Варианты построения отечественной инфраструктуры eSIM: PKI или симметричная криптография?

Александров Сергей Викторович

Необходимость исследования

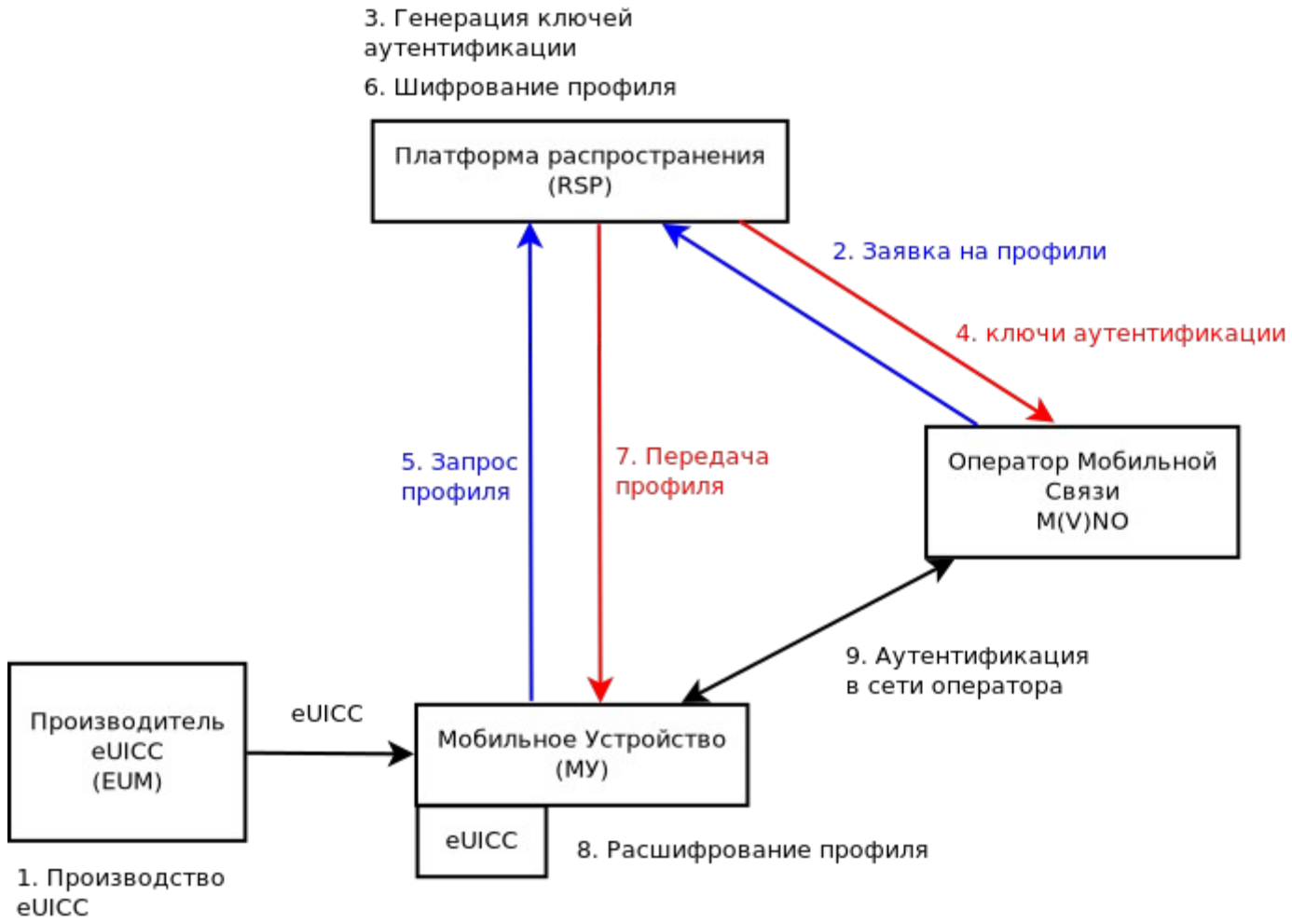
Был проведен ряд НИР и макетирование отдельных участков инфраструктуры eSIM на территории РФ. По результатам были получены замечания регулятора, в том числе, о необходимости обоснования выбранной ключевой системы.

Причины исследования вариантов КС:

- Нестойкость асимметричной криптографии в мире квантовых компьютеров;
- Более слабая стойкость асимметричной криптографии по отношению к симметричной на данный момент;
- Исследовательская работа подразумевает рассмотрение и анализ различных возможных вариантов исполнения.

