конференция
РусКрипто

Ежегодная международная научно-практическая конференция

# «РусКрипто'2024»

## Защищенный универсальный протокол передачи данных и управления микросхемой интеллектуальной карты UICC / eUICC в сетях подвижной радиосвязи (secure universal protocol for downloading data and managing the smart card chip – SECUNDA)

Софья Грезина, Алла Герасимова
ООО «Системы практической безопасности»

# Актуальность разработки протокола

Руководящие документы:

- «Концепции создания и развития сетей 5G/IMT-2020 в Российской Федерации» (приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации №923 от 27.12.2019);
- «Стратегии развития отрасли связи Российской Федерации на период до 2035 года» (Распоряжение Правительства Российской Федерации от 24.11.2023 г. №3339-р).

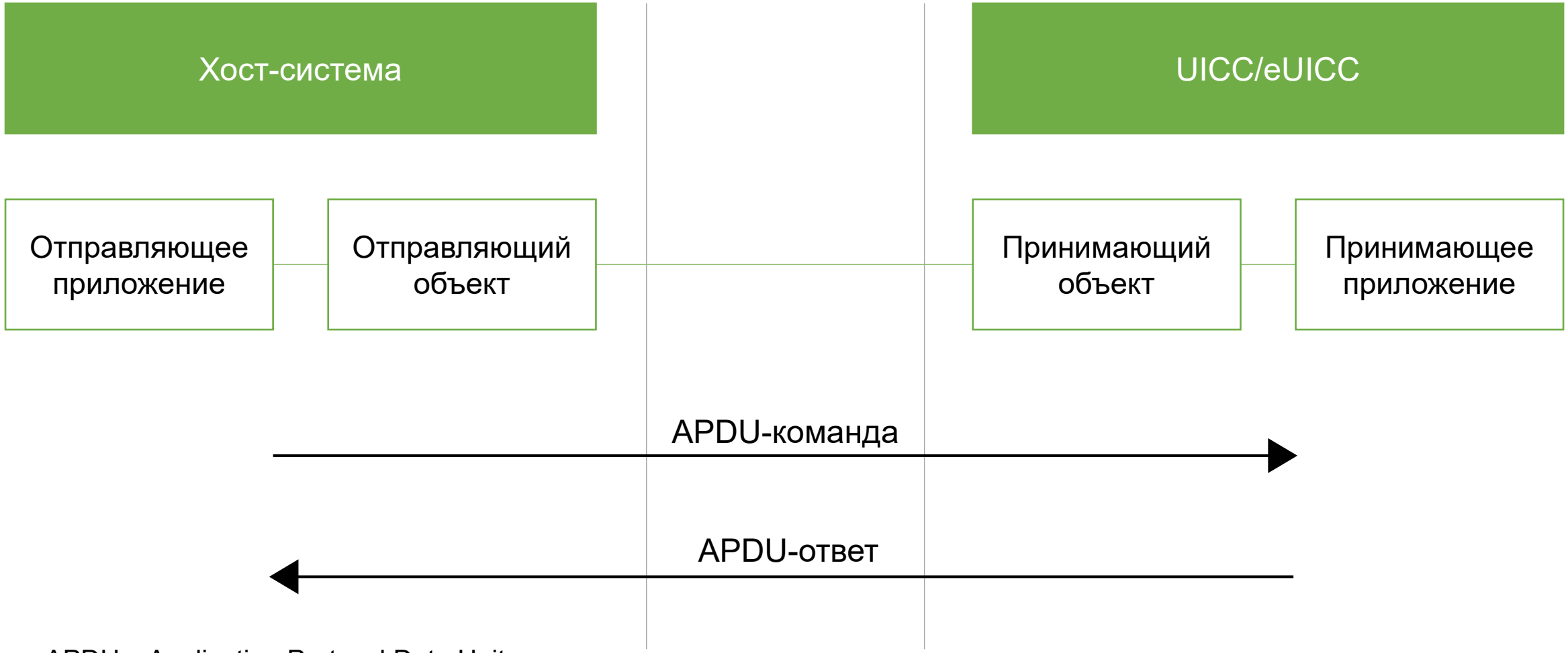
НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

