PC/SC: обзор стандарта для доступа к функциям смарт-карт из приложений

Сергей Панасенко,
компания «Актив»,
panasenko@guardant.ru

Рабочая группа PC/SC

Образована в 1996 г.

Основные цели:

1. Стандартизация интерфейсов взаимодействия с устройствами, работающими со смарт-картами.
2. Спецификация интерфейсов встраивания в ПО функций работы со смарт-картами.

Участники РГ в 1996 г.:

- Bull Personal Transaction Systems
- Gemplus
- Hewlett-Packard
- IBM
- Microsoft Corp.
- Schlumberger
- Siemens-Nixdorf Inc.
- Sun Microsystems
- Toshiba Corp.
- VeriFone

Участники РГ в 2023 г.:

- Advanced Card Systems
- HID Global
- Hewlett-Packard
- Identiv
- KAPELSE
- Kensington
- Olaqin
- Realtek
- SpringCard
- Sunrex Technology

Соотношение с другими стандартами

Спецификации PC/SC развивают существующие стандарты и спецификации, относящиеся к смарт-картам (прежде всего, ISO 7816/14443/15693 и EMV), не входя в противоречие с ними, а дополняя их, как минимум, следующим:

1 Описаниями низкоуровневых интерфейсов устройств работы со смарт-картами.

2 Унифицированными API доступа к смарт-картам, не зависящими от конкретных устройств.

3 Возможностями по обеспечению одновременного доступа к смарт-картам и считывателям со стороны нескольких программных приложений.

История версий:

1997

1.0 Исходная версия

2004

2.0

Основные дополнения:

