UOT 004.71 DOI: 10.25045/jpit.v11.i1.14

Джафарзаде К.Е.
Институт Информационных Технологий НАНА, Баку, Азербайджан
kamran@science.az

ТЕХНОЛОГИЯ eSIM: ТЕКУЩЕЕ СОСТОЯНИЕ, АРХИТЕКТУРНЫЕ ПРИНЦИПЫ И ВОПРОСЫ БЕЗОПАСНОСТИ

Поступила: 10.06.2019 Исправлена: 25.06.2019 Принята: 25.10.2019

В статье сделан обзор архитектуры технологии eSIM, рассматриваются основные типы коммуникационных профилей и их роль в управлении подписками SM-DP и SM-SR. А также проводится анализ алгоритма переключения профилей, использующийся в технологии eSIM. В нынешнее время традиционная SIM имеет достаточно уязвимостей в плане надежности и безопасности использования в отличие от встроенной SIM, где безопасность технологии основана на аппаратном элементе, вследствие чего считается более надежной и защищенной. Отсутствие удаленного управления и низкий уровень безопасности при хранении учетных данных операторов дают повод задуматься над кардинальным решением данных проблем через применение новой технологии виртуализации SIM-карт. В результате исследования также было установлено наличие дальнейших перспектив внедрения технологии eSIM на рынок мобильных устройств и полноценной замены ее предшественника.

Ключевые слова: *eSIM, встроенная SIM-карта, eUICC, менеджер подписки, профиль, MNO, SM-DP, SM-SR, QR-код.*

Введение

Несмотря на то, что SIM-карта (*англ. Subscriber Identification Module*) была создана для максимального удобства использования мобильных устройств, на данное время она является основной преградой для рынка смартфонов. Причина заключается не только в ее размере, но и в самой идее, так как она не обеспечивает достаточного уровня безопасности при хранении учетных данных операторов. Кроме того, традиционная SIM-карта имеет ряд недостатков, начиная с обычной проблемы безопасности, когда злоумышленник может получить полный доступ к данным пользователя в разных сервисах, просто переставив SIM-карту в другое устройство. Кроме неудобства и невыгодности следует отметить привязку пользователя к одному оператору, когда достаточно абоненту выехать за пределы страны, как он сразу сталкивается с проблемами связи в виде невыгодных тарифов в роуминге и необходимости подключения к местному оператору. А так как у современного пользователя в большинстве случаев бывает несколько устройств, которые он постоянно использует, то для этого приходится для каждого устройства в отдельности приобретать карту [1, 2].

Для решения вышеуказанных проблем более перспективным решением является внедрение в индустрию мобильной связи технологии виртуализации SIM-карт. В отличие от традиционной SIM-карты, безопасность технологии встроенной SIM (*англ. embedded-SIM, eSIM*) основана на аппаратном элементе и поэтому считается более надежной и защищенной. Подключение поддерживающих eSIM устройств к мобильной сети осуществляется без приобретения встраиваемой карты – оператор и тариф выбираются в настройках самого устройства. Как и вставляемые карты, предшествующие им, eSIM содержат все учетные данные, необходимые для подключения к мобильной сети.

Кардинально решить вопрос миниатюризации мобильных устройств ассоциацией GSMCA (Global System for Mobile Communications Association) было предложено в 2014 году посредством технологии виртуализации SIM-карт (*англ. Remote SIM Provisioning*). В рамках данной технологии SIM-карта в виде программируемой микросхемы устанавливается в плату самого устройства в процессе производства. Оператор мобильной

связи предоставляет клиенту не SIM-карту, а набор зашифрованных данных, которые клиент вводит в свое устройство. Эта технология позволяет не только отказаться от слотов под SIM-карты и самих карт, но и устанавливать в одно устройство несколько профилей операторов, решив проблему нескольких SIM-карт [3].