В 2023 году под эгидой АНО «НТЦ ЦК» была выполнена НИР «Исследование вариантов безопасного взаимодействия между хост-системой и микросхемами интеллектуальных карт (UICC*, eUICC**), применяемых в сетях подвижной радиосвязи», в рамках которой:

- Исследованы различные сценарии взаимодействия между хост-системами и UICC/eUICC;
- Проведен анализ протоколов семейства SCP (Secure Channel Protocol), определенных в спецификациях GlobalPlatform, GSMA (GSM Association) и ETSI (European Telecommunications Standards Institute);
- Определены требования безопасности и функциональные требования к разрабатываемому протоколу;
- Разработан проект «Защищенного универсального протокола передачи данных и управления микросхемой интеллектуальной карты UICC/eUICC в сетях подвижной радиосвязи» (**sec**ure **un**iversal protocol for **d**ownloading data **a**nd managing the smart card chip – SECUNDA).

*UICC - Universal Integrated Circuit Card - универсальная карта с интегральной схемой
**eUICC - Embedded Universal Integrated Circuit Card – встроенная универсальная карта с интегральной схемой

# Общая схема взаимодействия хост-системы и UICC/eUICC (в соответствии с ISO 7816-4 и спецификациями GlobalPlatform)




APDU – Application Protocol Data Unit

# Протоколы семейства SCP

| Обозначение | Назначение | Руководящий документ |
|---|---|---|
| SCP03 | Организация безопасного канала с использованием симметричных ключей | Дополнение D к спецификации GlobalPlatform (Card Specification v2.3) |
| SCP03t | Организация безопасного канала с использованием симметричных ключей | RSP Technical Specification (GSMA SGP.22 v2.5) |
| SCP10 | Аутентификация с использованием ассиметричной криптографии на основе алгоритма RSA | Дополнение L к спецификации GlobalPlatform (Card Specification v2.3) |
| SCP11 | Аутентификация с использованием ассиметричной криптографии на основе эллиптических кривых | Дополнение F к спецификации GlobalPlatform (Card Specification v2.3) |
| SCP80 | Организация безопасного канала с использованием симметричных ключей для сетей ПРС | ETSI TS 102 225,<br>ETSI TS 102 226 |
| SCP81 | Организация безопасного канала с использованием симметричных ключей на основе HTTP | Дополнение B к спецификации GlobalPlatform (Card Specification v2.3) |

# Общие требования к протоколу

- Обеспечение функциональных требований: управление и загрузка данных;
- Поддержка форматов команд, основанных на технологии GlobalPlatform;
- Соответствие требованиям безопасности, направленным на парирование угроз;
- Универсальность: возможность использования протокола для различных сценариев применения как для UICC, так и для eUICC;
- Самодостаточность: обеспечение заданной функциональности и защиты данных на всех стадиях без обязательного использования других протоколов;
- Гибкость: возможность использования различных способов управления ключевой информацией;
- Унификация: поддержка нескольких вариантов реализаций процедур и механизмов только там, где это продиктовано сценариями применения протокола;
- Технологичность: возможность реализации для бюджетных низкоресурсных микросхем.

