ОКБ АПР ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

УТВЕРЖДЕН

37222406.26.20.40.140.083:08 32–ЛУ

Специальное программное обеспечение «Резидентный компонент безопасности»

РУКОВОДСТВО СИСТЕМНОГО ПРОГРАММИСТА

37222406.26.20.40.140.083:08 32

Подп. и дата | Инв. № дубл. | Взаим. инв. № | Подп. и дата | Инв. № подл.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

ICSP	–	In Circuit Serial Programming
USB	–	Universal Serial Bus
РКБ	–	Резидентный компонент безопасности
СПО	–	Специальное программное обеспечение

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1 Специальное программное обеспечение «Резидентный компонент безопасности», 37222406.26.20.40.140.083:08 (СПО «РКБ») предназначено для выполнения отчужденных от центрального процессора функций безопасности.

1.2 СПО «РКБ» имеет следующие функциональные возможности:

- генерацию, хранение и использование ключевой информации;
- хранение базы данных СПО СДЗ «Аккорд-МКТ»;
- передача случайных чисел от датчика случайных чисел;
- поддержка интерфейса USB.

2. СТРУКТУРА ПРОГРАММЫ

2.1 Текст программы написан на языке С.

2.2 СПО «РКБ» реализовано в виде бинарного файла (файла firmware) и в заводских условиях устанавливается на микроконтроллер РКБ по технологии ICSP.

3. РАБОТА С ПРОГРАММОЙ

3.1 Работа с СПО «РКБ», установленным на микроконтроллер РКБ, производится из прикладного ПО через прикладной интерфейс, реализуемый библиотекой librkb.

3.2 Набор функций, предоставляемых библиотекой:

Генерация неизвлекаемого ключа подписи

Команда подается прикладным ПО. По этой команде на основе случайной последовательности байт, полученных с ФДСЧ, firmware РКБ создается ключ подписи и записывается с во внутреннюю память РКБ.

Название команды: rkb_cmd_gen_sign_key

Входные параметры: отсутствуют

Выходные данные: код ошибки с возможными значениями: SIGN_KEY_GEN_ERR, SUCCESS (см. Таблицу 1)

Получение ключа проверки подписи

Команда подается прикладным ПО. По этой команде вырабатывается ключ проверки подписи, соответствующий неизвлекаемому ключу подписи, и передается в процессор.

Название команды: rkb_cmd_gen_verify_key

Входные параметры: отсутствуют

Выходные данные: код ошибки с возможными значениями: VERIFY_KEY_BUFFER_TOO_SMALL, VERIFY_KEY_GEN_ERR, SUCCESS (см. Таблицу 1), длина массива ключа проверки подписи (verify_key_len), массив ключа проверки подписи (verify_key)

Расшифрование сессионного ключа

Команда подается прикладным ПО. По этой команде полученный зашифрованный сессионный ключ расшифровывается на ключе защиты ключей, который в свою очередь вырабатывается на основе неизвлекаемого ключа подписи и переданного ключа проверки подписи.

Название команды: rkb_cmd_extract_session_key

Входные параметры: длина массива ключа проверки подписи (verify_key_len), массив ключа проверки подписи (verify_key), длина массива зашифрованного

сессионного ключа (crypted_session_key_len), массив зашифрованного сессионного ключа (crypted_session_key)

Выходные данные: код ошибки с возможными значениями: VERIFY_KEY_BUFFER_TOO_SMALL, CRYPTED_SESSION_KEY_BUFFER_TOO_SMALL, EXTRACT_SESSION_KEY_ERR, SUCCESS (см. Таблицу 1), длина массива сессионного ключа (session_key_len), сессионный ключ (session_key)

Получение последовательности случайных чисел

Команда подается прикладным ПО. По этой команде происходит получение случайных чисел с шумовых диодов, их обработка, контроль качества и запись в массив.

