приемлемые эксплуатационные характеристики HSM AuC

Допустимое количество ключей аутентификации, защищаемых на одном LMK, а также частота их смены зависит от емкости и модели применения HSM AuC, особенностей алгоритмов обработки, используемой ключевой системы и определяется по результатам криптографического анализа. Тем не менее, имеются фундаментальные закономерности использования мастер-ключей, которые будут показаны на следующих слайдах.

Распределение нагрузки на LMK



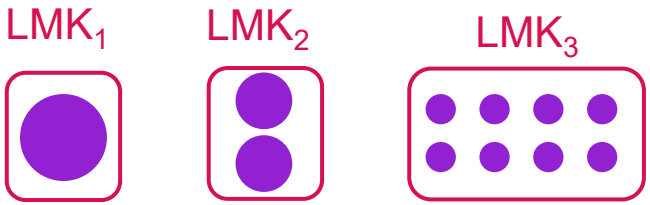
Нормальное распределение количества обращений к Ki

Экспоненциальное распределение количества обращений к Ki (имеется большое количество редко используемых ключей)

РусКрипто

Оптимизация нагрузки на LMK

Вариант 1 группировки:



Диаметр круга пропорционален частоте использования защищаемого ключа:

Часто используемые ключи

Редко используемые ключи

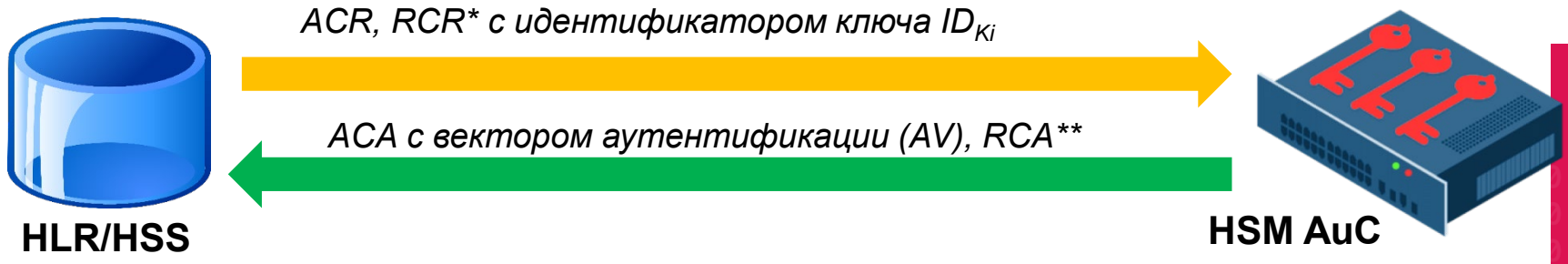
Вариант 2 группировки:

Группировка часто используемых ключей с редко используемыми сохраняет равное число ключей, защищенных на одном LMK

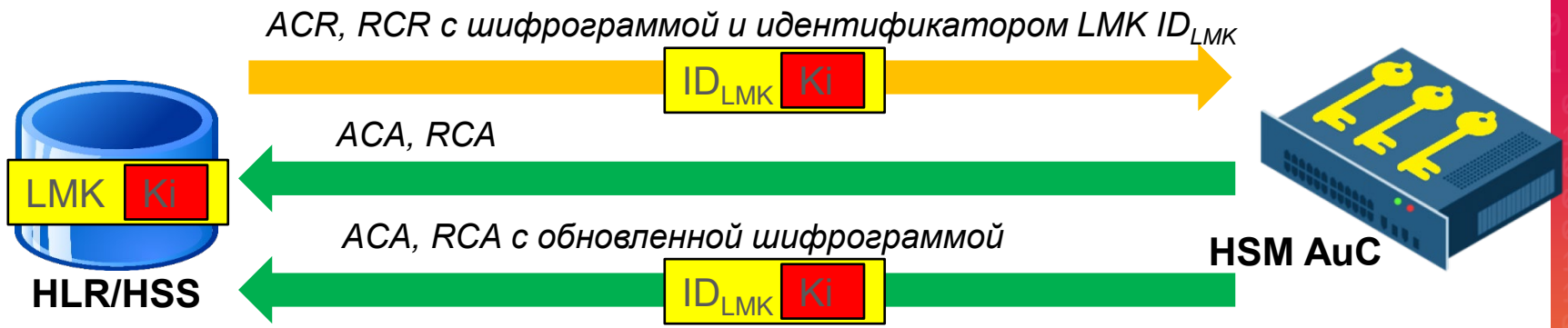
Оба подхода теоретически позволяют выровнять частоту обращения к разным LMK

Интерфейс взаимодействия HLR/HSS с HSM AuC

Без использования LMK:



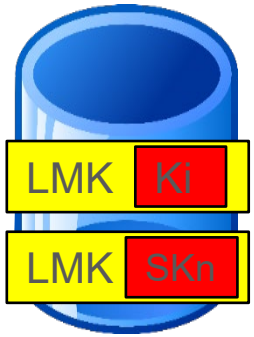
При использовании LMK:



*RCR - Resynchronization Crypto Request **RCA - Resynchronization Crypto Answer

Интерфейс взаимодействия UDM с HSM AuC при использовании LMK

РусКрипто



UDM

HSM AuC

ACR, RCR с шифрограммой и идентификатором LMK ID_{LMK}

ID_{LMK} Ki

ACR, RCA

ACA, RCA с обновленной шифрограммой

ID_{LMK} Ki

Запрос на расшифрование SUCI с шифрограммой секретного ключа сети ПРТС SKn и идентификатором LMK ID_{LMK}

ID_{LMK} SKn

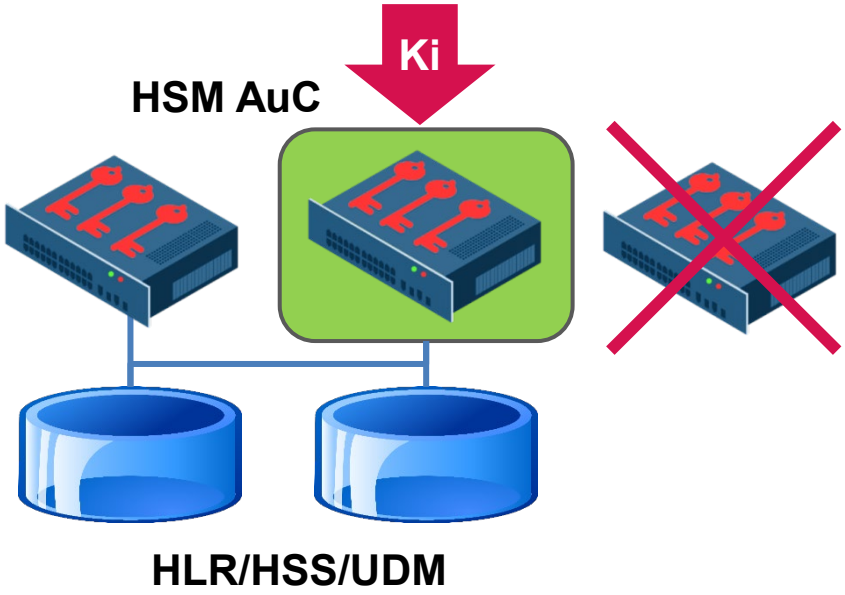
Ответ с SUPI

Ответ с SUPI и обновленной шифрограммой

ID_{LMK} SKn

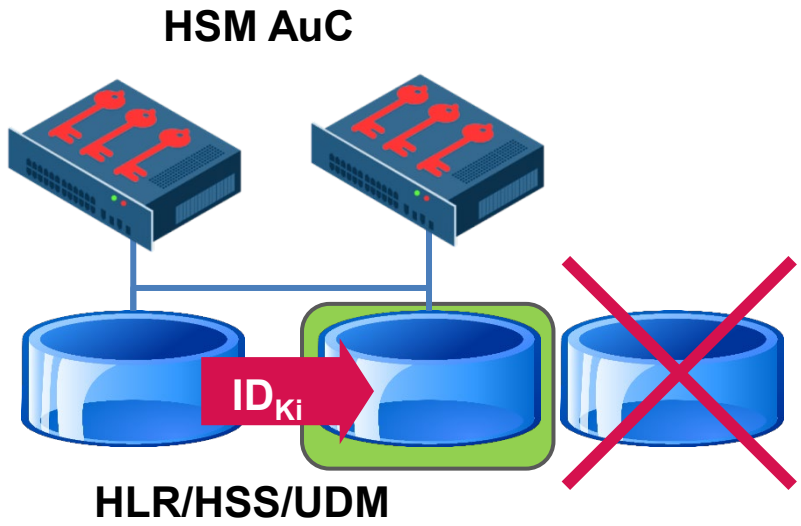
Резервирование и восстановление

Отказ HSM AuC



При замене отказавшего HSM AuC на новый необходимо ввести полный объем ключевой информации