- бесконтактные смарт-карты
- считыватели с дополнительными функциями

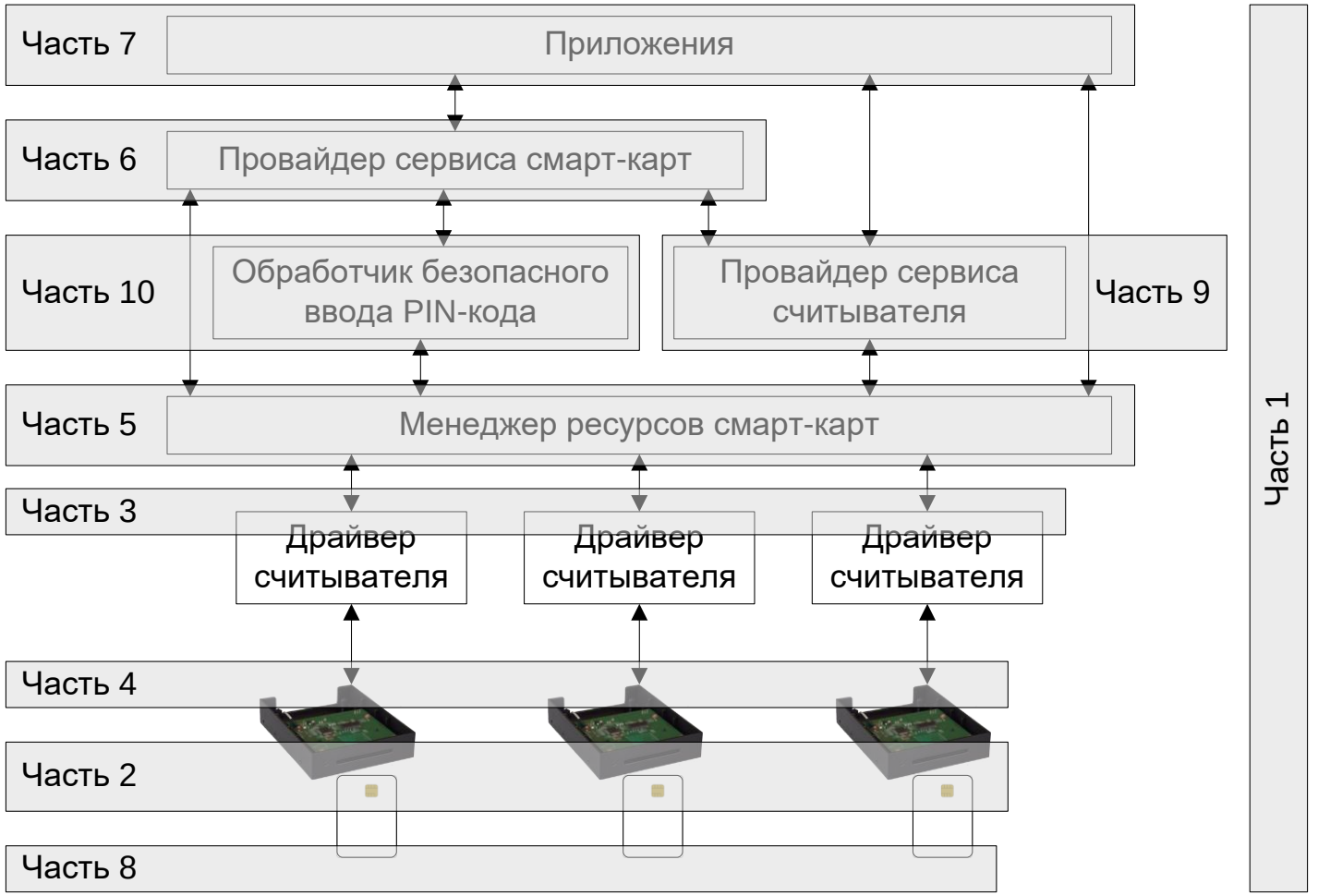
2013

2.01.14

Текущая версия (серия изменений и дополнений к версии 2.0)

Архитектура PC/SC и части спецификации

1. Introduction and Architecture Overview
2. Interface Requirements for Compatible IC Cards and Readers
3. Requirements for PC-Connected Interface Devices
4. IFD Design Considerations and Reference Design Information
5. ICC Resource Manager Definition
6. ICC Service Provider Interface Definition
7. Application Domain / Developer Design Considerations
8. Recommendations for ICC Security and Privacy Devices
9. IFDs with Extended Capabilities
10. IFDs with Secure Pin Entry Capabilities