eSIM работает так же, как обычная SIM-карта с запрограммированными уникальными идентификаторами UICC (Universal Integrated Circuit Card) и IMS (Instant Messaging Service). Сетевое решение, использующее технологию eSIM, также известную как встроенная универсальная интегральная карта (англ. Embedded Universal Integrated Circuit Card, eUICC), может широко применяться в различных вариантах интернет-вещей, включая устройства Mi-Fi, умные часы, интеллектуальные наушники и счетчик, трекер, рекламный плеер, устройства видеонаблюдения и т.д. С начала 2016 года многие известные корпорации, такие как Apple, Google, Samsung, LG, Huawei, начали внедрять новейшую разработку, тем самым выпустив на рынок телефоны и ряд умных устройств с поддержкой eSIM. Несмотря на свои преимущества и достижения, eSIM все еще не вошла в широкий обиход и пока не все страны поддерживают эту технологию [4].

Архитектура eSIM

Сеть оператора сотовой связи (*англ. Mobile Network Operator, MNO*) в активированном профиле используется для коммуникации. Все профили кроме текущего используемого отключены или не распознаются устройством. В обычных SIM-картах уникальный серийный номер (англ. Integrated Circuit Card Identifier, ICCID) используется в качестве уникального ключа для идентификации SIM-карты, но в случае с eUICC ICCID − это ключ, используемый для идентификации профилей, и определяется новый идентификатор, называемый eUICC-ID, который используется в качестве уникального ключа для eSIM [5].

Ассоциация GSMA определяет два основных типа профилей:

- Настраиваемый профиль. Это коммуникационный профиль, изначально сохраненный в eUICC при его отправке. Это профиль ограниченного применения, используется только для загрузки и переключения операционных профилей, описанных далее.
- Операционный профиль. Это коммуникационный профиль для подключения к корпоративным серверам или к Интернету. Он также может выполнять роли, предоставленные настраиваемым профилем.

eSIM не выполняет переключение профилей как простая функция у SIM-карты, а переключает профили на основе предписаний от оборудования, называемого менеджером подписки (англ. Subscription Manager, SM). Менеджер подписки поддерживается и управляется оператором мобильной связи. Общая архитектура eSIM, основанная на менеджере подписки, показана на рисунке 1 на примере переключения профилей в eUICC [6].

В eUICC должен быть сохранен по крайней мере один профиль, чтобы включить функцию OTA (Over-The-Air), и один из сохраненных профилей должен быть включен. К примеру, включенный профиль использует для коммуникации сеть MNO A. Когда пользователь переключает профили, инструкция по переключению отправляется в менеджер подписки. В то время, когда профиль для переключения отсутствует в eUICC, то сначала загружается профиль. Когда он получает инструкцию по переключению, eUICC как внутренний процесс выполняет переключение активированного профиля. После завершения переключения он использует сеть MNO B для отправки уведомления в менеджер подписки о завершении данного процесса. Эта же процедура используется для возврата к исходному MNO A или к какому-нибудь другому MNO C [7].