Исходные данные

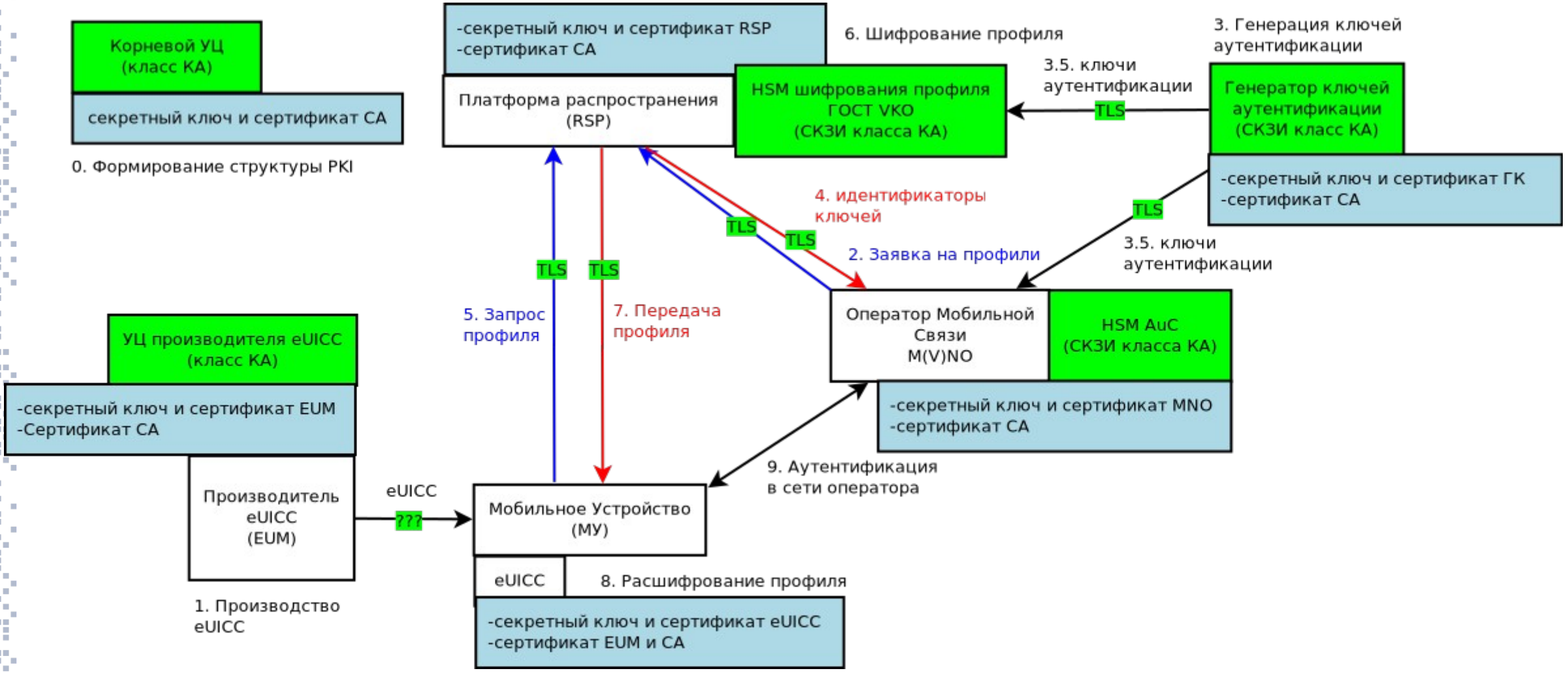
Упрощенная схема взаимодействия в инфраструктуре eSIM



Проблемные моменты

- Доведение микросхемы eUICC до производителя МУ и далее до конечного потребителя;
- Канал связи MNO — RSP: не определён стандартами;
- Требования по генерации ключей аутентификации (может быть как на стороне RSP, так и MNO);
- Возможность реализации LPA как в eUICC так и в МУ;
- По согласованной модели отечественного регулятора:
  - ядро сети — класс КА;
  - eUICC — класс КС3.

Вариант с PKI (GSMA)



Вариант с PKI (GSMA)

- eUICC содержит секретный ключ, защиты на этапе доведения не требуется из-за невысокого класса eUICC;
- Канал связи MNO — RSP: для защиты канала может использоваться TLS;
- 3 варианта взаимодействия генератора ключей аутентификации с RSP:
  - Отдельно стоящий. Требуется защита каналов связи до HSM AuC и HSM шифрования профилей. Может использоваться TLS;
  - В контролируемой зоне в RSP. Для доведения идентификаторов ключей до HSM AuC можно использовать канал связи MNO — RSP;
  - В контролируемой зоне у MNO. Для доведения идентификаторов ключей до HSM шифрования профиля также можно использовать канал связи MNO — RSP.