# Требования безопасности к протоколу

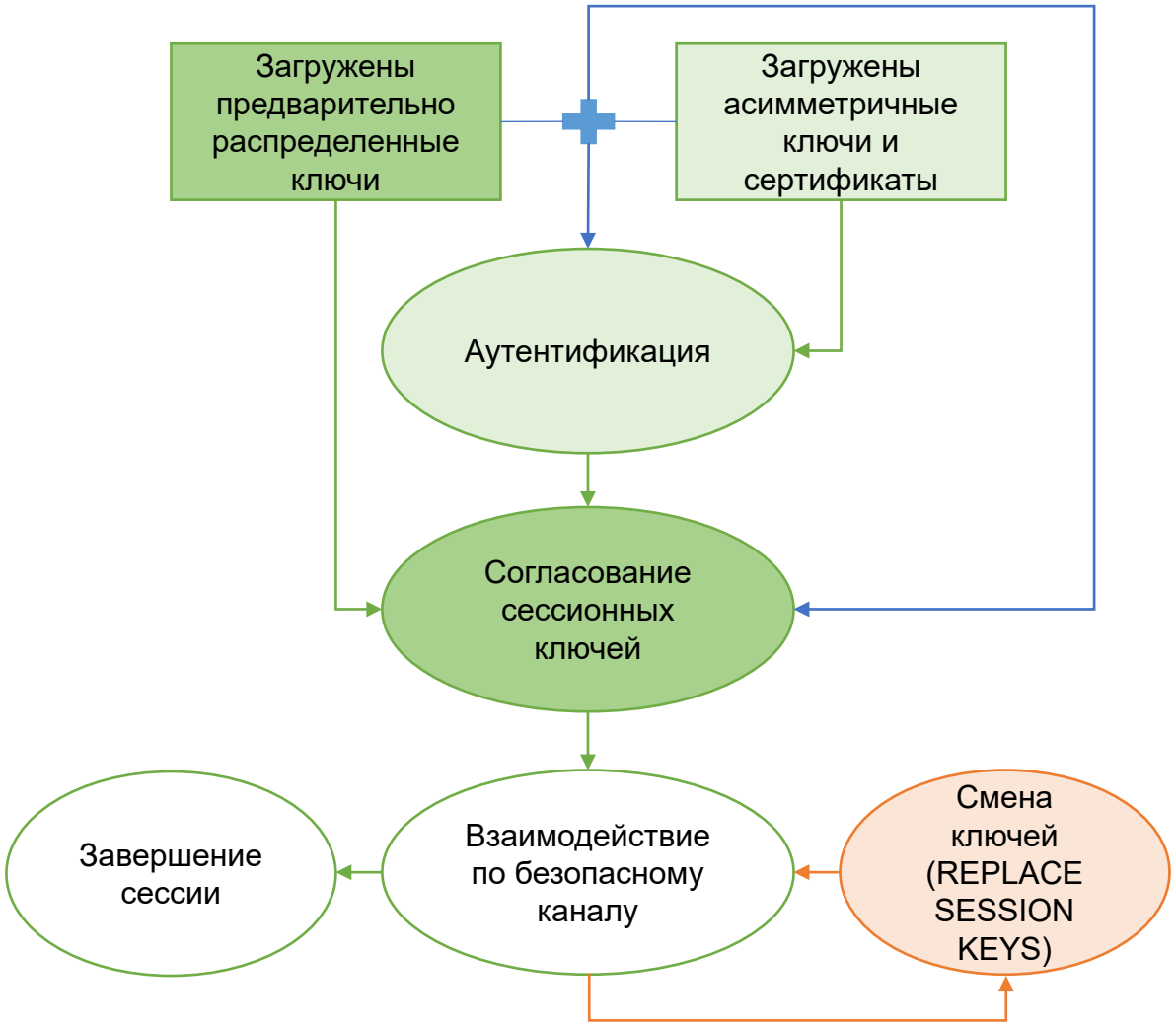
- Взаимная аутентификация хоста и карты с обеспечением подлинности (опционально);
- Конфиденциальность передаваемых сообщений;
- Конфиденциальность данных, нуждающихся в дополнительной защите (например, ключей);
- Целостность передаваемых сообщений, включая заголовок;
- Целостность дефрагментированной информации, передаваемой блоками посредством нескольких сообщений;
- Использование счетчика переданных и полученных сообщений;
- Использование функций выработки ключей, исключающих «чтение назад».