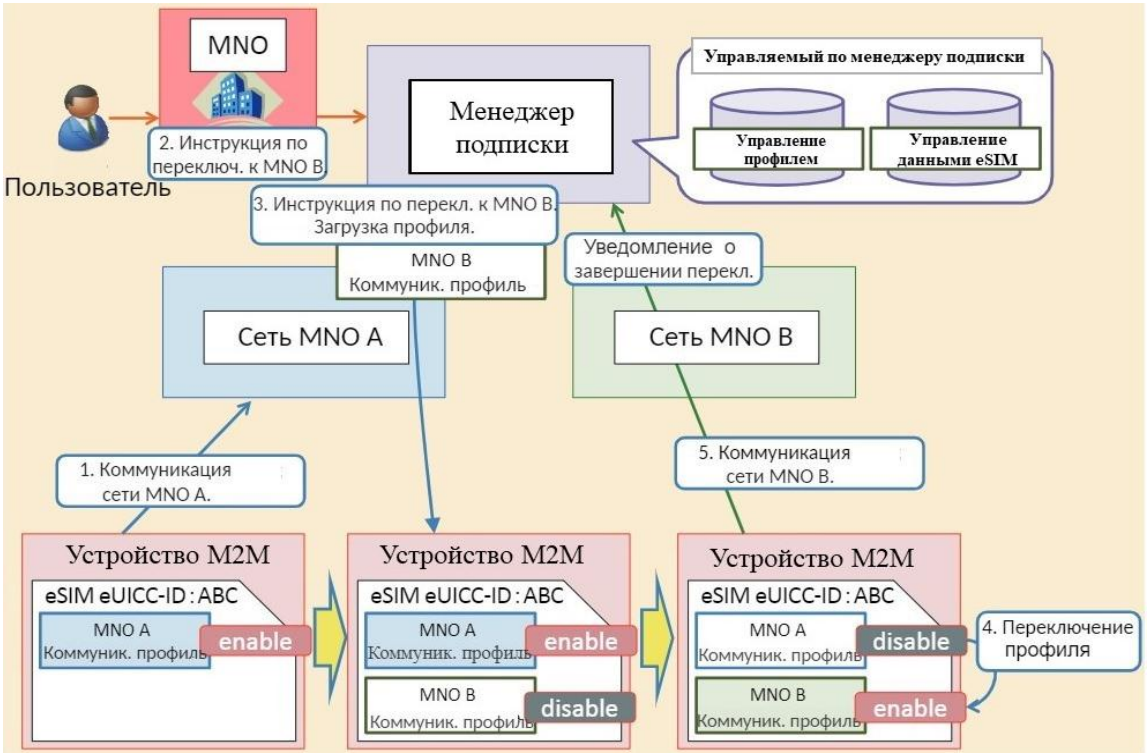

Рис.1. Переключение профилей при помощи менеджера подписки

Как упоминалось выше, переключение профилей осуществляется с помощью функциональности менеджера подписки. Менеджер подписки выполняет две роли: менеджер подписки подготовки данных *(англ. Subscription Manager Data Preparation, SM-DP*) и менеджер подписки безопасной маршрутизации (*англ. Subscription Manager Secure Routing, SM-SR*). На рисунке 2 подробно описаны эти функции менеджера подписки.

