РусКрипто

Возможность использования протокола SECUNDA для защищенной загрузки данных в процессе эмиссии платежных карт

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Софья Грезина, Алла Герасимова
ООО «Системы практической безопасности»

СПБ

Актуальность

РусКрипто

В соответствии с требованиями положения Банка России от 17 августа 2023 г. **N 821-П** «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», вступающими в силу **1 января 2031 г.**,
для обеспечения информационной безопасности в финансовой сфере необходимо осуществить переход на использование российских криптографических алгоритмов

Эмиссия платежных карт

РусКрипто

После изготовления микросхемы и ее имплантации в пластиковую карту выполняются:

- инициализация карты (файловая система и **приложения**);
- генерация и запись серийного номера карты;
- генерация и запись **ключей персонализации** (**пре-персонализация**);
- **персонализация**.

Защищенная загрузка данных выполняется с использованием зарубежных протоколов безопасного канала SCP (Secure Channel Protocol): SCP02, SCP03.

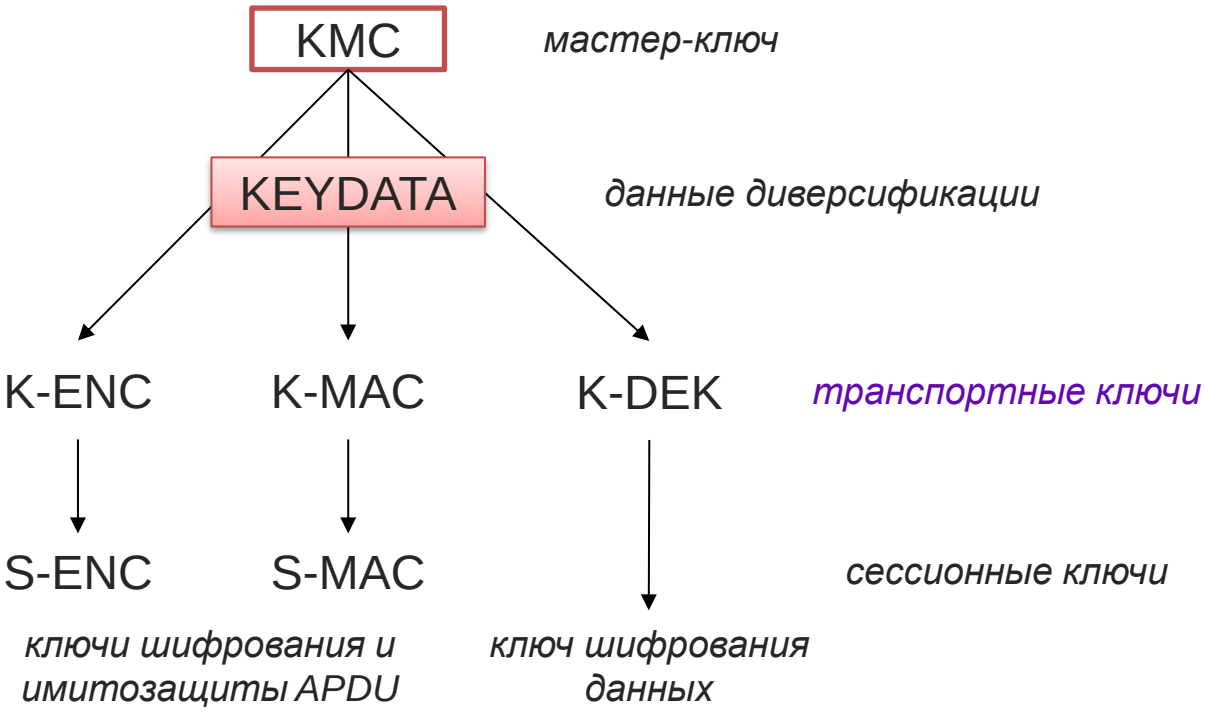
Ключевая схема пре-персонализации

РусКрипто

Передается изготовителю платежных карт **от изготовителя микросхем**

Загружаются **в микросхему изготовителем микросхем**

Вырабатываются при установлении безопасного канала **(загрузка приложений и пре-персонализация)**



