Программный модуль операционной системы смарт-карт, реализующий подсистему передачи данных по радиочастотному интерфейсу стандарта ГОСТ Р ИСО/МЭК 14443

Руководство оператора

Версия: 1.0 от 14.04.2023

Количество листов: на 14 листах

Москва, 2023

Общество с ограниченной ответственностью «СКОН ТЕХНОЛОГИИ»
Юридический адрес: 115230, город Москва, Электролитный проезд, д. 1 к. 3, помещ./этаж х/3 ком. 9, 13
ИНН 9726018244, КПП 772601001, р/с 40702810000000256170 в АО "Райффайзенбанк", г. Москва,
к/с 30101810200000000700, БИК 044525700, ОГРН 1227700461790
+7 925 011 30 07 | www.sconetech.ru

АННОТАЦИЯ

В данном программном документе приведено руководство оператора по настройке и проверке программного модуля операционной системы смарт-карт, реализующего подсистему передачи данных по радиочастотному интерфейсу стандарта ГОСТ Р ИСО/МЭК 14443.

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Таблица 1. Термины и определения

APDU	Application Protocol Data Unit – тип управляющих команд, используемых для интегральных схем. ГОСТ Р ИСО/МЭК 7816-4-2013 «Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена»
API	API (программный интерфейс приложения, интерфейс прикладного программирования) (англ. application programming interface, API [эй-пи-ай]) – описание способов (набор классов, процедур, функций, структур или констант), которыми одна программа может взаимодействовать с другой программой.
RF	Радиочастотный интерфейс по стандарту ГОСТ Р ИСО/МЭК 14443
МК	Микроконтро́ллер (англ. Micro Controller Unit, MCU) – микросхема, предназначенная для управления электронными устройствами, банковскими картами
ОС	Операционная система смарт-карт (англ. operating system smart cards, OS smart cards) – комплекс взаимосвязанных программ, предназначенных для управления ресурсами МК и организации взаимодействия с пользователем по средствам интерфейсов ввода\вывода.
ПО	Программное обеспечение
Платежное приложение (ПП)	Прикладное программного обеспечение, сертифицируемое ПС
Платежная система (ПС)	Платежные системы осуществляют перевод финансовых средств (денег, чеков, ценных бумаг, сертификатов, условных платёжных единиц) в электронном или реальном виде. Платежная система являет собой совокупность определенных процедур, правил и технической инфраструктуры для передачи стоимости одним субъектом экономики другому

2. НАЗНАЧЕНИЕ ПРОГРАММЫ

2.1. Функциональное назначение программы

Программный модуль операционной системы, реализующих функции приема-передачи данных APDU-команд через радиочастотный (RF) интерфейс по стандарту ГОСТ Р ИСО/МЭК 14443 на платформе микроконтроллеров в процессе жизненного цикла операционной системы смарт-карт, платежных приложений, позволяющих осуществлять банковские транзакции, в соответствии с требованиями платежных систем МИР, VISA, MasterCard, неплатежных дополнительных приложений, предназначенных для идентификации и аутентификации владельца карты, при ее применении для проезда на общественном транспорте, использовании в социальной сфере (социальные карты), использовании карты в системах контроля и управления доступом и др.

2.2. Эксплуатационное назначение программы

Программный модуль операционной системы смарт-карт обеспечивает безопасный прием и передачу данных во время жизненного цикла операционной системой и прикладных приложений по радиочастотному интерфейсу.

2.3. Описание функции модуля

Вызов функций модуля осуществляется при помощи интерфейса APDU команды со следующим синтаксисом:

2.3.1. Функция отправки и получения эхо ответа

Запуск трансивера в соответствии с ГОСТ Р ИСО/МЭК 14443 с учетом текущего состояния.

Эта функция отправит данные APDU и вернет следующую полученную APDU к клиентской ОС.

Синтаксис команды представлен в таблице 2.

