Операционная система встраиваемого модуля безопасности "ОС РуСим МБ"

Описание программы (Функциональные характеристики)

ТРБП.10003-01.1

Листов 19

АННОТАЦИЯ

Настоящий документ является описанием программного комплекса (далее – ПК) "Операционная система РуСим встраиваемого модуля безопасности" ТРБП.10003-01.1 ("ОС РуСим встраиваемого модуля безопасности", далее по тексту – "ОС РуСим МБ" или "программа").

В документе приведены общие сведения о программе:

- описание функциональных характеристик ОС РуСим встраиваемого модуля безопасности являющейся составной частью модуля безопасности для использования в интеллектуальных приборах учета и аналогичных направлениях;
- описаны логическая структура и алгоритм работы программы;
- указаны технические средства, которые используются при работе программы, способы её вызова и загрузки, входные и выходные данные.

Оглавление

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование и обозначение программы.

Наименование программы: Программный комплекс "Операционная система РуСим встраиваемого модуля безопасности" (сокращенно "ОС РуСим МБ").

Обозначение программы: ТРБП.10003-01.1.

1.2. Программа не требует для своего функционирования какого-либо специального или общесистемного программного обеспечения (далее – ПО).

1.3. Языки программирования

При разработке программы использованы следующие языки программирования, запросов, представления и визуального моделирования:

– язык программирования C;
– язык программирования Assembler для архитектуры ARM Cortex M;
– среда разработки и отладки приложений Keil ARM, Eclipse.

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1.Программа предназначена для обеспечения функционала безопасности (конфиденциальность, целостность, аутентичность) в интеллектуальных приборах учета и аналогичных направлениях.

2.2.Программа обеспечивает решение следующих функциональных задач:

– хранение и генерация в неизвлекаемом виде криптографических ключей;

– шифрование данных;

– формирование электронной подписи;

– организация защищенного обмена в рамках протокола CRISP;

2.3.Программа является ПО, все компоненты которого должны инсталлироваться («прошиваться») в модуль безопасности при его изготовлении.

2.4.Общие функциональные ограничения программы

2.4.1. Программа предоставляет инфраструктуру и средства для обеспечения безопасности при реализации прикладной функциональности в интеллектуальных приборах учета и аналогичных направлениях.

2.4.2. Основной задачей программы, установленной в модуль безопасности, является обеспечение надежной работы с криптографическими ключами, в рамках всего жизненного цикла.

3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1. Структура программы

3.1.1. Программа является встраиваемой операционной системой модуля безопасности.

3.1.2. Программа является встраиваемой системой, выполнение функционала которой связано с правильной работой аппаратных средств модуля безопасности, а именно микроконтроллера (МК). Применение программы без использования аппаратных средств модуля безопасности является невозможным.

3.2. Встраиваемая ОС модуля безопасности.

3.2.1. ОС модуля безопасности удовлетворяет требованиям стандартов, приведенных в таблице 1.

Таблица 1

№ п/п	Наименование стандарта
1.	**ГОСТ**
1.1.	ГОСТ 34.10-2018
1.2.	ГОСТ 34.11-2018
1.3.	ГОСТ 34.12-2018
1.4.	ГОСТ 34.13-2018
2.	**Методические рекомендации и рекомендации по стандартизации**
2.1.	Р 1323565.1.029-2019
2.2.	Р 1323565.1.017-2018
2.3.	Р 50.1.113-2016

3.2.2. ОС модуля безопасности включает в себя следующие компоненты:

– библиотека функций работы с памятью;
– функции поддержки физического уровня операций ввода-вывода;
– реализацию криптографических алгоритмов
– реализацию прикладной логики работы

3.2.3. Библиотеки функций работы с памятью интегрированы с первичным программным обеспечением, предоставляемым непосредственно производителем МК. Они включены в пакет примеров, прилагаемых к спецификации и отладчику для конкретного МК.

3.2.4. Операции ввода-вывода выполнены на МК до физического уровня. Знание адресного пространства, где располагается буфер обмена, и сигнальных признаков событий получения байта реализует низкоуровневую функцию контроля ввода вывода, согласно установленному физическому протоколу. Протокол подробно описан в стандарте ISO7816-3. Это обычный последовательный полудуплексный канал с использованием переговоров о параметрах передачи вначале установления канала при подаче питания на МК.

На данном низком уровне обработка ввода-вывода необходима для проверки корректности протокола, проверки паритета и управления ожиданием.

3.2.5. Архитектура МК исключает возможность использования динамической загрузки компонент в защищенную от записи область ROM (FLASH). Поэтому никакой угрозы функциональному ограничению такой подход не имеет. При подготовке ROM весь двоичный код образа уже связан адресами с вызовами внутри себя и исключает какое-либо динамическое переприсвоение.