Название команды: rkb_cmd_get_rnd

Входные параметры: длина массива случайных чисел (len)

Выходные данные: код ошибки с возможными значениями: RND_GEN_ERR, SUCCESS (см. Таблицу 1), массив случайных чисел (buf)

Установка ключа подписи

Команда подается прикладным ПО. По этой команде происходит запись во внутреннюю память РКБ ключа подписи.

Название команды: rkb_cmd_set_sign_key

Входные параметры: длина ключа подписи (sign_key_len), массив ключа подписи (sign_key)

Выходные данные: код ошибки с возможными значениями: SIGN_KEY_SET_ERROR, SUCCESS (см. Таблицу 1)

Выработка подписи

Команда подается прикладным ПО. По этой команде происходит выработка подписи на основе ключа подписи и массива со значением хэша

Название команды: rkb_cmd_sign

Входные параметры: длина массива с хэшем (hash_len), массив с хэшем (hash)

Выходные данные: код ошибки с возможными значениями: SIGN_ERR, SUCCESS (см. Таблицу 1), длина массива подписи (sign_len), массив подписи (sign)

Сброс ключа подписи

Команда подается прикладным ПО. По этой команде происходит удаление ключа подписи из внутренней памяти РКБ

Название команды: rkb_cmd_reset

Входные параметры: отсутствуют

Выходные данные: код ошибки с возможными значениями: RESET_ERR, SUCCESS (см. Таблицу 1)

Проверка подписи

Команда подается прикладным ПО. По этой команде происходит проверка подписи на базе ключа подписи, массива со значением хэша и массива со значением подписи

Название команды: rkb_cmd_verify

Входные параметры: длина массива со значением хэша (hash_len), массив со значением хэша (hash), длина массива со значением подписи (sign_len), массив со значением подписи (sign)

Выходные данные: код ошибки с возможными значениями: HASH_BUFFER_TOO_SMALL, SIGN_BUFFER_TOO_SMALL, VERIFY_ERR, SUCCESS (см. Таблицу 1)

Установка сертификата

Команда подается прикладным ПО. По этой команде происходит запись во внутреннюю память РКБ сертификата.

Название команды: rkb_cmd_set_cert (uint32_t, uint8_t *)

Входные параметры: длина массива с сертификатом (cert_len), массив с сертификатом (cert)

Выходные данные: код ошибки с возможными значениями: TOO_MUCH_DATA, SET_CERT_ERR, SUCCESS (см. Таблицу 1)

Получение сертификата

Команда подается прикладным ПО. По этой команде происходит чтение сертификата из внутренней памяти РКБ.

Название команды: rkb_cmd_get_cert (uint32_t *cert_len, uint8_t *cert)

Входные параметры: отсутствуют

Выходные данные: код ошибки с возможными значениями: GET_CERT_ERR, SET_CERT_ERR, SUCCESS (см. Таблицу 1), длина массива с сертификатом (cert_len), массив с сертификатом (cert)

4. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

4.1 Перечень сообщений, получаемых системным программистом при работе с СПО «РКБ», отражен в таблице 1.

Таблица 1

Сообщение	Код
#define SUCCESS	0x0
#define VERIFY_KEY_BUFFER_TOO_SMALL	0x201
#define SESSION_KEY_BUFFER_TOO_SMALL	0x202
#define CRYPTED_SESSION_KEY_BUFFER_TOO_SMALL	0x203
#define SIGN_KEY_GEN_ERR	0x204
#define VERIFY_KEY_GEN_ERR	0x205
#define SESSION_KEY_GEN_ERR	0x206
#define EXTRACT_SESSION_KEY_ERR	0x207
#define RND_GEN_ERR	0x208
#define SIGN_KEY_BUFFER_TOO_SMALL	0x209
#define SIGN_KEY_SET_ERROR	0x20A
#define HASH_BUFFER_TOO_SMALL	0x20B
#define SIGN_ERR	0x20C
#define RESET_ERR	0x20D
#define SIGN_BUFFER_TOO_SMALL	0x20E
#define VERIFY_ERR	0x20F
#define TOO_MUCH_DATA	0x210
#define SET_CERT_ERR	0x211
#define GET_CERT_ERR	0x212