Акционерное общество «ИНТЕРСМАРТ»

ОГРН 1027735006056, Российская Федерация, 124482, город Москва, город Зеленоград, к.313А,
ИНН 7735115508, КПП 773501001, ФИЛИАЛ «ЦЕНТРАЛЬНЫЙ» БАНКА ВТБ (ПАО)
р/с 40702810400180001868, БИК 044525411, к/с 30101810145250000411, ОКТМО 45377000,
ОКПО 59697367, Телефон: +7(925) 415-94-45, e-mail: sim@i-smarts.ru

Описание операционной системы «Натрон 1.1» для USIM карт различных форм-факторов

на 11 листах

Правообладатель:

АО «Интерсмарт», г. Москва

Оглавление

1 Введение

Данный документ является функциональным описанием операционной системы для USIM-карт «Натрон 1.1» и представляет функциональное назначение и файловую структуру операционной системы, перечень соответствия стандартам, структуру и функции основных компонентов.

2 Функциональное назначение

Карточная Операционная Система «Натрон 1.1», далее – COS (Card Operating System) обеспечивает функционирование USIM-карт (Universal Subscriber Identity Module – Универсальный Модуль Идентификации Абонента) в абонентских устройствах подвижной радиотелефонной связи стандартов 2G, 3G/LTE с поддержкой алгоритма аутентификации на основе S3G.

Алгоритм S3G реализован в дополнительном программном обеспечении, разработанном третьим лицом - российской организацией - партнером Правообладателя.

Настоящая COS используется для производства USIM-карт в различных форм-факторах.

В операционной системе реализован интерфейс поддержки программного обеспечения партнера, реализующего функционал защищенного хранения ключей аутентификации, защищенного взаимодействия с энергонезависимой памятью и низкоуровневого ввода/вывода.

Программа является встроенной операционной системой, инсталлируется в ходе производственного цикла в энергонезависимую память чипа и не может быть использована вне аппаратных средств USIM-карты, а именно соответствующего микроконтроллера, имплантированного в USIM-карту.

Функционирование операционной системы «Натрон 1.1» происходит без прямого взаимодействия с Пользователем, потому что программа инсталлируется напрямую в энергонезависимую память микроконтроллера, встроенного в USIM-карты различных форм-факторов в ходе технологического процесса их производства.

Для работы программы установка и удаление программного обеспечения не требуется, а также к операционной системе «Натрон 1.1» не выдвигаются конкретные системные требования, потому что программа в ходе технологического процесса производства загружается непосредственно в энергонезависимую память чипа, инициализируется и взаимодействует с конкретным микроконтроллером после подачи питания на USIM-карту.

Функции операционной системы:

а) распределение памяти типов FLASH и RAM и работу с ней во взаимодействии с программным обеспечением партнера;

б) взаимодействие с программным обеспечением партнера с целью подготовки информации для подключения к сети оператора сотовой связи;

в) поддержка функциональности JCVM (JavaCard Virtual Machine) в соответствии со спецификацией JavaCard v.3.0.1;

г) реализация поддержки команд APDU в соответствии с требованиями стандартов ISO7816 и ETSI TS 102 221;

д) реализация поддержки команд из спецификации Global Platform v.2.2.1;

е) реализация поддержки стандартной функциональности SIM Toolkit по стандарту 3GPP TS 43 019, USIM Toolkit по стандарту ETSI TS 131 130, UICC Toolkit по стандарту ETSI TS 102 241;

ж) реализация поддержки функциональности RAM (Remote Application Management) и RFM (Remote File Management – удаленное управление файловой системой);

з) реализация функциональности коротких сообщений (SMS), одиночных и конкатенированных;

и) во взаимодействии с программным обеспечением партнера, подключение абонентского оборудования к сетям 2G, 3G/LTE оператора сотовой связи;

к) при обработке команд APDU, реализация одновременного функционирования нескольких логических каналов;

л) взаимодействие с абонентским оборудованием терминалом в процессе его работы в сетях 2G, 3G/LTE;

м) реализация функций файловой системы с USIM-карты в соответствии с требованиями стандартов ISO7816 и ETSI TS 102 221;

н) хранение настроечной информации в файловой структуре, размещенной на USIM-карте и соответствующей международным стандартам;

о) хранение телефонной книжки абонента в файловой структуре соответствующей стандарту 3GPP TS 31 102;

п) обеспечение защиты файловых транзакций от потери данных при незапланированном отключении питания (используется методика резервирования копии исходного содержимого и поэтапного подтверждения транзакции).