# Анализ российских криптографических алгоритмов и протоколов

| Протокол/ схема Критерий | Р 1323565.1.004-2017 | Р 1323565.1.032–2020 | Р 1323565.1.028–2019 | Р 1323565.1.018-2018 | Р 1323565.1.025–2019 | Р 1323565.1.018-2018 |
|---|---|---|---|---|---|---|
| Краткое название | Эхинацея-3 (Э-3), Эхинацея-2 (Э-2), Лимонник-3 (Л-3) | DLMS | – | CRISP | CMS | – |
| Назначение | Выработка ключа с взаимной или односторонней аутентификацией на основе схемы с открытыми ключами | Согласование ключа для защищенного взаимодействия между системами сбора данных и измерительными устройствами | Выработка ключа с взаимной или односторонней аутентификацией на основе схемы с открытыми ключами между контрольными и измерительными устройствами | Защищенный обмен сообщениями для индустриальных систем | Защищенная передача сообщений | Взаимная аутентификация с выработкой ключа в контрольных устройствах для автотранспорта |
| Режим работы (варианты реализации) | –с взаимной аутентификацией (Э-3, Л-3);<br>–с односторонней аутентифика-цией (Э-2) | –с обеспечением конфиденциальности и целостности, а также передачей ключевой информации в контейнере;<br>–с дополнительной предварительной выработкой ключей | –для использования на сеансовом уровне;<br>–для использования на канальном уровне | –с шифрованием и имитозащитой;<br>–только с имитозащитой | Возможны различные типы содержимого:<br>–простые данные;<br>–подписанные данные;<br>–конверт данных;<br>–хэшированные данные;<br>–зашифрованные данные;<br>–аутентифицированные данные | –взаимная аутентификация |
| Криптографические алгоритмы/механизмы | –ГОСТ 34.12–2018 («Кузнечик») в режиме CMAC;<br>–HMAC_GOSTR3411_2012_512 Р 50.1.113;<br>–ГОСТ Р 34.11—2012 с длиной хэш-кода 512 бит;<br>–PRF_TLS_GOST3411_2012_512 Р 50.1.113 | –Набор 8: ГОСТ 34.12–2018 («Кузнечик») в режимах CTR и CMAC ГОСТ 34.13–2018 | –ГОСТ Р 34.11—2012;<br>–HMAC_GOSTR3411_2012_256 и HMAC_GOSTR3411_2012_512 Р 50.1.113;<br>–ГОСТ Р 34.10;<br>–ГОСТ Р 34.12 («Магма» или «Кузнечик») в режимах CTR, CMAC ГОСТ Р 34.13 и MGM Р 1323565.1.026-2019 | –Наборы 1, 3: ГОСТ 34.12–2018 («Магма») в режимах CTR и CMAC ГОСТ Р 34.13.<br>–Наборы 2, 4: ГОСТ 34.12–2018 («Магма») в режиме CMAC ГОСТ Р 34.13 | –ГОСТ Р 34.12 («Магма» или «Кузнечик») в режиме CMAC ГОСТ Р 34.13 и CTR-ACPKM Р 1323565.1.017;<br>–ГОСТ Р 34.10;<br>–ГОСТ Р 34.11;<br>–KDF_TREE_GOSTR3411_2012_256 Р 50.1.113;<br>–KExp15 Р 1323565.1.017 | –HMAC_GOSTR3411_2012_512 Р 50.1.113;<br>–ГОСТ Р 34.10;<br>–ГОСТ Р 34.12 («Магма») в режиме CTR ГОСТ Р 34.13; |
| Уровень модели OSI | Не определен | Сеансовый / транспортный | Прикладной | Прикладной | Прикладной | Прикладной |

# Стадии взаимодействия по протоколу SECUNDA

1. Инициирование установления защищенного соединения, согласование параметров безопасности сессии. Инициатором выступает хост;
2. Взаимная аутентификация хоста и карты. Опциональная стадия;
3. Формирование сессионных ключей в соответствии с согласованной схемой управления ключами – финальная стадия установления защищенного соединения;
4. Передача сообщений по установленному защищенному соединению (безопасному каналу). На этой стадии опционально возможно выполнение процедуры смены ключей;
5. Завершение сессии (прекращение передачи сообщений, удаление сессионных ключей).



# Ключевая система

**Ключи аутентификации**

- статические ключи карты (SK.SD.EC, PK.SD.EC);
- статические ключи хоста (SK.OCE.EC, PK.OCE.EC);
- открытый ключ УЦ (PK.CA.EC);

**Предварительно распределенные ключи**

- ключ шифрования (Key-ENC);
- ключ имитозащиты (Key-MAC);
- ключ шифрования конфиденциальных данных (Key-DEK);
- ключ имитозащиты конфиденциальных данных (Key-DMAC);

**Асимметричные ключи**

- эфемерные ключи карты (eSK.SD.EC, ePK.SD.EC);
- эфемерные ключи хоста (eSK.OCE.EC, ePK.OCE.EC);
- статические ключи хоста (SK.OCE.EC, PK.OCE.EC);