Таблица 2. Структура команды

Поле	**Значение**	**Описание**
CLA	'80'	
INS	‘EE’	80EE0000023B8400
P1	‘00’	

P2	‘00’	
L_C	‘NN’	Длина данных команды
Data[1..NN]		Данные команды
Le	‘00’	

Смарт карта возвращает последовательность элементов следующего вида, представленных в таблице 3.

Таблица 3. Ответные данные

Длина	**Значение**
NN	Данные

2.4. Описание команд загрузки модуля в составе ОС на МК

2.4.1. Функция запроса случайного числа МК, MUTUAL CHALLENGE

Синтаксис команды представлен в таблице 4.

Таблица 4. Структура команды

Поле	**Значение**	**Описание**
CLA	'C0'	
INS	‘C3’	
P1	‘00’	
P2	‘00’	
L_C	‘06’	Длина данных запроса случайного числа МК
Data	‘00 53 00 02 00 81 00’	Данные для запроса случайного числа

Смарт карта возвращает последовательность элементов следующего вида, приставленных в таблице 5.

Таблица 5. Ответные данные

Длина	**Значение**
90 53 00 10 xx..xx	xx..xx – случайное число, 16 байт

2.4.2. Функция аутентификации с МК, MUTUAL AUTHENTICTION

Синтаксис команды представлен в таблице 6.

Таблица 6. Структура команды

Поле	**Значение**	**Описание**
CLA	'C0'	
INS	‘C3’	
P1	‘00’	
P2	‘00’	
L_C	‘64’	Длина данных аутентификации
Data	64 00 54 00 60 Token AB 00	Token AB – данных для аутентификации для МК, 96 байт

Смарт карта возвращает последовательность элементов следующего вида, приставленных в таблице 7.

Таблица 7. Ответные данные

Длина	**Значение**
90 54 00 50 Token BA	Token BA – данных для аутентификации от МК, 96 байт

2.4.3. Функция загрузки микропрограммы МК FLASH LOAD DATA

Синтаксис команды представлен в таблице 8.

Таблица 8. Структура команды

Поле	**Значение**	**Описание**
CLA	'C0'	
INS	‘C3’	

Поле	Значение	Описание
P1	‘00’	
P2	‘00’	
L_C	‘XX’	Длина данных микропрограммы МК
Data	‘AA’	Данные микропрограммы МК

3. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Модуль имеет архитектуру типа монолит и представляет собой подготовленные для подключения к основному проекту ОС смарт-карт файлы исходного кода c,h.

Загрузка модуля во встроенную память микропроцессорной карты в составе ОС смарт-карт осуществляется с помощью APDU-команд согласно протоколу по ГОСТ Р ИСО/МЭК 7816, либо ГОСТ Р ИСО/МЭК 14443.

3.1. Минимальный состав программно-аппаратных средств

Программно-аппаратные требования смарт карт представлены в таблице 9.

Таблица 9 – Программные, аппаратные требования смарт карт

Наименование требования	Значение
Среда разработки	
Среда разработки	Eclipse IDE
Компилятор	GNU ARM Embedded Toolchain
Язык разработки	C
Артефакты разработки	Файлы исходного кода, заголовочные файлы, файлы библиотек
Аппаратные требования	
Семейство микроконтроллеров	Infineon SLC36PD, SAMSUNG S3D350A и другие
Криптографический сопроцессор	SCP
Безопасность	В составе ОС смарт-карт
Объем ПЗУ \Flash	20 KB
Объем ОЗУ\RAM	6 KB
Подсистема ввод-вывод - Радиоинтерфейс	
Размер приемопередающего буфера	256 КБ
Скорость передачи	116 бит/с
Несущая частота	14,7 МГЦ

3.2. Требования к составу периферийных устройств

Включая, но не ограничиваясь, семейства МК Infineon SLC36PD и Samsung S3D350A.

Устройства чтения/записи смарт-карт, например, PC\SC кард-ридеры с радиоинтерфейсом.

3.3. Требования к персоналу (оператору)

Пользователь должен обладать практическими навыками владения персонального ПК, иметь знания в области смарт-карт, обладать практическими навыками системного программирования для МК.