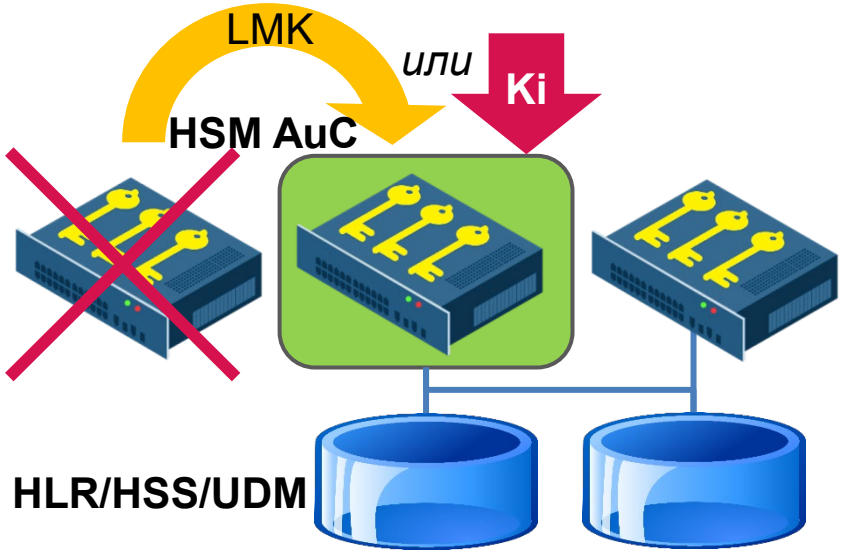
Отказ HLR/HSS/UDM



При замене отказавшего HLR/HSS/UDM в новый необходимо ввести идентификаторы ключей ID_{Ki} вместе с остальной абонентской информацией

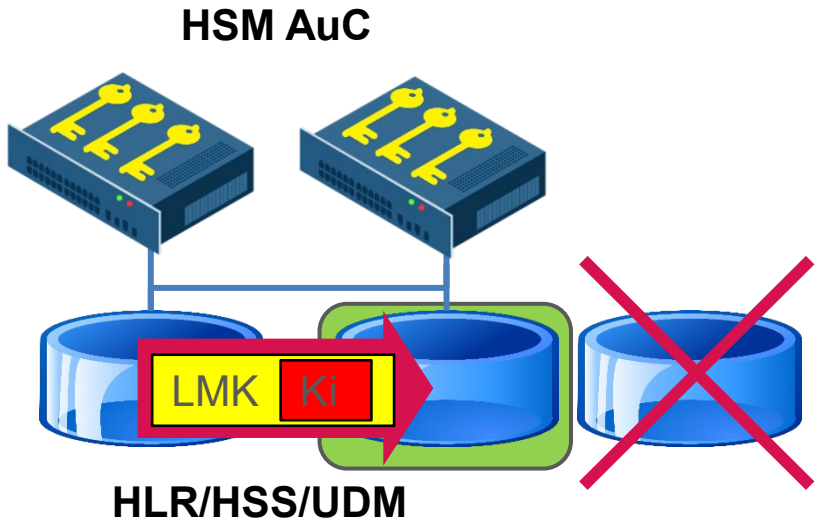
Резервирование и восстановление

Отказ HSM AuC



- Можно загрузить полный объем Ki и обновить шифрограммы
- Можно только ввести LMK (если они были резервированы)

Отказ HLR/HSS/UDM



При замене отказавшего HLR/HSS/UDM в новый необходимо ввести шифрограммы ключей вместе с остальной абонентской информацией

Выводы

- Технология хранения ключей аутентификации в сети ПРТС вместе с остальной абонентской информацией в HSS или UDM в виде шифрограмм, защищенных с использованием LMK, применима для HSM AuC. Она позволяет сократить объем хранимой ключевой информации в HSM AuC, что позволит упростить его эксплуатацию, повысить надежность и безотказность
- Хранение ключей аутентификации абонентов Ki вне HSM AuC позволяет избежать расходования его ресурсов на редко используемые ключи аутентификации, а также упрощает процедуру удаления ключей
- В HSM AuC могут быть реализованы несложные алгоритмические меры, позволяющие достичь близкого к равномерному распределения нагрузки между LMK
- Процедуры резервирования и восстановления HSM AuC при использовании LMK не имеют существенных отличий от процедур, используемых при хранении в HSM ключей аутентификации

Проблемные вопросы

- Предлагаемая концепция может быть реализована при условии взаимодействия разработчиков HLR/HSS/UDM с разработчиками HSM AuC
- Описанный в приказах Минцифры № 275 и 319 интерфейс взаимодействия HLR/HSS с HSM AuC (H-интерфейс) не позволяет реализовать взаимодействие с HSM AuC, обеспечивающим защиту Ki с использованием LMK. Для сопряжения HSM AuC с UDM в сетях 5G в настоящее время интерфейс не определен. Целесообразно уточнение интерфейса сопряжения HLR/HSS/UDM с HSM AuC для возможности внедрения предлагаемой концепции построения центра аутентификации

Дальнейшие работы

I. Обоснование стойкости предлагаемой схемы защиты ключей аутентификации абонентов Ki с использованием LMK и разработка ключевой системы с учётом следующих факторов:

- количества абонентов в HLR/HSS/UDM;
- частоты и предельного количества запросов к ключам Ki;
- ПЭМИН.

II. Разработка протокола взаимодействия HLR/HSS/UDM с HSM AuC, включающего:

- запросы и ответы ACR, RCR, ACA, RCA и др., содержащие шифрограммы ключей, защищаемых с использованием LMK;
- специализированные команды для реализации функций в сетях 5G;
- команды для запроса и передачи диагностической информации.

РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