KDF

VKO+KDF

**Сессионные ключи**

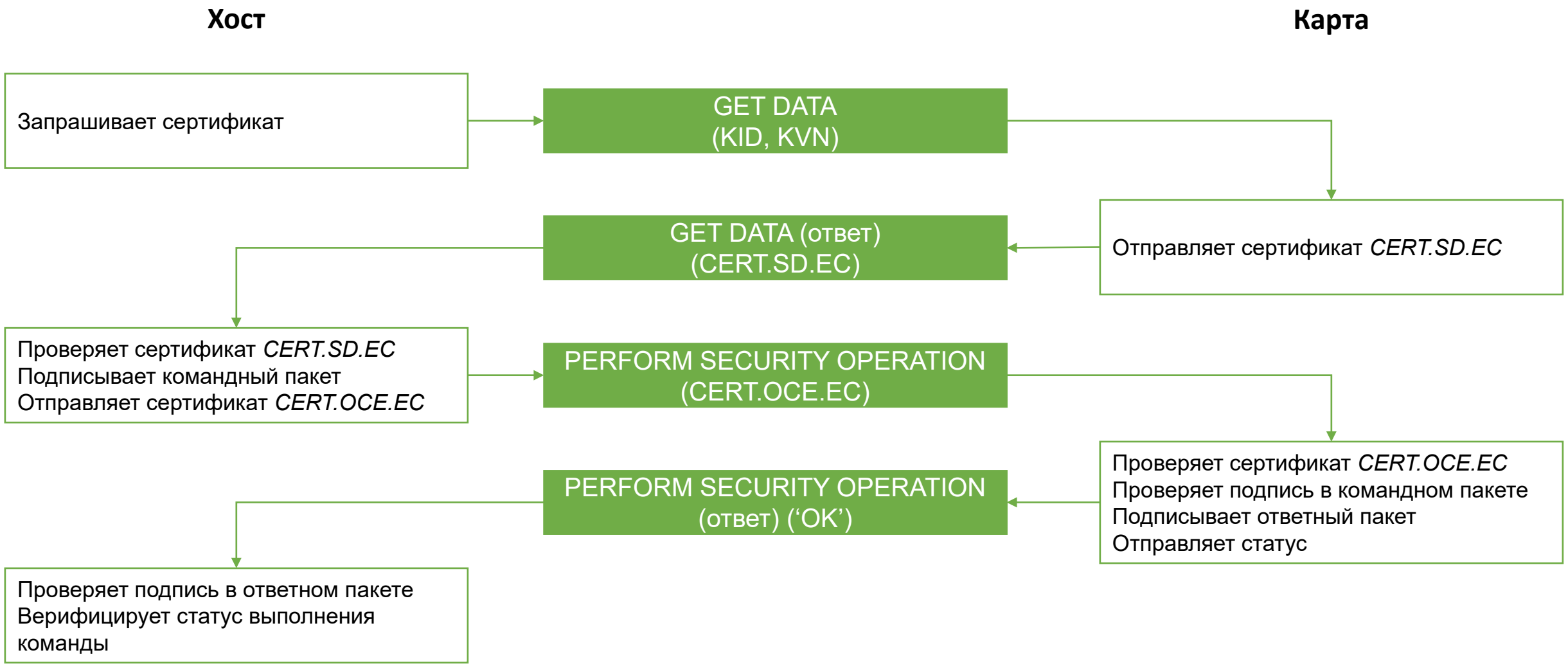
- ключ шифрования команд (S-ENC/eS-ENC);
- ключ имитозащиты команд (S-MAC/eS-MAC);
- ключ имитозащиты ответов (S-RMAC/eS-RMAC);
- ключ шифрования конфиденциальных данных (Key-DEK/eS-DEK/PPK-DEK);
- ключ имитозащиты конфиденциальных данных (Key-DMAC/eS-DMAC/PPK-DMAC);

