конференция
РусКрипто 2022

О дополнительных требованиях к отечественным криптографическим механизмам доверенных элементов безопасности, внедряемых в технологию ESIM

Дрелихов В.О.
АО «ИТМиВТ»

Обычные SIM-карты - загрузка ПО и профиля абонента загружаются при изготовлении SIM-карты (инициализация и персонализация SIM-чипов) и не подлежат изменению.

eSIM – это разработанный ассоциацией GSMA стандарт, позволяющий на интегрированное с оборудованием абонента электронное устройство (eSIM-микрочип eUICC) загружать и хранить профили различных Операторов РПСС и подключать оборудование абонента к сотовой связи через различных Операторов РПСС.

Абонентские профили конкретных операторов связи могут загружаться в eSIM через сеть Интернет по радиоканалу.

GSMA: eSIM M2M,
eSIM Consumer.

Общие принципы – использование платформы Subscription Manager. SM-DP (Subscription Manager Data Preparation) хранит цифровые профили абонентских SIM-карт, по запросу формирует данные от Оператора РПСС (IMSI, параметры алгоритма аутентификации, персональные ключи - OP, OPc, KI, коды защиты PIN, PUK и др.), загружаемые по радиоканалу в eSIM-чип.

Пример. Загрузка абонентского профиля для eSIM M2M

1. Устройство (оборудование) абонента с eSIM-чипом включено и зарегистрировано в мобильной сети. Регистрация в мобильной сети выполняется с помощью загрузочного профиля (bootstrap), bootstrap входит в состав СПО eSIM-чипов.

2. Устройство взаимодействует с оборудованием Оператора РПСС. Подсистема Оператора принимает решение и информирует SM-DP о готовности к загрузке заданного абонентского профиля на заданный eSIM-чип.

3. SM-DP по каждой заявке формирует и передаёт запрос на загрузку на SM-SR.

4. SM-SR (Subscription Manager Secure Routing) – персонально для каждого eSIM-чипа формирует специальное служебное SMS с набором команд загрузки абонентского профиля и отправляет SMS для заданного eSIM-чипа через SMS-центр Оператора.

5. eSIM-чип, получив SMS, выполняет последовательность команд загрузки. Устанавливается HTTP подключение к SM-DP через SM-SR и загружается по радиоканалу абонентский профиль. eSIM-чип переключается на новый профиль и регистрируется в подсистеме Оператора РПСС. По готовности подсистемы абонент получает соответствующую информацию.

Доверенность механизмов подключения и доставки профиля

Доверенность процесса инициализация в eSIM-чип СПО и служебной информации.

Доверенность процесса интеграции eSIM в оборудование.

Доверенность ключевой информации технологии PKI, используемой в обеспечении безопасности процесса загрузки абонентского цифрового профиля.

Доверенность криптографических механизмов защиты от НСД и имитозащиты, используемых для передачи профиля абонента по радиоканалу.

Целевые функции для долговременных ключей аутентификации

Загрузка и хранение долговременных ключей аутентификации – SM-DP, AuC.

Выработка аутентификационных данных, предназначенных для взаимной аутентификации и формирования сеансового ключа (системы ключей различного назначения, используемых в сеансе связи).

Целевые функции – обеспечение защиты долговременных ключей SIM карт/абонентских профилей от НСД, обеспечение имитозащиты долговременных ключей .

SM-DP, AuC - СКЗИ, класс защищенности – КА.

Подсистемы криптографической защиты в СКЗИ

1). Защищенный информационный обмен в сети связи с другими СКЗИ. Целевые функции защиты – аутентификация абонента, защита от НСД и имитозащита передаваемой информации;

2). Защита от НСД и имитозащита ключевой информации при её загрузке, хранении или обработке в СКЗИ.

3). Аутентификация операторов и администраторов СКЗИ.

Различия в сценариях реализации атак.

Для 1) – активное воздействие. Доступ к каналу связи в процессе эксплуатации. Участие в информационном обмене, формирование ложных запросов и т.п.

2) и 3) – криптография для внутреннего пользования.

Для 2) – анализ содержимого электронных компонентов. Доступ к ним после срабатывания системы обнаружения НСД.

Рекомендации по стандартизации Р 1323565.1.012-2017 «Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации»

…

6.1.3 В качестве составной части СКЗИ всех классов должна быть реализована система защиты от несанкционированного доступа к используемой в СКЗИ ключевой … информации.

6.1.4. В ходе тематических исследований СКЗИ должны быть определены технические характеристики СКЗИ и их предельные значения, позволяющие обеспечить выполнение предъявляемых к СКЗИ требований.

6.1.5 В СКЗИ всех классов должен быть реализован контролирующий механизм, … блокирующий работу СКЗИ при достижении предельных значений технических характеристик СКЗИ.

6.1.7 В СКЗИ любого класса должна быть предусмотрена реализация блокирования работы СКЗИ при достижении предельных значений технических характеристик СКЗИ.

А.4.5 СЗКИ должны противостоять атакам, использующим технические каналы распространения информативных сигналов.

1. Срок действия долговременных ключей абонентов сети – не менее срока действия SIM-карты. Для eSIM-чипа - срок действия сопоставим со сроком использования оборудования.

В процессе эксплуатации СКЗИ технические характеристики могут превысить предельно допустимые границы для «нагрузки на ключ». Контроль технических параметров, в данном случае – количество вычислений алгоритмом S3G аутентификационных данных с использованием долговременного ключа.

Максимальное количество долговременных ключей абонентов в сети – до 4 млрд.

Максимальное количество параметров, контролируемых нагрузки на ключи – до 4 млрд.

При срабатывании системы обнаружения НСД необходимо сохранить в энергонезависимой памяти массив контролируемых параметров в имитозащищенном виде.

Как быть при отключении внешнего питания СКЗИ?

Алгоритм S3G основан на использовании функции вычисления хэш-значения длины 512 двоичных разрядов. Для обеспечения длительного срока использования долговременных ключей аутентификации **необходимо реализовать алгоритмические меры защиты ключевой информации.**

Ключи абонентов должны храниться с обеспечением защиты:

– в энергонезависимой памяти (защита от НСД, имитозащита),

– в ОЗУ (защита от НСД).

При срабатывании системы обнаружения НСД необходимо защитить от НСД массив ключей в ОЗУ.

AUC обслуживает до 5 млн запросов в секунду. При непрерывной работе AuC в течение 3 лет может быть сформировано $4.7\ 10^{14}$ производных ключей доступа к ключам абонентов для вычисления аутентификационных данных.

Применительно к AuC необходимо использование криптографических примитивов, позволяющих **выполнить требования по защите** от ПЭМИН в условиях повышенной нагрузки на ключи защиты от НСД. Необходимо **реализовать алгоритмические меры защиты ключевой информации**.

Минимизация ресурсов при маскировании данных – актуальная сложная задача.

S. V. Matveev, “GOST 28147-89 masking against side channel attacks”, Матем. вопр. криптогр., 6_2 (2015), 35–43.

T.A. Lavrenteva, S.D. Matveev, Side-Channel Attacks Countermeasure Based on Decomposed S-Boxes for Kuznyechik, CTCrypt’2020.

Вопросы

???