3 Перечень поддерживаемых стандартов

ISO (International Organization for Standardization - Международная Организация Стандартизации - ИСО):

- 7816-3
- 7816-4
- 7816-9

Global Platform (globalplatform.org – Глобальная Платформа):

- GPC Specification 2.2.1

ETSI (European Telecommunications Standards Institute - Европейский институт по стандартизации в области телекоммуникаций):

- TS 101 220
- TS 102 127
- TS 102 221
- TS 102 222
- TS 102 223
- TS 102 226
- TS 143 019
- TS 131 130
- TS 102 241
- TS 123 040
- TS 123 041
- TS 151 011

3GPP (3rd Generation Partnership Project – Проект партнерства 3-го поколения):

- TS 51.011
- TS 51.014
- TS 31.102
- TS 31.111
- TS 31.115
- TS 31.116

- TS 35.205
- TS 35.206
- TS 35.207
- TS 35.208
- TS 43.019
- TS 31.130
- TS 23.040
- TS 23.041

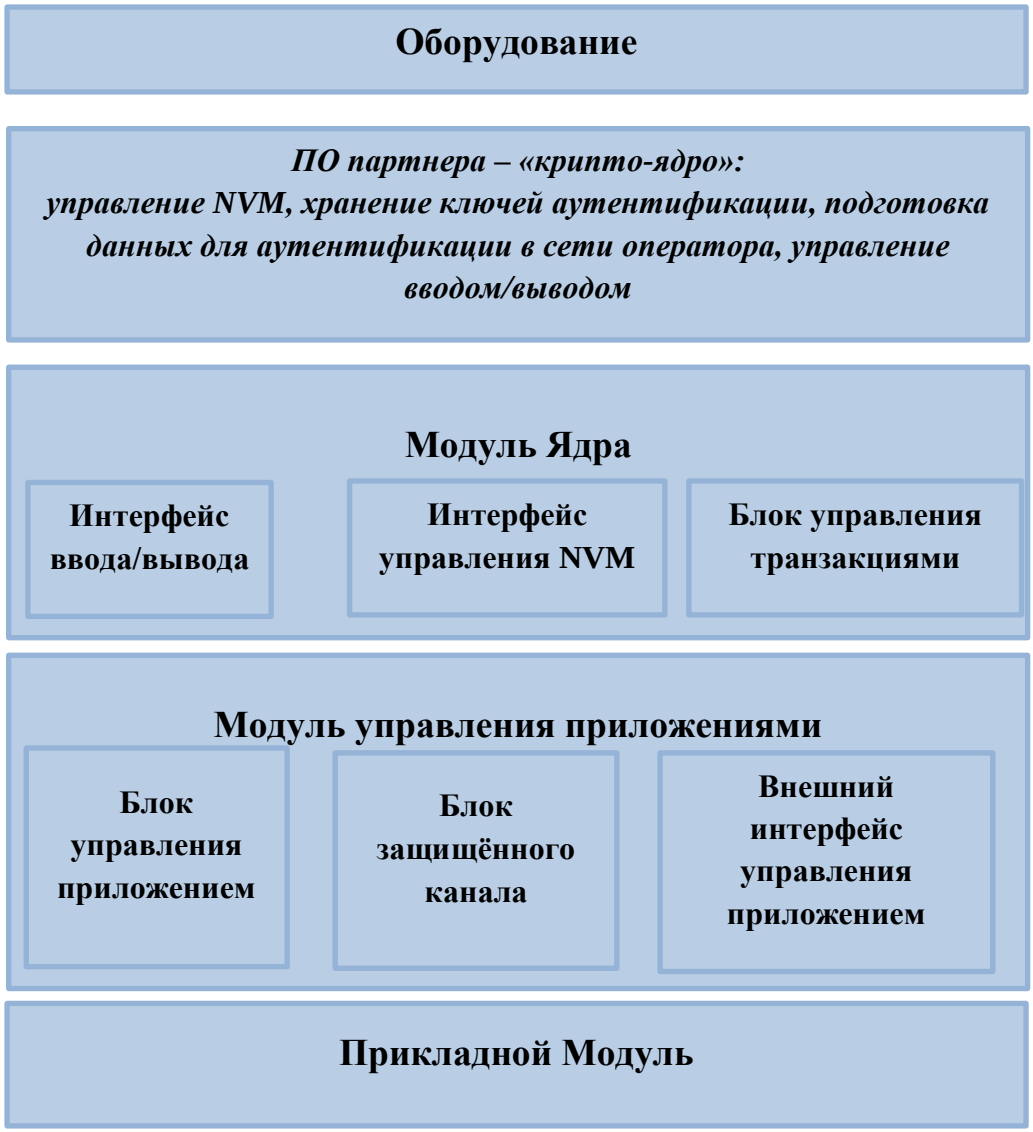
Java Card API specification, Runtime Environment Specification, Virtual Machine Architecture Specification 3.0.1 (Спецификация API Java Card, Спецификация среды времени выполнения, Спецификация архитектуры виртуальной машины 3.0.1)