**Предварительно выработанные хостом ключи**

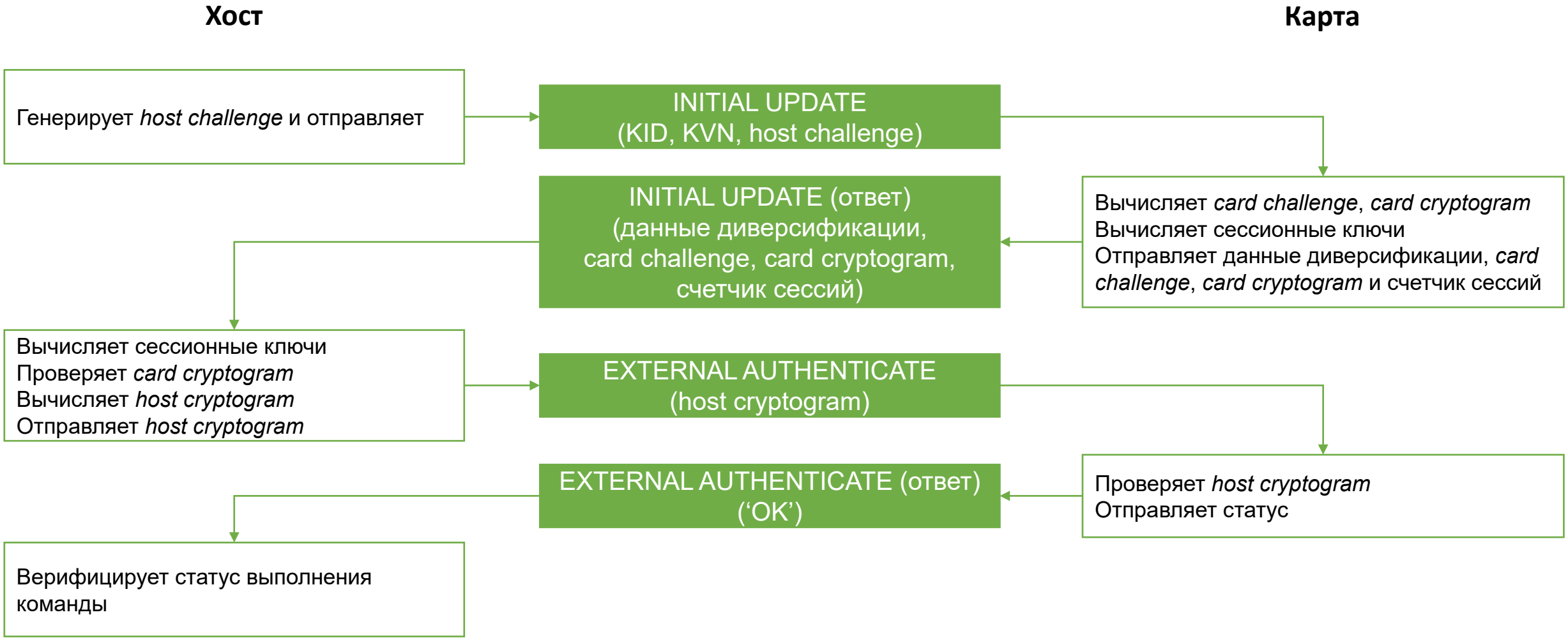
- ключ шифрования конфиденциальных данных (PPK-DEK);
- ключ имитозащиты конфиденциальных данных (PPK-DMAC);