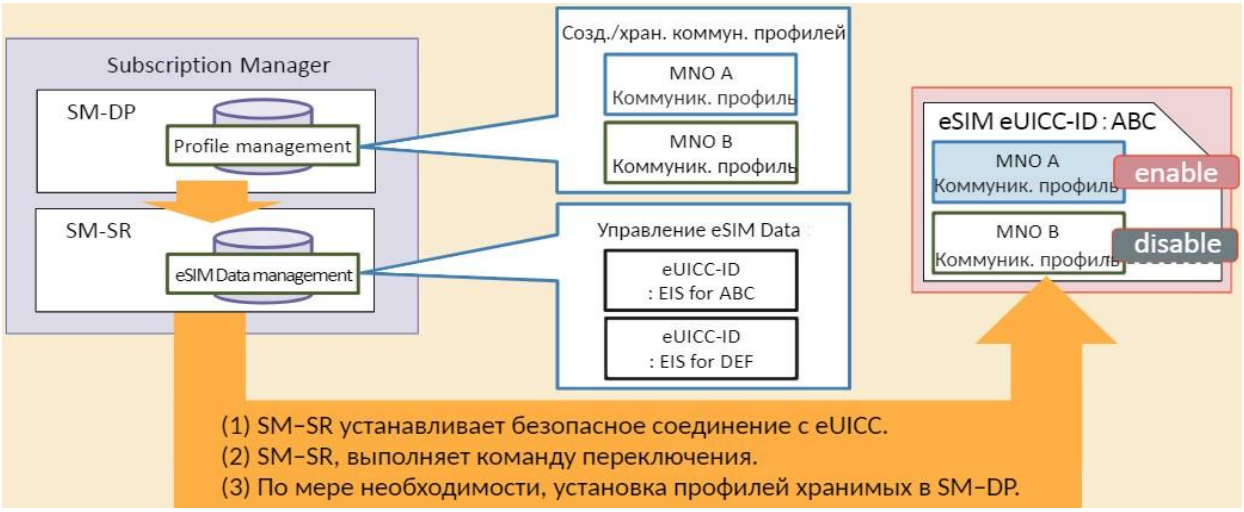

Рис.2. Функции менеджера подписки

- Роль SM-DP – безопасно создает и хранит коммуникационные профили. Он получает информацию, необходимую для создания профиля (MSISDN, IMSI и т.д.) от MNO, и создает профиль связи. Затем он сохраняет свой созданный профиль.
- Роль SM-SR – играет роль при установлении безопасной связи с eUICC. Профили связи, хранящиеся в eUICC, являются строго конфиденциальной информацией и требуют механизма для предотвращения их чтения или изменения вне системы. По этой причине безопасная среда создается путем разделения SM-DP, который создает

профили, и SM-SR, который устанавливает связь с eUICC. Для установки безопасной связи с eUICC в SM-SR используется EIS (eUICC Information Set). EIS имеет ключевую информацию для доступа к eUICC (учетные данные управления платформой) и информацию о состоянии, к примеру, об активности каждого профиля [6, 8, 9].

Учетные данные управления платформой позволяют SM-SR получать безопасный доступ к eUICC и выполнять инструкции по переключению включенного профиля.

Преимущества и вопросы безопасности eSIM

Технология eSIM имеет ряд следующих преимуществ [10]:

- Занимает меньше места. Нет нужды в отдельном слоте для SIM-карты, а значит, проще обеспечить пыле- и влагозащиту, а также сделать корпус тоньше, что также важно для различных портативных устройств.
- Быстрое подключение. Нет необходимости идти в офис поставщика услуг для получения SIM-карты или смены ее на новую, другого оператора. Достаточно всего лишь переключить опцию в меню устройства, просканировав специальный QR-код (Quick Response Code) нужного оператора.
- Возможность использования более двух профилей. Можно хранить несколько профилей мобильной сети и быстро переключаться между ними по мере необходимости.
- Надежность. eSIM гораздо менее подвержен механическим повреждениям, поскольку он встроен в плату устройства и недоступен без его взлома.
- Удаленное управление. Позволяет минимизировать кражи смартфонов, поскольку идентификатор позволяет удаленно блокировать и администрировать устройство при помощи встроенного чипа.
- Эффективность. eSIM более эффективен при приеме и передаче сигналов.

Несмотря на достаточное число преимуществ данной технологии, рынок устройств с поддержкой традиционной SIM за 2018 год, исходя из данных исследовательской компании IHS Markit, все еще значительно преобладает над рынком eSIM, как показано на рисунке 3 [11, 12].