4 Структура операционной системы «Натрон 1.1»

4.1 Модули операционной системы USIM карты

Операционная система USIM-карты состоит из Модуля ядра, Модуля управления приложениями и Прикладного Модуля.

Структура операционной системы «Натрон 1.1» представлена на следующем рисунке.



Функционал Модуля ядра: основные операции карточной операционной системы «Натрон 1.1», такие как приём и отправка данных ввода-вывода, чтение и запись данных в энергонезависимую память (NVM – Non-Volatile-Memory) микроконтроллера, встроенного в USIM-карту, производятся, в том числе посредством функционала программного обеспечения партнера - «крипто-ядра». Подготовка данных и команд для передачи и приема между абонентским оборудованием и смарт-картами различных форм-факторов и др. производится в Модуле ядра и передается в «крипто-ядро», которое взаимодействует с

оборудованием напрямую. Модуль ядра состоит из Интерфейса ввода/вывода, Интерфейса управления энергонезависимой памятью и Блока управления транзакциями. Интерфейс ввода-вывода обеспечивает обмен данными между USIM-картами и устройствами считывания карт посредством «крипто-ядра». Интерфейс управления NVM используется для хранения энергонезависимых данных в USIM-карте, обеспечивая функции чтения и записи в NVM, а также надежность и безопасность данных. Передача данных в NVM производится посредством «крипто-ядра». Блок управления транзакциями служит для предотвращения потери данных, вызванной отключением питания или программными ошибками в процессе обновления данных.

Функционал Модуля управления приложениями: обеспечение API (Application Programming Interface), в том числе в операционной системе «Натрон 1.1» реализован **интерфейс** поддержки программного обеспечения парнера, реализующего функционал защищенного хранения ключей аутентификации; установка, регистрация, удаление, распределение команд, выбор приложений и т.д., управление логическими каналами и управление содержимым карты для приложений в соответствии со стандартом Global Platform Specification v.2.2.1. Модуль управления приложениями состоит из Блока управления приложением, Блока защищенного канала и внешнего интерфейса управления приложением.

Функционал Прикладного Модуля реализует подготовку и проверку данных с целью подключения к сети операторов сотовой связи, в том числе с использованием интерфейса поддержки программного обеспечения партнера - «крипто-ядра», развертывание и обновление данных файловой системы, обеспечивает поддержку обработки инструкций APDU (протокола, используемого для обмена данными между устройствами согласно национальным и международным стандартам), а также обеспечивает поддержку обработки и управления данными на карте (создание, чтение, запись файлов и др.), в том числе с поддержкой алгоритма аутентификации на основе S3G.

4.2 Модуль ядра

Блоки, входящие в состав Модуля ядра, подразделяются на Интерфейс ввода/вывода, Интерфейс управления NVM, Блок управления транзакциями.

4.2.1 Интерфейс ввода/вывода (I/O)

На уровне ядра выполняется ввод и вывод данных с USIM-карты, чтение и запись в NVM. Интерфейс ввода/вывода выполняет передачу и прием данных и команд между ME (Mobile Equipment – мобильное/абонентское оборудование) и USIM-картой. Для обеспечения целостности передачи данных при вводе/выводе используется аппаратный механизм защиты целостности данных с использованием

критерия по четности, а также соответствующие меры защиты в программном обеспечении.

В процессе передачи символов ввода/вывода система добавляет механизм защиты целостности данных с использованием критерия по четности. Уведомление ME о повторной передаче с помощью индикации ошибок. Механизм ретрансляции реализуется аппаратными средствами микроконтроллера, а управление системой осуществляется через регистры, предоставляемые микроконтроллером.