REPLACE SESSION KEYS

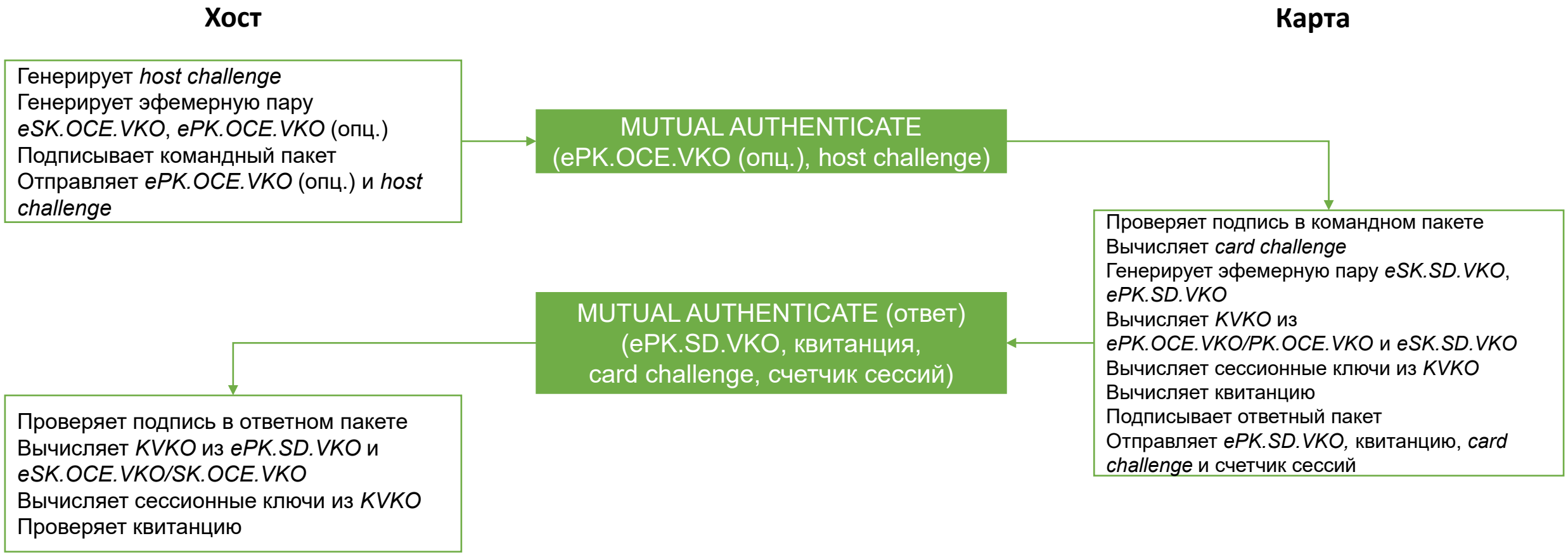
# Взаимная аутентификация хоста и карты



# Формирование сессионных ключей с использованием предварительно распределенных ключей



# Формирование сессионных ключей с использованием асимметричных ключей



# Формат командного пакета

| Поле | Длина (в байтах) |
|---|---|
| Идентификатор командного пакета (CPI) | 1 |
| Длина командного пакета (CPL) | Переменная |
| Идентификатор заголовка команды (CHI) | 1 |
| Длина заголовка команды (CHL) | 1 |
| Индикатор параметров безопасности (SPI) | 3 |
| Индикатор алгоритма шифрования конфиденциальных данных (DPI) | 1 |
| Индикатор алгоритма имитозащиты конфиденциальных данных (DCI) | 1 |
| Идентификатор приложения (TAR) | 3 |
| Счетчик (CNTR) | 8 |
| Индикатор цепочки (CHAIN) | 1 |
| Счетчик дополнения (PCNTR) | 1 |
| Имитовставка (CC)<br>или электронная подпись (PS) | для CC: 8 или 16<br>для PS: 64 |
| Защищаемые данные (Secured Data) | Переменная, $\leq L_{MAX}$ |

- Имитозащите подлежат все поля, кроме CC/PS
- Алгоритм имитозащиты – «Магма» или «Кузнечик» в режиме выработки имитовставки

- Шифрованию подлежат поля CHAIN||PCNTR||CC/PS||Secured data
- Алгоритм шифрования – «Магма» или «Кузнечик» в режиме гаммирования, синхропосылка – значение CNTR

- Подписываются все поля, кроме CC/PS
- Алгоритм подписи – ГОСТ 34.10-2018 (512 бит )

# Формат ответного пакета

| Поле | Длина (в байтах) |
|---|---|
| Идентификатор ответного пакета (RPI) | 1 |
| Длина ответного пакета (RPL) | Переменная |
| Идентификатор заголовка ответа (RHI) | 1 |
| Длина заголовка команды (RHL) | 1 |
| Идентификатор приложения (TAR) | 3 |
| Счетчик (CNTR) | 8 |
| Индикатор цепочки (CHAIN) | 1 |
| Счетчик дополнения (PCNTR) | 1 |
| Код статуса ответа (RSCO) | 1 |
| Имитовставка (CC)<br>или электронная подпись (PS) | для CC: 8 или 16<br>для PS: 64 |
| Защищаемые данные (Secured Data) | от 0 до $L_{MAX}$ |

- Имитозащите подлежат все поля, кроме CC/PS
- Шифрование не требуется
- Подписываются все поля, кроме CC/PS