Вариант с симметричной криптографией

Вариант с симметричной криптографией

- eUICC содержит ключ шифрования профиля (КШП), защиты на этапе доведения не требуется из-за невысокого класса eUICC;
- Канал связи МУ — RSP (запросы + SCP03ru): необходимо разработать протокол обмена и обосновать его стойкость;
- Канал связи MNO — RSP: может использоваться канальный СКЗИ;
- Взаимодействия генератора ключей аутентификации с RSP и MNO аналогично схеме с PKI. Необходимы канальные СКЗИ.

Ключевая система

Вариант с симметричной криптографией:

- Требуется разработка новых протоколов обмена и обоснование их стойкости;
- Большая нагрузка на ключ шифрования профиля;
- Требуется предусмотреть дубликаты КШП по количеству RSP;
- Требуется предусмотреть возможность добавления нового RSP;
- Срок действия КШП — срок жизни мобильного устройства.

Вариант с PKI:

- Срок действия секретного ключа eUICC — срок жизни мобильного устройства;
- При реализация LPA в eUICC — можно не реализовывать второй контур (SCP03ru).

Компрометации

Вариант с симметричной криптографией:

- Любой RSP — хранение всех ключей шифрования профиля — компрометации всей системы;
- Генератор КШП на производителе eUICC — компрометации всех выпущенных eUICC данного производителя;
- Нет возможности отзыва скомпрометированных КШП.

Вариант с PKI:

- Корневой УЦ — компрометация всей системы;
- УЦ производителя eUICC — компрометации всех выпущенных eUICC данного производителя;
- Есть возможность отзыва скомпрометированных сертификатов.

Надёжность

Вариант с симметричной криптографией:

- Требуется дублирование всех КШП на всех RSP;
- Резервирование генератора ключей у производителя eUICC;
- Резервирование HSM шифрования профиля RSP.

Вариант с PKI:

- Холодный резерв корневого УЦ;
- Резервирование УЦ производителя eUICC;
- Резервирование HSM шифрования профиля RSP.

Масштабируемость

Вариант с симметричной криптографией:

- Требуется копирование всех ключей шифрования профиля при добавлении нового RSP;
- Требуется дополнительная настройка при организации новых защищенных каналов с RSP или использование дополнительных СКЗИ.

Вариант с PKI:

- Не требуется дополнительных затрат.

Преимущества и недостатки

Характеристика	PKI-инфраструктура	Симметричная криптография
Сложность КС	• Простая	• Сложная • Требуется разработка новых протоколов взаимодействия RSP — eUICC
Количество СКЗИ	• Два УЦ класса КА	• Один генератор КШП класса КА
Надёжность системы в целом	• Более надёжна, за счёт меньшего объема хранения ключей	
Результаты компрометации	• Возможность отзыва сертификатов через CRL	• Компрометация всех ключей шифрования профиля и соответственно зашифрованных на них ключей аутентификации в случае компрометации RSP или производителя eUICC
Удобство эксплуатации	• Не требует перенастройки сети шифрованной связи в случае изменения количества объектов	• Требуется поддержка как минимум одной сети шифрованной связи на классических канальных СКЗИ
Масштабируемость	• Легко (ещё один сертификат)	• Увеличение числа шифрованных каналов, увеличение времени формирования КШП за счёт большего числа дубликатов
Доведение ключевой информации	• Открытые сертификаты	• Фельдсвязь;
Разработка новых СКЗИ	• УЦ класса КА • HSM шифрования профиля на ГОСТ VKO	• Генератор ключей шифрования профиля • HSM шифрования профиля на КШП
Стоимость внедрения и обслуживания	Низкая	Высокая

Выводы

Оптимальным вариантом построения архитектуры для российской экосистемы eSIM всё-таки является инфраструктура открытых ключей.

Она обеспечивает:

- Простую и удобную эксплуатацию всей системы;
- Более дешёвое обслуживание системы;
- Безопасную загрузку абонентских профилей в доверенные МУ с российской EUICC до появления квантовых компьютеров;
- Простое масштабирование как по производителям eUICC, так и по мобильным операторам или платформам RSP.

Спасибо за внимание!