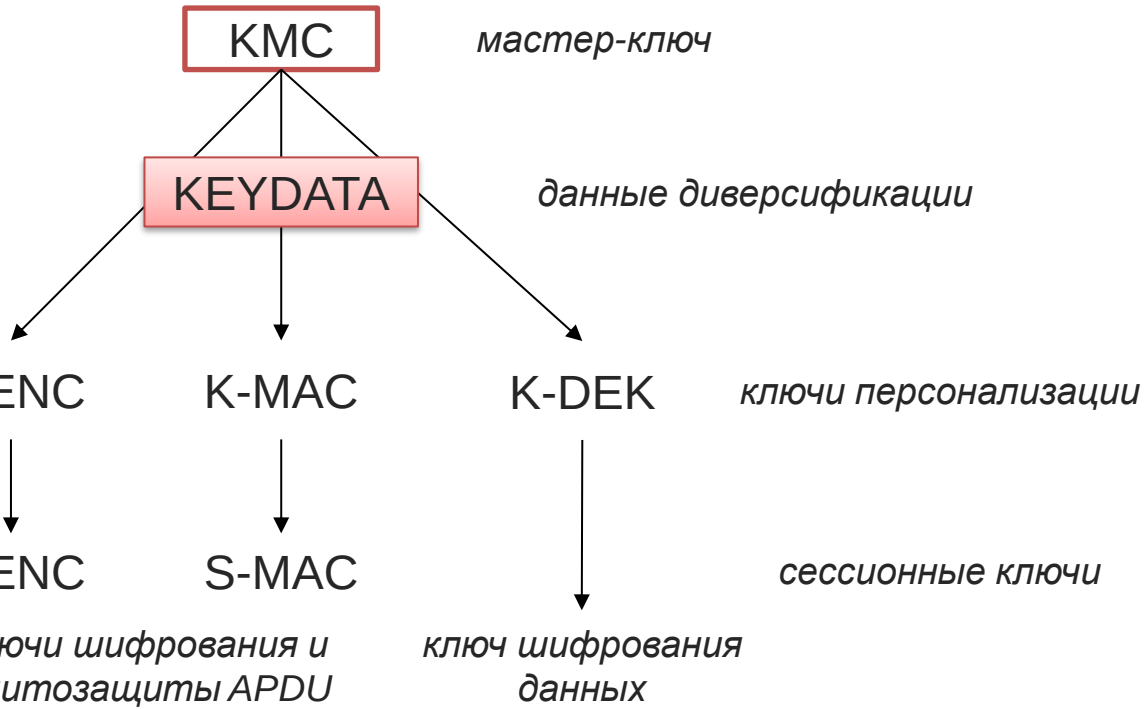
Ключевая схема персонализации

РусКрипто

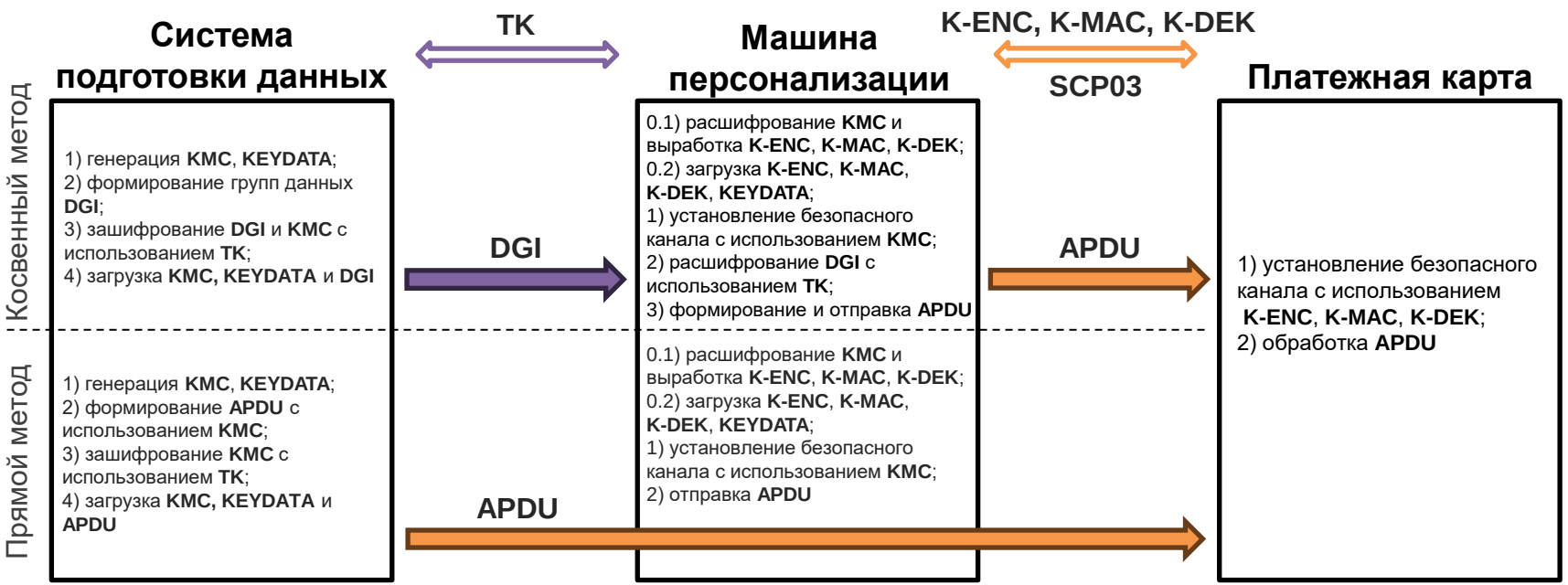
Загружается **на машину персонализации**

Загружаются **на карту** с использованием транспортных ключей **(пре-персонализация)**

Вырабатываются при установлении безопасного канала **(персонализация)**



Персонализация платежных карт



DGI – группы данных в формате TLV (Tag, Length, Value)
TK – транспортный ключ

EMV Card Personalization Specification v.2.0

KMC – мастер-ключ
K-ENC, **K-MAC**, **K-DEK** – ключи персонализации
KEYDATA – данные диверсификации ключей персонализации
0.N – пре-персонализация

Протокол SECUNDA

В 2023-2024 гг. в рамках НИР* АНО «НТЦ ЦК» был разработан защищенный универсальный протокол передачи данных и управления микросхемой интеллектуальной карты SECUNDA (secure universal protocol for downloading data and managing the smart card chip).

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

РусКрипто

Проект протокола был представлен на РусКрипто'2024 в докладе «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)».

Модели применения протокола SECUNDA в инфраструктуре сетей подвижной радиосвязи:

- процесс предварительной персонализации модулей аутентификации типа UICC /eUICC**;
- процесс дистанционного доведения цифровых профилей абонентов в модули аутентификации типа eUICC;
- процесс дистанционного управления цифровыми профилями абонентов.

* НИР «Исследование вариантов безопасного между хост-системой и микросхемами интеллектуальных карты (UICC, eUICC), применяемых в сетях подвижной радиосвязи», 2023 г.
* НИР «Исследование модели применения «Защищенного универсального протокола передачи данных и управления микросхемой интеллектуальной карты UICC / eUICC в сетях подвижной радиосвязи» (SECUNDA) в инфраструктуре перспективных сетей подвижной радиосвязи», 2024 г.