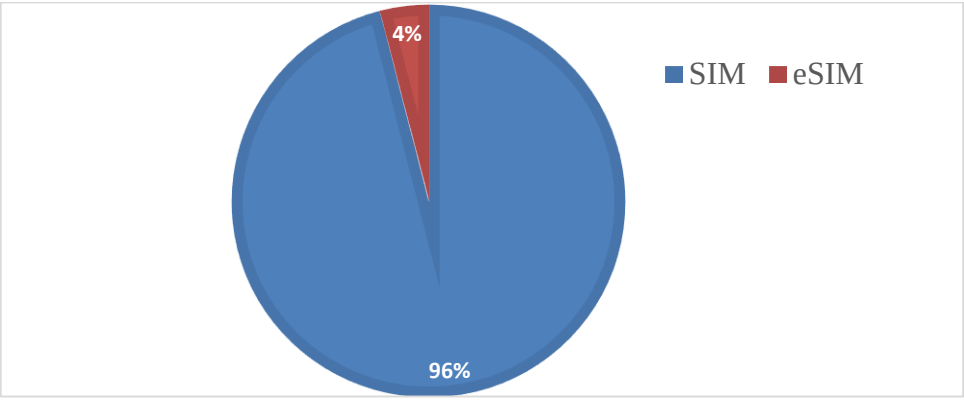

Рис.3. Динамика использования устройств, поддерживающих SIM и eSIM

eSIM дает пользователям возможность загружать профиль прямо на свой телефон. Отправка профилей по беспроводной сети теоретически может создать риск взлома, внедрив новый профиль на чужое устройство и получив над ним контроль. Учитывая все это, предлагается использовать уникальный ключ, который будет запрашивать подтверждение через сторонний сервер всякий раз, когда кто-то запрашивает новый профиль. В данном

случае это называется сервером подготовки данных менеджера подписок (англ. SM-DP+). После этого устройство, которое пытается загрузить новый профиль, инициирует запрос к SM-DP+, который впоследствии будет подтвержден оператором.

Переактивация нужного нам соединения без сканирования QR-кода или ввода специального пароля, предоставленного оператором, влечет за собой ряд уязвимостей в системе безопасности eSIM, что впоследствии облегчает хакерам возможность получения доступа к идентификационным данным [13].

В текущих используемых устройствах с отдельными слотами для SIM-карт, например в смартфоне или часах, съемный характер SIM-карты является фактором риска. Обычную SIM-карту можно извлечь из телефона законного владельца, если он украден или потерян, − после этого довольно легко снять все имеющиеся блокировки и использовать устройство с новой SIM-картой самостоятельно либо перепродав его. В отличие от них, телефоны с технологией eSIM не имеют никаких слотов, тем самым перекрыв физический доступ, что является огромным преимуществом в целях безопасности. С eSIM без ведома владельца контракта или не зная определенного ключа безопасности, нельзя будет загрузить новый профиль, что сделает использование устройства невозможным; более того, при каждом включении оно будет загружать именно первоначальный профиль и тем самым упрощать определение местоположения смартфона [14].

В тот момент, когда устройство с поддержкой eSIM включено, имея возможность перепрограммирования, в целях безопасности оно может легко отслеживаться в сети. Эта возможность также была бы чрезвычайно полезной в более широком промышленном масштабе. Транспортные средства, оборудование и любые другие устройства с возможностью подключения к eSIM всегда легко обнаружаемы, поэтому случайная потеря или преднамеренная кража может быть легко устранена.

Заключение

В статье был проведен обзор архитектуры технологии виртуализации SIM-карт, а также типов коммуникационных профилей и их основной роли. Проанализирован алгоритм переключения профилей, использующийся в технологии eSIM, а также были исследованы основные вопросы безопасности технологии виртуализации SIM-карт. Кроме того, была исследована динамика использования устройств, поддерживающих SIM и eSIM за последний год.

Поскольку традиционные SIM-карты имеют недостаточный уровень безопасности при хранении учетных данных операторов, было предложено внедрение более перспективной технологии виртуализации SIM-карт, так как безопасность технологии eSIM реализуется на аппаратном уровне и является более надежной и защищенной. Кроме того, ряд существенных преимуществ данной технологии над SIM позволяет расширить список поддерживающих мобильных операторов и устройств в будущем.

Литература

1. Peppard J., Rylander A. From Value Chain to Value Network: Insights for Mobile Operators. // European Management Journal, 2006, vol.24, pp.128–141.
2. Борьба за SIM. Что не так с SIM-картами. https://vc.ru/tech/26660-borba-za-sim/
3. SIM-карта. eSIM. https://ru.wikipedia.org/wiki/SIM-карта/
4. Gerpott T., May S. Embedded Subscriber Identity Module eSIM. // Business and Information Systems Engineering, 2017, vol.59, no.4, pp.293–296.
5. Alendal M. Operators need an ecosystem to support 50 billion connections. // Ericsson Business Review, 2010, no.3, pp.42.
6. Suzuki K., Azuma T. Standardization of Embedded UICC Remote Provisioning. // NTT DOCOMO Technical Journal, 2014, vol.16, no.2.