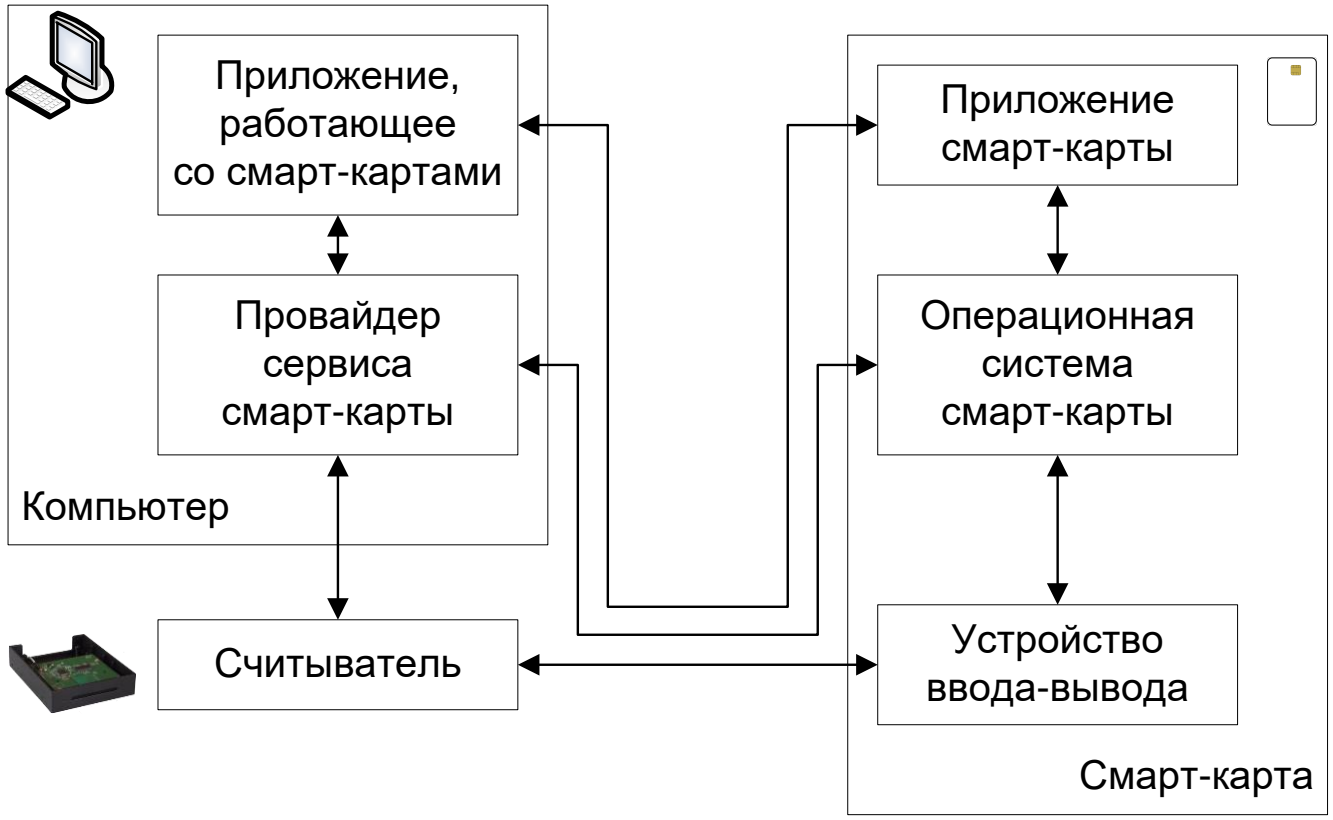
Часть 2: Требования к интерфейсу совместимых смарт-карт и считывателей

Определяет нижний из логических уровней обмена данными между смарт-картой и компьютером:

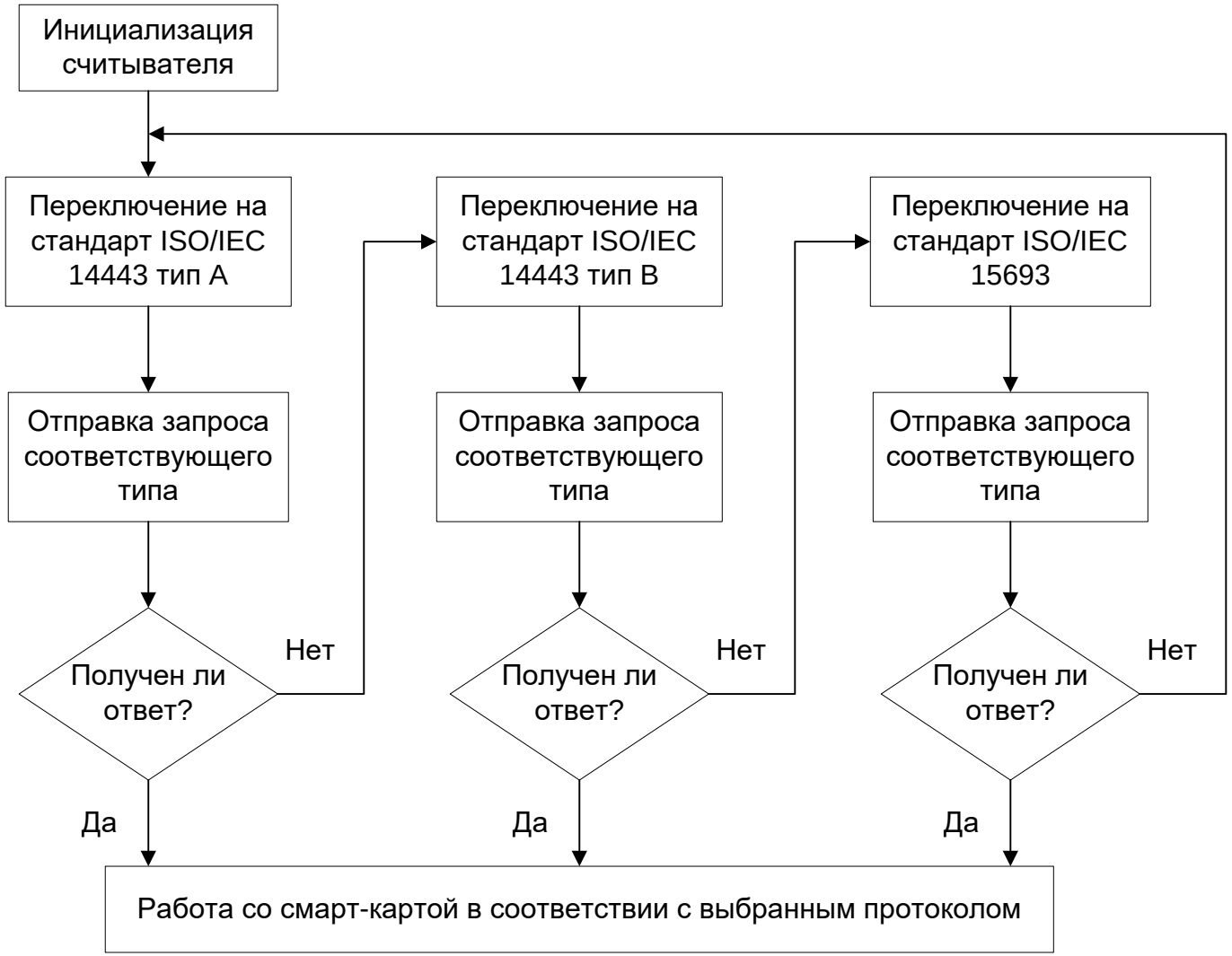
- требования к физическому интерфейсу;
- требования к электрическим параметрам;
- низкоуровневые протоколы взаимодействия считывателей и смарт-карт.

Новые требования относительно стандартов ISO 7816:

- для смарт-карт: необходимость противодействия атакам, использующим съем данных по побочным каналам;
- для считывателей: определение и передача событий введения/извлечения карты, обязательная поддержка обоих типов протоколов из ISO 7816-3 и другие.