4.2.2 Интерфейс управления энергонезависимой памятью (NVM)

Хранилища данных в USIM-картах можно условно разделить на следующие типы:

- Пакет CAP

- Значение статического объекта

- Параметры установки для приложения

- Значение объекта экземпляра

Для объединения управления вышеперечисленными типами данных определена таблица AddrIndexTable (Таблица индексов адресов) для управления всеми адресами в NVM. Код приложения должен сохранять только индекс адреса. При перемещении пространства NVM необходимо изменять только содержимое таблицы AddrIndexTable.

Общая структура области хранения NVM:

4.2.3 Блок управления транзакциями

Транзакция - это обновление серии постоянных данных. Очень важна атомарность транзакций: либо обновляются все домены данных, либо не обновляется ни один.

Механизм транзакций предотвращает потерю данных в результате отключения питания или ошибок программирования в процессе обновления данных.

Операционная система USIM-карты создает в ее памяти NVM область резервного копирования и область управления состоянием. Область резервного копирования используется для резервного копирования содержимого целевой области NVM, подлежащей модификации, а область управления состоянием - для управления состоянием транзакций. При выполнении транзакции данные целевой области NVM сначала записываются в резервную область, затем устанавливается состояние области управления состоянием и флаг транзакции, и происходит модификация данных целевой области NVM. При фиксации транзакции флаг транзакции будет сброшен, что свидетельствует о том, что резервные данные недействительны. Если транзакция завершается, то содержимое резервной области записывается обратно в целевой области NVM, а флаг транзакции снимается, завершая операцию отката транзакции. При каждом сбросе карты проверяется, установлен ли флаг транзакции. Если он установлен, то будет выполнен откат транзакции.

В связи с тем, что пространство NVM микроконтроллера управляется постранично, резервное копирование данных в области резервного копирования также осуществляется постранично. Даже если требуется перезаписать только часть страницы, в области резервного копирования будет сохранена вся страница. Затем будет установлена область маркеров резервного копирования для записи информации о резервном копировании страницы, например, номер целевой страницы, номер резервной страницы, маркер отправки и т.д. При каждом сбросе карты будет проверяться, установлен ли флаг резервного копирования страниц. Если флаг резервирования страницы установлен, то будет выполнен откат страницы.

4.3 Модуль управления приложениями

Основной функцией Модуля управления приложениями является обеспечение API (Application Programming Interface), в том числе в операционной системе «Натрон 1.1» реализован **интерфейс** поддержки программного обеспечения партнера, реализующего функционал защищенного хранения ключей аутентификации: установка, регистрация, удаление, распределение команд, выбор приложений и т.д., управление логическими каналами и управление содержимым карты для приложений в соответствии со стандартом Global Platform Specification v.2.2.1. Модуль управления приложениями состоит из Блока управления приложением, Блока защищенного канала и внешнего интерфейса управления приложением.

4.4 Прикладной модуль

Основной задачей прикладного уровня является обеспечение поддержки инструкций APDU согласно стандартам, и последующая обработка данных на карте. Сюда входит создание файлов, чтение и запись файлов.

Прикладной уровень отвечает за обработку APDU команд с внешних уровней, за управление данными карты, такое как создание, чтение, запись файлов, подготовка и проверка данных для подключения к сети операторов сотовой связи, в том числе с использованием интерфейса поддержки программного обеспечения партнера - «крипта-ядра», развертывание и обновление данных файловой системы, обеспечивает поддержку обработки инструкций APDU (протокола, используемого для обмена данными между устройствами согласно национальным и международным стандартам), а также обеспечивает поддержку обработки и управления данными на карте (создание, чтение, запись файлов и др.), в том числе с поддержкой алгоритма аутентификации на основе S3G

USIM карта поддерживает обработку команд, описанных в стандарте ETSI TS 102 221.

Дополнительное программное обеспечение, разработанное третьим лицом – российской организацией – партнером Правообладателя, поддерживает алгоритм шифрования S3G256, обеспечивает защищенную передачу данных между оборудованием и операционной системой, обеспечивает подготовку и проверку данных для подключения к сети оператора.

5 Библиотеки и стандарты, используемые при разработке операционной системы

Функции, обеспечивающие корректную работу операционной системы, были разработаны в соответствии со стандартами, находящимися в открытом доступе. Библиотеки, разработанные сторонними организациями, не использовались в процессе создания COS.

6 Языки программирования.

Для разработки операционной системы был выбран язык программирования C.

7 Обращение в Службу технической поддержки

Если при работе с программным обеспечением у вас возникли проблемы или вопросы – свяжитесь со службой технической поддержки по электронной почте sim@i-smarts.ru в будние дни с 9.00 до 18.00 по московскому времени.