С. В. Гороховик

ПРИНЦИПЫ УСТРОЙСТВА И ПРОГРАММИРОВАНИЯ SIM-КАРТ

SIM-карта — идентификационный модуль абонента, применяемый в мобильной связи. Они применяются в сетях GSM и 3G. Другие современные сотовые сети обычно также применяют другие модули идентификации, внешне схожие с SIM и выполняющие аналогичные функции — USIM в сетях UMTS, R-UIM в сетях CDMA . В сетях 1G идентификацию абонента в сети проводили по заводскому номеру телефона. Таким образом, как сотовый телефон, так и абонент идентифицировались единым кодом. Такой подход порождал полную зависимость номера абонента и пакета предоставляемых ему услуг от конкретного экземпляра телефона. Поменяв аппарат, абонент был вынужден обращаться в офис оператора для того, чтобы телефон перепрограммировали. Очевидно, что более удобна идентификация абонента, независимая от телефона. В стандарте GSM было предложено разделить идентификацию абонента (с помощью SIM-карты) и оборудования (для этого используется IMEI) . Стандарт на специфические особенности карты для GSM SIM устанавливает Европейский институт телекоммуникационных стандартов. На самом деле SIM-карта — это частный случай контактной смарт-карты с микропроцессором. По сути, представляет из себя достаточно защищенный микрокомпьютер с CPU, ROM (опционально), RAM и NVRAM (которая выступает в качестве аналога жесткого диска в PC), с аппаратными генераторами случайных чисел и аппаратной реализацией крипто-алгоритмов. Все SIM-карты можно разделить на три группы исходя из их внешнего вида: ID-1 UICC – самый первый вариант – имеет размер обычной банковской карты, такие карты использовались в сотовых телефонах 90-х годов. В настоящее время в новых моделях мобильных телефонов практически не используется из-за больших габаритов. Plug-in UICC – наиболее распространенный сейчас формат. Обычно такие модули выламываются из карт размера ID-1 по просечкам, сделанным во время изготовления. Mini-UICC – формат карт, который начала использовать компания Apple в iPhone 4, iPad. Сейчас и другие производители мобильных телефонов и других устройств намерены выпускать модели, в которые нужно будет вставлять модули именно такого формата. Иногда этот формат называют 3FF, или «микро-SIM». И эти карты обычно выламываются из карты формата ID-1. Причины появления такого разнообразия очевидны – экономия места внутри корпуса телефона. Главным внешнем элементом любой SIM-карты является контактная площадка (см. рис.1). В обиходе встречаются модули с разным рисунком контактной площадки и разным числом контактов. Стандартами предусмотрены 8 позиций для площадок, через которые модули соединяются с мобильными терминалами, но не всегда используются все из них. Чаще всего встречаются карты с 6-ю контактами, а остальная металлизированная часть обычно подключена к «земле». Используемые контакты: C1 — Vcc — питание; C2 — Reset – контакт управления картой; C3 — CLK — Clock – тактовая частота; C5 — общий («земля»); C6 — Vpp – напряжение программирования, которое используется при записи служебной информации; C7 — I/O – линия последовательного интерфейса ввода/вывода.

Рис. 1 – Схема контактной площадки

Стандартами предусмотрено использование и контактов C4 и C8 в режиме обмена информацией с мобильным терминалом в режиме USB, обеспечивающем более высокую скорость передачи информации, чем через обычный I/ O интерфейс SIM. Давайте рассмотрим структуру памяти SIM-карты. Корневая директория MF (Master File) содержит в себе поддиректории DF (Dedicated Files) и файлы EF (Elementary File). Поддиректории, в свою очередь, тоже содержат файлы первого и второго уровня. Каждый элементарный файл (EF) может принадлежать к одному из трех следующих семейств: прозрачные, линейные и циклические. Элементарные файлы содержат разнообразную служебную информацию. Такой информацией может быть код IMSI абонента, список поддерживаемых языков, таблица доступных услуг и так далее. Файл состоит из заголовка (header) и тела (body). Заголовок детально описывает структуру файла и условия доступа к нему. Тело содержит собственно данные.Прозрачный файл состоит из определенного числа байтов, доступных по отдельности и блоками, для чего необходимо уточнить их относительный адрес (offset) и длину (length).