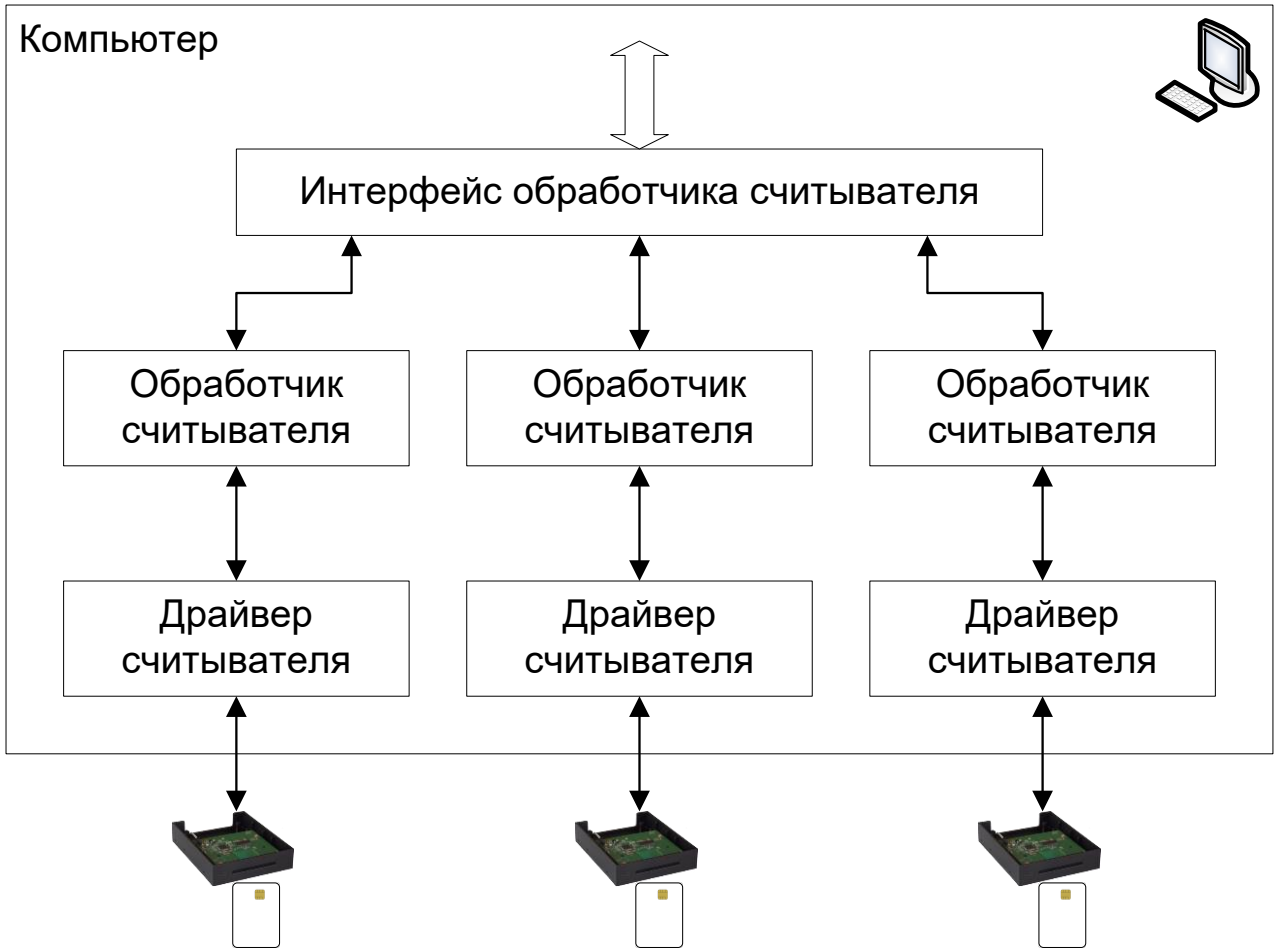
Часть 2: Требования к интерфейсу совместимых смарт-карт и считывателей



Дополнительные требования в части бесконтактных смарт-карт:

- обязательна поддержка антиколлизионного механизма;
- допускается в конкретный момент времени работа с картами только одного типа.

Часть 3: Требования к интерфейсу считывателей, подключаемых к персональным компьютерам



Основные требования:

- разработчик считывателя должен обеспечивать наличие программных модулей, входящих в подсистему считывателя, и их функционирование в соответствии со спецификацией;
- независимо от функций считывателя и способа его подключения к компьютеру должен быть предоставлен стандартный интерфейс;
- ПО должно скрывать детали работы со смарт-картой и предоставлять стандартный интерфейс доступа, аналогичный ISO 7816-4.

Часть 3: Требования к интерфейсу считывателей, подключаемых к персональным компьютерам

Дополнительные требования к подсистеме считывателя:

- должна уметь разбирать ATR и устанавливать оптимальные протокол и параметры в соответствии с ним;
- должна уметь разбирать ошибки взаимодействия и пытаться исправлять их (по возможности) на своем уровне;
- должна передавать на верхний уровень информацию о событиях введения/извлечения карты и неисправляемых ошибках;
- может поддерживать одновременную работу с несколькими бесконтактными картами (в этом случается представляется как несколько независимых логических считывателей);
- может поддерживать любые дополнительные функции, не противоречащие спецификации.