** UICC - Universal Integrated Circuit Card - универсальная интегральная карта
** eUICC - Embedded Universal Integrated Circuit Card – встроенная универсальная интегральная карта

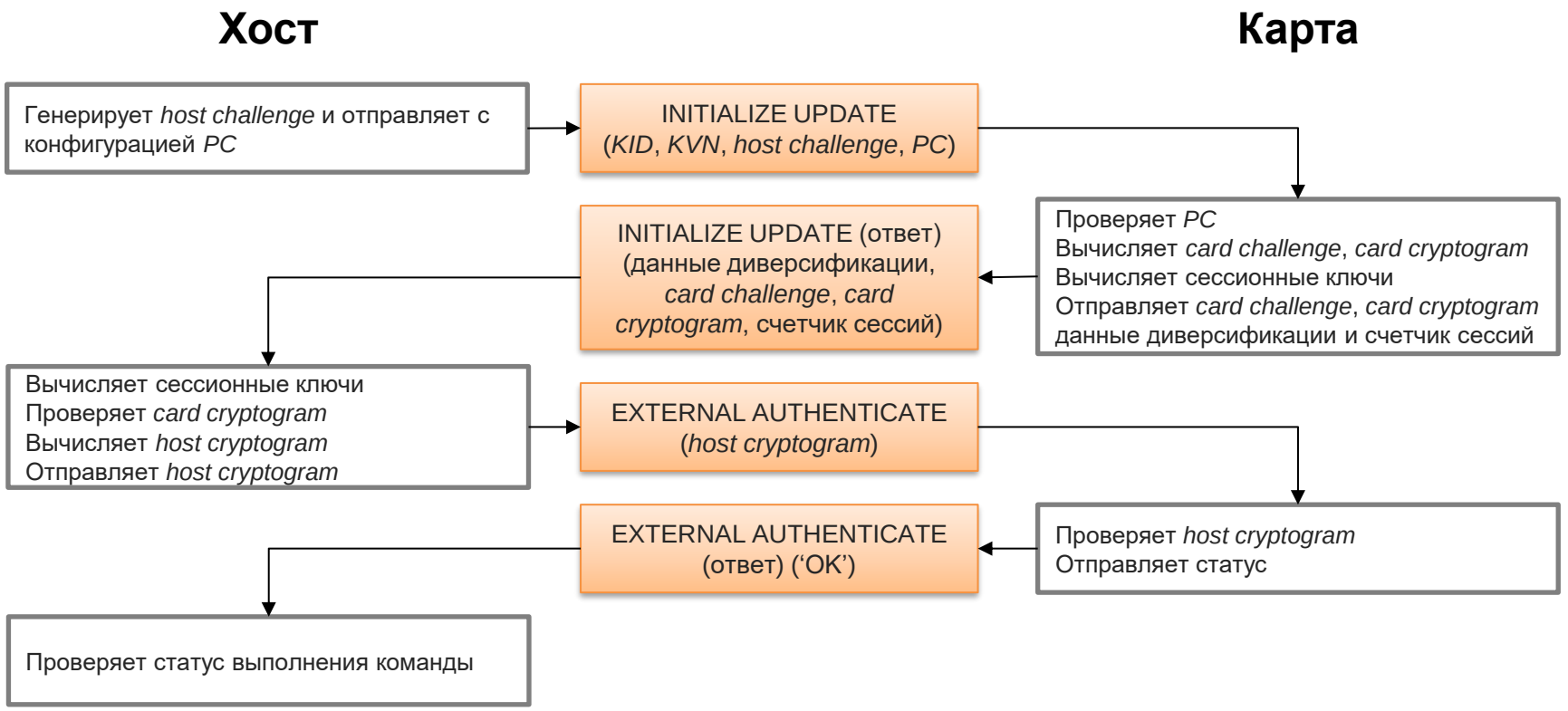
Взаимодействие по протоколу SECUNDA

1. Инициирование установления защищенного соединения, установление параметров конфигурации протокола. Инициатором выступает хост-система;
2. Взаимная аутентификация хост-системы 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).