Линейный файл состоит из

байт, не считая расширения. Циклический файл содержит определенное число записей фиксированной длины. При этом каждая новая запись всегда занимает первую позицию, в то время как последняя оказывается "затертой".

По типу используемой памяти в последнее время SIM-карты делятся на 2 группы: карты, в которых используется ROM и EEPROM, и карты, где используется Flash память. В первом типе карт операционная система (ОС) и постоянно используемые приложения помещаются в ROM производителем чипа (первый этап производства). Цикл производства в этом случае очень долгий. EEPROM используется производителем карт для загрузки файловой системы (ФС) и приложений. В случае с Flash картой ОС, ФС и приложения хранятся на Flash памяти. Использование Flash позволяет загружать ОС в процессе сборки модулей или при производстве карты. На данный момент карты с использованием flash памяти практически вытеснили ROM с рынка. Flash чипы дешевле и позволяют достаточно легко вносить изменения в ОС. Также производителю карт проще планировать заказ чипов, так как не надо заказывать чипы с конкретными версиями ОС, а просто заказываются чипы с различным размером памяти, и нужная ОС загружается уже под конкретного оператора.

По программной «начинке» смарт-карты делятся на 2 большие группы — *native* и *javacard*. ПО для native-карт пишется на языке С. Приложения (если таковые требуются производителем) обычно тесно интегрированы с ОС и загружаются одновременно с ОС на карту. Устанавливать какие-либо приложения, разработанные другой компанией, на native-карту нельзя. Дополнительную функциональность, затребованную оператором, зачастую приходится добавлять в код ОС. Размеры самой ОС из-за использования С и простоты ОС достаточно маленькие (для SIM карт порядка 10-20Кбайт). Поэтому native-карты на данный момент используются, когда оператор ничего не хочет на карте, кроме простого меню.

В эпоху распространения языка Java компания Sun Microsystems написала спецификации javacard. Идея javacard была в том, чтобы сделать возможным установку приложений (апплетов) на карты различных производителей (и на различные чипы). В 1996 году подразделение смарт-карт корпорации Gemalto представила первую javacard. Идея достаточно простая. Кроме ОС карта содержит виртуальную машину Java. Разработанное приложение компилируется в байткод и загружается на карту. Приложения в этом случае загружаются уже после загрузки ОС (в процессе производства карты), также, если карта содержит Remote Applet Manager, javacard апплет может быть установлен после выпуска карты посредством СМС.

Язык для разработки под javacard — это сильно урезанная Java. Приемы программирования, используемые в типичном приложении Java Card, значительно отличаются от применяемых в Java SE. Однако, тот факт, что Java Card является строгим подмножеством языка Java, значительно ускоряет обучение этой технологии, а также позволяет использовать среду Java SE для разработки и отладки приложений. Более того, можно совместно запускать и отлаживать в одной среде и приложение для Java Card, и его серверную часть, которую предполагается выполнять на PC. На современных SIM-картах могут быть предустановлены приложения, предоставляемые оператором. Для использования приложений на SIM-карте телефон должен поддерживать стандарт SIM Tool Kit (STK). Приложения на SIM-карте при помощи STK могут использовать различные функции сотового телефона, в том числе пользовательский интерфейс, модуль связи, и т. д., что позволяет реализовать достаточно широкий набор функциональности. Приложения STK находятся под полным контролем оператора и считаются наиболее безопасными, так как могут использовать встроенный в карту модуль шифрования, что делает их чрезвычайно привлекательными для реализации финансовых сервисов. Существует также возможность загрузки и обновления этих приложений оператором непосредственно при помощи сотовой сети. Минус таких приложений состоит в том, что для их использования требуется выпуск карты, поддерживающей SIM Tool Kit с достаточным объемом памяти и передача ее абоненту, что достаточно сложно с организационной точки зрения.

Часто STK используется для реализации сервиса SIM-меню, имеющегося у большинства операторов. Для взаимодействия с оператором это приложение использует скрытые от абонента SMS-, USSD- или CB-сообщения.

1. 3D news.Daily Digital Digest [Electronic resource] / Mode of access: http://www.3dnews.ru/phone/sim/. – Date of access: 14.09.2012.
2. Tajwap [Electronic resource] / Mode of access: http://tajwap.ru/spravochnaya/chto-takoe-sim-karta.html. – Date of access: 20.02.2011.

Гороховик С.В.,
Научный руководитель: Рак Т.А.,