4. ПРИМЕР РАБОТЫ С ПРИЛОЖЕНИЕМ

4.1. Загрузка модуля

Ниже представлен пример загрузки модуля на МК в составе ОС смарт-карт, соответствующей требованиям раздела 3.2:

МК	APDU интерфейс	Управлявшее прикладное ПО и устройство работы со смарт-картами	Комментарий
	← Reset		
	ATR bootloader [3B 10 96/97]		
	1. Mutual Authentication		
	← GET ITEM Kc LABEL [c0 c3 00 00 08 00 50 00 04 00 80 00 00 00]		
	90 80 00 02 AA BB + SW 9000 →		
	← GET ITEM Kd LABEL [c0 c3 00 00 08 00 50 00 04 00 81 00 00 00]		
	90 81 00 02 CC DD+ SW 9000 →		
	← GET ITEM Kfdi LABEL [c0 c3 00 00 08 00 50 00 04 00 82 00 00 00]		
	90 82 00 02 EE FF+ SW 9000 →		
	← MUTUAL CHALLENGE [c0 c3 00 00 06 00 53 00 02 00 81 00]		
	90 53 00 10 fd 5e ef e0 b3 c1 24 8f 7c 6a a1 54 a0 7b ff 75 + SW 9000 →		
	← MUTUAL AUTHENTICTION [c0 c3 00 00 64 00 54 00 60 Token AB 00]		

МК	APDU интерфейс	Управлявшее прикладное ПО и устройство работы со смарт-картами	Комментарий
	90 54 00 50 Token BA+ SW 9000 →		
	←INVALIDATE USER NVM [c0 c3 00 00 04 00 60 00 00]		
	SW 9000 →		
	← FLASH LOAD DATA [c0 c3 00 00 xx +Data]		
	SW 9000 →		
	….		
	← SET STARUP OS [c0 c3 00 00 06 00 61 00 02 00 01]		
	SW 9000 →		

4.2. Персонализация приложения через модуль

Ниже представлен пример персонализации приложения с помощью модуля на МК в составе ОС смарт-карт, соответствующей требованиям раздела 3.2:

Модуль	APDU интерфейс	Управлявшее прикладное ПО и устройство работы со смарт-картами	Комментарий
	← Reset		
	ATR →		
	Построение безопасного канала с менеджером карты		
	← SELECT AID ISD/CM		Выбор менеджера карты по AID
	FCI ISD/CM + SW 9000 →		
	← INITIALIZE UPDATE		Взаимная аутентификация, протокол
	DATA + SW 9000 →		

Модуль	APDU интерфейс	Управлявшее прикладное ПО и устройство работы со смарт-картами	Комментарий
	←EXTERNAL AUTHENTICATE		
	SW 9000 →		
	Инсталляция экземпляра апплета		
	←INSATLL FOR INSATLL and MAKE SELECTABLE 80E60C003B0C325041592E5359532E4444460E325041592E5359532E44444630310E325041592E5359532E444446303101000CC90AA508BF0C0561034F01110000		Инсталляция экземпляра приложения AID 325041592E5359532E444446303100
	00 + SW 9000 →		
	Персонализация экземпляра апплета		
	← SELECT AID 325041592E5359532E444446303100		Выбор экземпляра приложения AID 53434F6E65566974616C446174610101
	FCI + SW 9000 →		

4.3. Чтение данных приложения через модуль

Ниже представлен пример чтения данных приложения через модуль, загруженный на МК в составе ОС смарт-карт, соответствующей требованиям раздела 3.2:

Модуль	APDU интерфейс	Управлявшее прикладное ПО и устройство работы со смарт-картами	Комментарий
	← Reset		
	ATR →		
	← SELECT AID 325041592E5359532E444446303100		Выбор экземпляра приложения AID 325041592E5359532E444446303100

Модуль	APDU интерфейс	Управлявшее прикладное ПО и устройство работы со смарт-картами	Комментарий
	FCI + SW 9000 →		
	← ECHO [80EE0000023B8400]		Отправка данных
	3B84 + SW 9000 →		ECHO ответ