РусКрипто

Формирование сессионных ключей в SECUNDA

РусКрипто



Формат сообщений протокола SECUNDA

РусКрипто

Командный пакет

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)	1
Индикатор конфиденциальных данных (CDI)	1
Индикатор цепочки (CHAIN)	1
Идентификатор приложения (TAR)	3
Счетчик пакетов (CNTR)	8
Длина дополнения (PCNTR)	1
Защищаемые данные (Secured Data)	$\leq L_{MAX}$
Имитовставка (CC)	8 или 16

Ответный пакет

Поле	Длина (в байтах)
Идентификатор ответного пакета (RPI)	1
Длина ответного пакета (RPL)	Переменная
Идентификатор заголовка ответа (RHI)	1
Длина заголовка ответа (RHL)	1
Индикатор цепочки (CHAIN)	1
Идентификатор приложения (TAR)	3
Счетчик пакетов (CNTR)	8
Длина дополнения (PCNTR)	1
Код статуса ответа (RSCO)	1
Защищаемые данные (Secured Data)	$\leq L_{MAX}$
Имитовставка (CC)	8 или 16

Защищаемые данные – APDU-команды и APDU-ответы, соответствующие спецификациям GlobalPlatform

Сравнительный анализ протоколов SCP и SECUNDA

Параметры	SCP02	SCP03	SCP04	SECUNDA
Базовые ключи безопасного канала	K-ENC, K-MAC, K-DEK			K-ENC, K-MAC, K-DEK, K-DMAC
Сессионные ключи	S-ENC, S-MAC, S-DEK	S-ENC, S-MAC, S-RMAC		S-ENC, S-MAC, S-RENC, S-RMAC
Формирование базовых ключей из мастер-ключа	Поддерживается (данные диверсификации в ответе INITIALIZE UPDATE)			
Блочный шифр	DES	AES	AES, SM4	«Магма», «Кузнечик»
Режимы шифрования	CBC – команды ECB, CBC - данные	CBC	CBC, AES-GSM – команды CBC – данные	CTR, MGM – команды CTR – данные
Алгоритм имитозащиты	Retail MAC	CMAC		OMAC1
Смена ключа шифрования данных (DEK) для загрузки предварительно зашифрованных данных	Не поддерживается (нужно выполнить смену ключей безопасного канала)			Поддерживается (загрузка временных ключей PPK-DEK, PPK-DMAC после установления сессии)
Контроль целостности дефрагментированных данных	Не поддерживается			Поддерживается (K-DMAC)
APDU, выполняемые в процессе установления безопасного канала	SELECT, INITIALIZE UPDATE, EXTERNAL AUTHENTICATE			GET DATA, INITIALIZE UPDATE, EXTERNAL AUTHENTICATE

РусКрипто

Выводы

РусКрипто

Протокол SECUNDA решает те же задачи, что и протоколы SCP, а именно:

- ✓ конфиденциальность загружаемых данных;
- ✓ контроль целостности передаваемых сообщений;
- ✓ контроль очередности передаваемых сообщений/данных;
- ✓ дополнительный контур защиты конфиденциальных данных.

Протокол SECUNDA решает дополнительные задачи:

- ✓ контроль целостности дефрагментированных данных;
- ✓ использование временных ключей для шифрования конфиденциальных данных и переход на них после установления сессии;
- ✓ передача нескольких APDU-команд из цепочки (STORE DATA) в одном сообщении.

Выводы

РусКрипто

Таким образом, протокол SECUNDA может заменить используемые протоколы SCP в процессе эмиссии платежных карт, обеспечивая при этом:

- ✓ выполнение требований регуляторов по использованию российских криптографических алгоритмов;
- ✓ дополнительные функции безопасности;
- ✓ оптимизацию процессов подготовки и загрузки данных;
- ✓ гибкую настройку используемых криптографических алгоритмов.

Процесс	Использование протокола SECUNDA
Загрузка приложений	✓
Пре-персонализация	✓
Персонализация	✓

Реализация протокола SECUNDA в домене безопасности на уровне операционной системы с аппаратной поддержкой криптопримитивов позволит российским производителям микросхем использовать единые решения как для SIM/eSIM, так и для платежных карт

Заключение

РусКрипто

Текущий план работ

- Разработка методических рекомендаций ТК 26 протокола SECUNDA в рамках рабочей группы «Криптографические механизмы для подвижной радиотелефонной связи».
- Проработка модели применения протокола SECUNDA в процессе эмиссии платежных карт для расширения области применения протокола SECUNDA.

РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