# Формат APDU-команды и APDU-ответа

| Поле | Длина (в байтах) | Описание |
|---|---|---|
| CLA (Class Byte) | 1 | Класс команды: $C7_{16}$ в соответствии с GlobalPlatform |
| INS (Instruction code) | 1 | Код инструкции (тег команды):<br>$CA_{16}$ – GET DATA;<br>$2A_{16}$ – PERFORM SECURITY OPERATION;<br>$82_{16}$ – MUTUAL AUTHENTICATE;<br>$84_{16}$ – INITIALIZE UPDATE;<br>$85_{16}$ – EXTERNAL AUTHENTICATE |
| P1 | 1 | Первый параметр команды. Если отсутствует, равен $00_{16}$ |
| P2 | 1 | Второй параметр команды. Если отсутствует, равен $00_{16}$ |
| Lc | 1 | Длина поля Data |
| Data | Переменная | Данные команды |
| Le | 1 или отсутствует | Ожидаемая длина ответа |

| Поле | Длина (в байтах) | Описание |
|---|---|---|
| Data | Переменная | Данные ответа, если есть |
| SW1 (Status Word – 1) | 1 | Код статуса – результат обработки команды |
| SW2 (Status Word – 2) | 1 | |

- В случае успешной обработки команды в APDU-ответе отправляется статус $9000_{16}$
- Размер передаваемых данных в APDU-команде и APDU-ответе не может превышать максимальное значение $L_{APDU} = 255$ байт
- Иначе данные разбиваются на фрагменты длины $\leq L_{APDU}$ и отправляются цепочкой команд или ответов

# Используемые российские криптографические алгоритмы и механизмы

| Назначение криптографического алгоритма/механизма | Российский криптографический алгоритм/механизм |
|---|---|
| Шифрование сообщений и конфиденциальных данных | Блочные шифры «Магма» и «Кузнечик» ГОСТ 34.12 в режиме гаммирования ГОСТ 34.13-2018 |
| Контроль целостности сообщений и конфиденциальных данных | Режим выработки имитовставки ГОСТ 34.13-2018 – OMAC1 для блочных шифров «Магма» и «Кузнечик» ГОСТ 34.12 |
| Формирование и проверка электронной подписи на эллиптических кривых | Алгоритм формирования и проверки электронной цифровой подписи длиной 512 бит ГОСТ 34.10-2018<br>Параметры эллиптических кривых для криптографических алгоритмов и протоколов Р 1323565.1.024-2019 |
| Экспорт ключей | Алгоритмы экспорта KExp15 и импорта KImp15 ключа Р 1323565.1.017-2018 |
| Диверсификация ключей (KDF) | Функции диверсификации KDF_GOST3411_2012_256 Р 50.1.113-2016 |
| Выработка общих ключей в результате процедуры согласования ключей (VKO) | Алгоритмы согласования ключей VKO_GOST3410_2012_256 Р 50.1.113-2016 |
| Функция хэширования | Функция хэширования «Стрибог» ГОСТ 34.11-2018 |

# Примеры сценариев применения протокола SECUNDA в UICC/eUICC

| Хост-система | Функции | Протокол SCP | Протокол SECUNDA |
|---|---|---|---|
| OTA-платформа | Удаленное управление файловой системой;<br>Удаленное управление приложениями UICC/eUICC | SCP80<br>SCP81 | ✓ |
| Машина инициализации/ персонализации | Преперсонализация/персонализация UICC/eUICC | SCP03 | ✓ |
| SM-SR | Создание подчиненного домена безопасности;<br>Активация/деактивация цифрового профиля;<br>Удаление цифрового профиля;<br>Управление настройками eUICC | SCP80<br>SCP81 | ✓ |
| SM-DP/SM-DP+ | Загрузка и установка цифрового профиля в eUICC | SCP03<br>SCP03t | ✓ |
| SM-DP+ | Передача команд взаимной аутентификации SM-DP+ и eUICC;<br>Создание безопасного канала управления загрузкой профиля | SCP11<br>(или TLS) | ✓ |

# Заключение

## Текущий результат

- Разработан проект «Защищенного универсального протокола передачи данных и управления микросхемой интеллектуальной карты UICC/eUICC в сетях подвижной радиосвязи» (SECUNDA), который в перспективе может заменить применяемый на сегодняшний день в сетях подвижной радиосвязи набор протоколов взаимодействия между хост-системой и микросхемой интеллектуальной карты, с обеспечением необходимых, как функциональных требований, так и требований безопасности российского регулятора.

## Продолжение работы

В рамках заявленной в 2024 году НИР под эгидой АНО «НТЦ ЦК» планируется :

- Уточнение модели нарушителя для сценариев применения протокола;
- Доработка ключевой системы и параметров протокола (при необходимости);
- Обоснование криптографической стойкости протокола;
- Макетирование протокола

# Спасибо за внимание!