3.2.6. Постоянное хранилище данных ОС модуля безопасности состоит из следующих сегментов

1) Конфигурационная область;
2) Сегмент ключевых пара;
3) Сегмент симметричных ключей;
4) Сегмент открытых ключей

4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

4.1. Условием работы программы является наличие технических (аппаратных) средств с параметрами, удовлетворяющими следующим требованиям:

– микроконтроллер с ПЗУ не менее 20 кбайт и ОЗУ не менее 4096 байт;

– интегральная схема карты с перезаписываемой памятью (ROM – ППЗУ) размером не менее 132 кбайт.

4.2. Программа обеспечивает поддержку следующих аппаратных платформ в уточняемых конфигурациях:

– Samsung SC000 ARM (TM) S3D350A.

– Infineon SC300 ARM (TM) SLM97CFX1M00PE;

– HUADA семейство CIU98*

– TMC семейство THD89;

– KMXSCE;

– Микрон MIK51AD144D.

Портирование и доработка прорабатываются и применимы для различных аппаратных платформ соответствующей конфигурации.

4.3. Программа не требует для своего функционирования какого-либо специального или общесистемного программного обеспечения.

5. ВЫЗОВ И ЗАГРУЗКА

5.1. Программа начинает функционировать при подаче напряжения питания и старте работы МК модуля безопасности под управлением "ОС РуСим МБ", дополнительных действий для вызова программы не требуется.

6. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

6.1. Входными данными программы являются данные, получаемые ПК, установленным на модуле безопасности, от интеллектуального прибора учета по заранее определенным правилам. Данные правила должны соответствовать ГОСТ Р ИСО/МЭК 7816-3-2013 и ГОСТ Р ИСО/МЭК 7816-4-2013.

6.2. Выходными данными программы являются ответы команд и возвращаемые ими данные "ОС РуСим МБ".

7. ИНСТАЛЛЯЦИЯ ПРОГРАММЫ

7.1. Инсталляция программы производится путем загрузки образа (маски) "ОС РуСим МБ" встраиваемого модуля безопасности на интегральную схему в процессе ее изготовления (этап 5 жизненного цикла продукта – см. Приложение 2).

8. НАСТРОЙКА ПРОГРАММЫ

8.1. Порядок настройки программы описан в блок-схеме, представленной на рисунке 1.

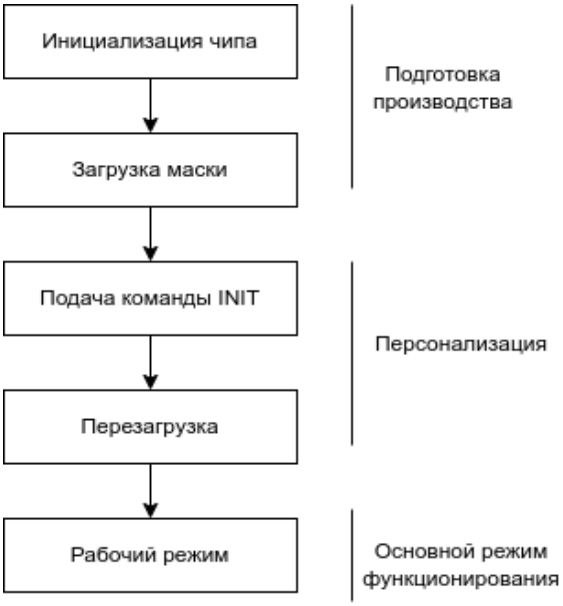

Рисунок 1

9. ПРОВЕРКА ПРОГРАММЫ

9.1. Для проверки работоспособности программы нам необходимо убедиться в том, что команда GENERATE RANDOM выполняется успешно.

9.2. Программа считается работоспособной, если команда GENERATE RANDOM выполняется успешно.

10.НАЧАЛО РАБОТЫ С ПРОГРАММОЙ

10.1.Программа начинает функционировать при подаче напряжения питания и старте работы МК модуля безопасности под управлением "ОС РуСим МБ", дополнительных действий для вызова программы не требуется.

11.ВЫПОЛНЕНИЕ ПРОГРАММЫ

11.1.Общие сведения о работе с программой

11.1.1Запуск программы

Программа начинает функционировать при подаче напряжения питания и старте работы МК модуля безопасности под управлением "ОС РуСим МБ", дополнительных действий для вызова программы не требуется.

11.1.2 Завершение работы с программой

Завершение работы программы происходит при прерывании питания МК модуля безопасности.