7. Vesselkov A., Hämmäinen H., Ikäläinen P. Value networks of embedded SIM-based remote subscription management. / IEEE Conference of Telecommunication, Media and Internet Techno-Economics (CTTE), 2015.
8. Shahnaz M. Embedded SIM Remote Provision Architecture. // Value Network Analysis of Embedded Subscriber Identity Module in Machine to Machine Communication, 2014, pp.26–29.
9. Park J., Baek K., Kang C. Secure Profile Provisioning Architecture for Embedded UICC. / International Conference on Availability, Reliability and Security, 2013, pp.297–303.
10. What is an eSIM, and why should you care. eSIM advantages. https://www.broadbandgenie.co.uk/features/what-an-esim/
11. SIM Card Shipments to Reach 5.6 Billion Units by 2020, IHS Says. https://news.ihsmarkit.com/press-release/technology/sim-card-shipments-reach-56-billion-units-2020-ihs-says/
12. eSIM Market Projected to Increase Nearly Nine-Fold, to Almost One Billion Shipments. https://technology.ihs.com/591806/esim-market-projected-to-increase-nearly-nine-fold-to-almost-one-billion-shipments/
13. eSIM Whitepaper. The what and how of Remote SIM Provisioning, march 2018. GSMA.
14. How safe is the eSIM. https://www.truphone.com/about/newsroom/how-safe-is-the-esim

UOT 004.77

Cəfərzadə Kamran E.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
kamran@science.az

eSIM texnologiyası: müasir vəziyyəti, arxitektur prinsipləri və təhlükəsizlik məsələləri

Məqalədə eSIM texnologiyasının arxitekturası, kommunikasiya profillərinin əsas növləri, onların SM-DP və SM-SR abunə idarəçiliyində rolları və eSIM texnologiyasında istifadə olunan profillərin dəyişdirilməsi alqoritmi analiz edilir. Hal-hazırda ənənəvi SİM etibarlılıq və istifadə təhlükəsizliyi baxımından müəyyən zəifliklərə malikdir. Məsafədən idarəetmənin mümkünsüzlüyü və operatorların uçot verilənlərinin mühafizəsi zamanı təhlükəsizlik səviyyəsinin aşağı olması Sim-kartların virtualizasiyasının yeni texnologiyalarının tətbiqi ilə bu problemlərin əsaslı şəkildə həll edilməsi haqqında düşünməyə əsas verir. Tədqiqat nəticəsində eSIM texnologiyasının mobil qurğular bazarında tətbiq olunması və sələfinin tam əvəz edilməsi üçün gələcək perspektivlərin olduğu müəyyən edilmişdir.

Açar sözlər: *eSIM, quraşdırılmış SIM, eUICC, abunə meneceri, profil, MNO, SM-DP, SM-SR, QR kodu.*

Kamran E. Jafarzade
Institute of Information Technology of ANAS, Baku, Azerbaijan
kamran@science.az

eSIM technology: state-of-the-art, architectural principles and security issues

The article reviews the architecture of the eSIM technology, the main types of communication profiles and their role in subscription manager SM-DP and SM-SR. It also offers an analysis of the profile switching algorithm used in eSIM technology. At present, the traditional SIM has enough vulnerabilities in terms of reliability and safety of use. The lack of remote control and the low level of security when storing operator credentials give reason to think about solving these problems using the new technology for virtualizing SIM cards. As a result of the study, it is also found that there are further prospects for introducing eSIM technology into the mobile device market and fully replacing its predecessor.

Keywords: *eSIM, embedded SIM, eUICC, subscription manager, profile, MNO, SM-DP, SM-SR, QR code.*