ПРИЛОЖЕНИЕ 1. ОПРЕДЕЛЕНИЯ

APDU (Application Protocol Data Units)	Стандартный коммуникационный протокол обмена сообщениями между устройством считывания карт (ME) и смарт-картой (модулем безопасности).
Приложение (Application)	Приложение состоит из набора механизмов безопасности, файлов, данных и протоколов (за исключением протоколов передачи).
Асимметричное шифрование (Asymmetric Cryptography)	Метод шифрования, использующий два взаимосвязанных преобразования: публичное преобразование (определяемое компонентом публичного ключа) и закрытое преобразование (определяемое компонентом секретного ключа); эти два компонента имеют следующее свойство: невозможно вычислить закрытый ключ, даже если известен публичный ключ.
Открытый текст (Clear Text)	Незашифрованная информация.
Криптограмма (Cryptogram)	Результат операции шифрования.
Криптографическая контрольная сумма (Cryptographic Checksum)	Преобразование данных методом симметричного шифрования, обеспечивающее проверку подлинности источника данных и их целостность.
Электронная подпись (Digital Signature)	Преобразование данных методом асимметричного шифрования, позволяющее получателю доказать происхождение и целостность данных; электронная подпись защищает отправителя и получателя от подделки данных третьими лицами; она также защищает от подделки отправителя получателем.
Код проверки подлинности сообщения, MAC (Message Authentication Code)	Преобразование данных методом симметричного шифрования, обеспечивающее проверку подлинности источника данных и их целостность.
Контроль избыточности (Redundancy Check)	Преобразование данных, позволяющий получателю проверить целостность данных без использования секретного ключа.
Симметричное шифрование (Symmetric Cryptography)	Метод шифрования, использующий одинаковый секретный ключ для преобразований на стороне отправителя и на стороне получателя; без знания секретного ключа затруднительно вычислить преобразования отправителя/получателя.

ПРИЛОЖЕНИЕ 2. ЖИЗНЕННЫЙ ЦИКЛ "ОС РУСИМ МБ"

Жизненный цикл "ОС РуСим МБ" является частью жизненного цикла продукта, т. е., модуля безопасности – от стадии разработки до использования абонентом (Таблица П1).

Инсталляция "ОС РуСим МБ" осуществляется на стадии (этап 5, таблица П1) при производстве модуля безопасности, при этом результат на этой стадии – инициализированный модуль безопасности.

Таблица П1

№этапа ЖЦ[1]	**Интегрированный продукт модуль безопасности[2]**	**Применяемый микроконтроллер – (ИС[3])**	**Разрабатываемый ПК ОС РуСим МБ — встраиваемого модуля безопасности**
Этап 1	Разработка (проектирование) ВПО[4] для ИС	Разработка прошивки (ВПО) ИС	Разработка (проектирование) ОС
Этап 2		Разработка ИС (проектирование, разработка структуры, логической и (или) электрической принципиальной схемы ИС, топологии ИС)	Осуществление доставки образа разработанной ОС на производство.
Этап 3		Производство ИС (полный цикл от пластины к кристаллу)	Хранение файлов разработчика ОС на производстве, подготовка к персонализации, тестирование ОС
Этап 4		Упаковка ИС (корпусирование)	Хранение файлов разработчика ОС на производстве, подготовка к персонализации, тестирование ОС
Этап 5	Инициализация модуля безопасности. Комплектация составного продукта (внедрение компонентов программного обеспечения в ИС)	Сборка ИС, ВПО, платформы	ОС – платформа инсталлируется в модуль безопасности

1 ЖЦ – жизненный цикл.
2 Интегрированный продукт сим-карта включает в себя ИС с установленным на нее ВПО.
3 ИС – интегральная схема.
4 ВПО – встроенное программное обеспечение (Chip firmware, OS, applets, user code).

Этап 6	Персонализация продукта, предшествующая его использованию (внедрение данных серийного номера и инициализации)	Персонализация (Сборка ИС, ВПО, ОС – платформы, данных серийного номера и инициализации)	Персонализация ОС – платформы. В инициализированную ОС дополнительно внедряются данные серийного номера, доверенный стартовый вектор.
Этап 7	Эксплуатация	Эксплуатация ИС в составе модуля безопасности	Эксплуатация ОС – платформы в составе модуля безопасности
Этап 8	Сбор возникающих проблем у конечных пользователей и внесение информации о них в систему отслеживания проблем (bugtracker) для последующего устранения.	Сбор возникающих проблем у конечных пользователей и внесение информации о них в систему отслеживания проблем (bugtracker) для последующего устранения.	Сбор возникающих проблем у конечных пользователей и внесение информации о них в систему отслеживания проблем (bugtracker) для последующего устранения.

Процесс инициализации состоит в выполнении циклов операций, состоящих из загрузки команды внешним устройством в буфер чип-карты, выполнении команды чип-картой и возврате чип-картой сообщения о результате выполнения команды внешнему устройству.

Перед операцией загрузки внешним устройством формируют блок команд, содержащий административную команду, в которой в качестве данных используются несколько команд, подаваемых на карту, выполняют упомянутый блок команд и возвращают сообщение о результате выполнения блока команд внешнему устройству. При этом количество команд в блоке должно быть максимально возможным для сокращения циклов обмена и определяется длиной команд, размером буфера команд, максимально допустимой длиной данных в используемом протоколе передачи.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

МК	–	микроконтроллер
ОС	–	операционная система
ПЗУ	–	постоянное запоминающее устройство
ПК	–	программный комплекс
ПО	–	программное обеспечение
ППЗУ	–	перезаписываемое постоянное запоминающее устройство
ПРТС	–	подвижная радиотелефонная связь