Функции подсистемы считывателя:

Обязательные
IFD_Get_Capabilities
IFD_Set_Capabilities
IFD_Set_Protocol_Parameters
IFD_Power_ICC
IFD_Transmit_to_ICC
IFD_Is_ICC_Present
IFD_Is_ICC_Absent
Опциональные
Device_List_Devices
IFD_Swallow_ICC
IFD_Eject_ICC
IFD_Confiscate_ICC

Часть 3: Требования к интерфейсу считывателей, подключаемых к персональным компьютерам

Информация, которая должна предоставляться подсистемой считывателя:

Информация о вставленной карте

- Присутствует ли карта
- Подано ли питание
- Тип и ATR карты

Механические характеристики

- Наличие возможностей захвата/ удержания/выброса карты

Управление питанием

- Поддерживается ли

Протокол обмена

- Поддерживаемые протоколы обмена
- Типы бесконтактных карт
- Основная и макс. скорость обмена
- Осн. и макс. частота синхронизации
- Максимальный размер данных

Дополнительные возможности

- Наличие устройств ввода аутентификационной информации

О считывателе

- Производитель
- Модель
- Номер версии
- Серийный номер

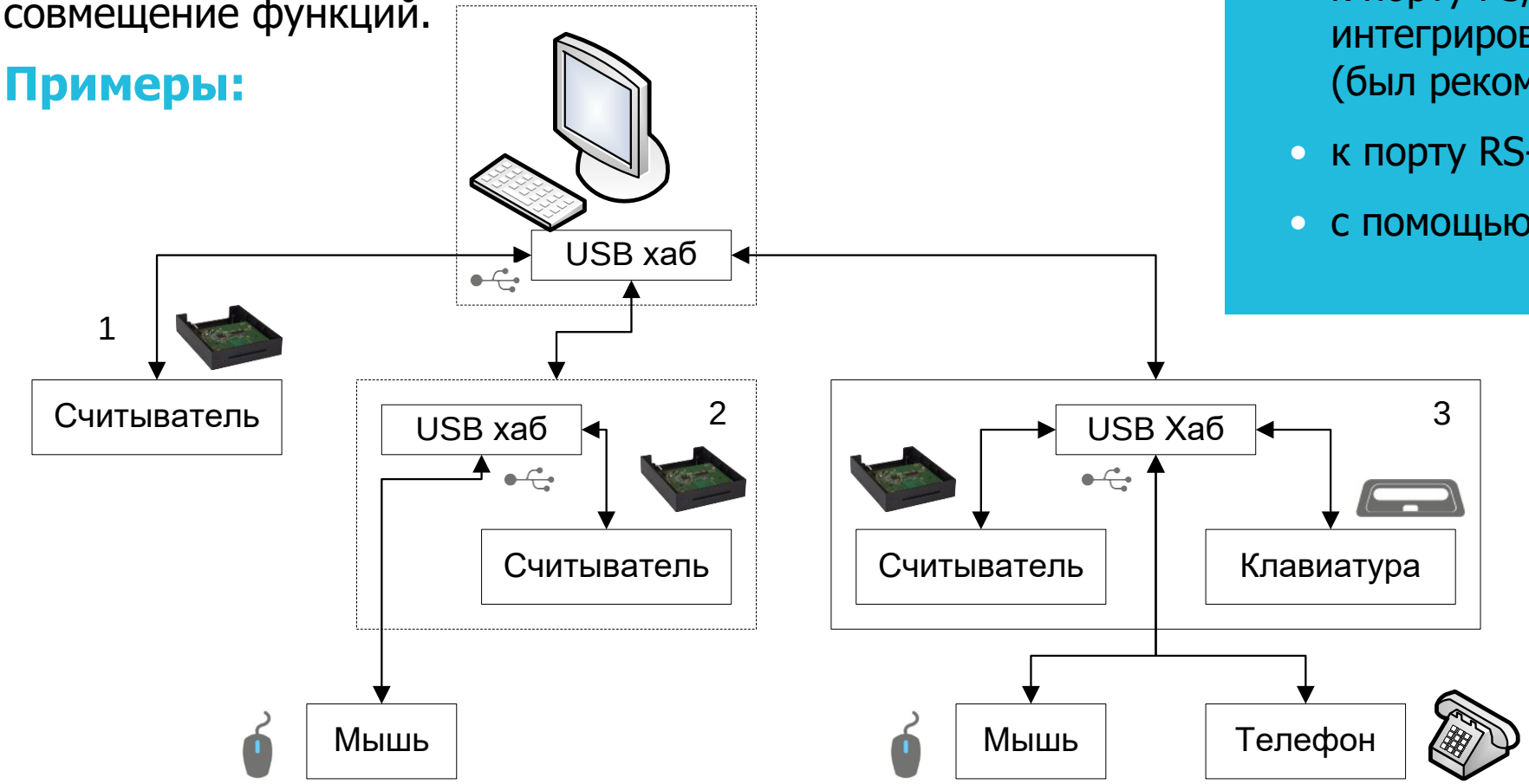
Канал связи

- Тип канала связи

Часть 4: Конструктивные требования к считывателям

Рекомендуется использование считывателей, подключаемых к порту USB. Допустимо совмещение функций.

Примеры:



Другие варианты подключения:

- к порту PS/2 – для считывателей, интегрированных с клавиатурой (был рекомендован в версии 1.0);
- к порту RS-232;
- с помощью PC Card.

Часть 5: Требования к менеджеру ресурсов смарт-карт

Ключевой компонент архитектуры и обязательный программный слой, через который проходят все обращения к считывателям. Взаимодействует с обработчиками считывателей.

Основные функции:

1. Идентификация ресурсов и отслеживание их состояния:
   - определение подключенных считывателей и предоставление приложениям информации о них;
   - отслеживание событий введения/извлечения карты.
2. Распределение ресурсов считывателей между приложениями.
3. Поддержка транзакций.

Основные требования:

1. Поддержка определенного набора функций.
2. Разделение логических потоков взаимодействия различных приложений с разными картами.
3. Поддержка различных сценариев работы:
   - обращение к любой карте, вставленной в конкретный считыватель;
   - обращение к конкретной карте, вставленной в указанный считыватель;
   - обращение к любой карте, соответствующей заданному подмножеству типов, вставленной в любой считыватель, принадлежащий к конкретной группе и т. п.
4. Наличие собственного графического интерфейса для администрирования.

Часть 5: Требования к менеджеру ресурсов смарт-карт

Классы и функции менеджера ресурсов смарт-карт:

RESOURCEMANAGER
EstablishContext
ReleaseContext

RESOURCEDB
IntroduceReader
ForgetReader
IntroduceReaderGroup
ForgetReaderGroup
AddReaderToGroup
RemoveReaderFromGroup
IntroduceCardType
ForgetCardType

RESOURCEQUERY
ListReaderGroups
ListReaders
ListCardTypes
GetProviderId
ListInterfaces

SCARDTRACK
LocateCards
GetStatusChange
Cancel

SCARDCOMM
Connect
Reconnect
Disconnect
Status
BeginTransaction
EndTransaction
Cancel
Transmit
Control
GetReaderCapabilities
SetReaderCapabilities

Часть 6: Требования к провайдеру сервиса смарт-карт

Находится на более верхнем уровне по сравнению с менеджером ресурсов и должен предоставлять интерфейс, позволяющий использовать возможности смарт-карт различных типов (каждый тип представляется отдельным провайдером сервиса).

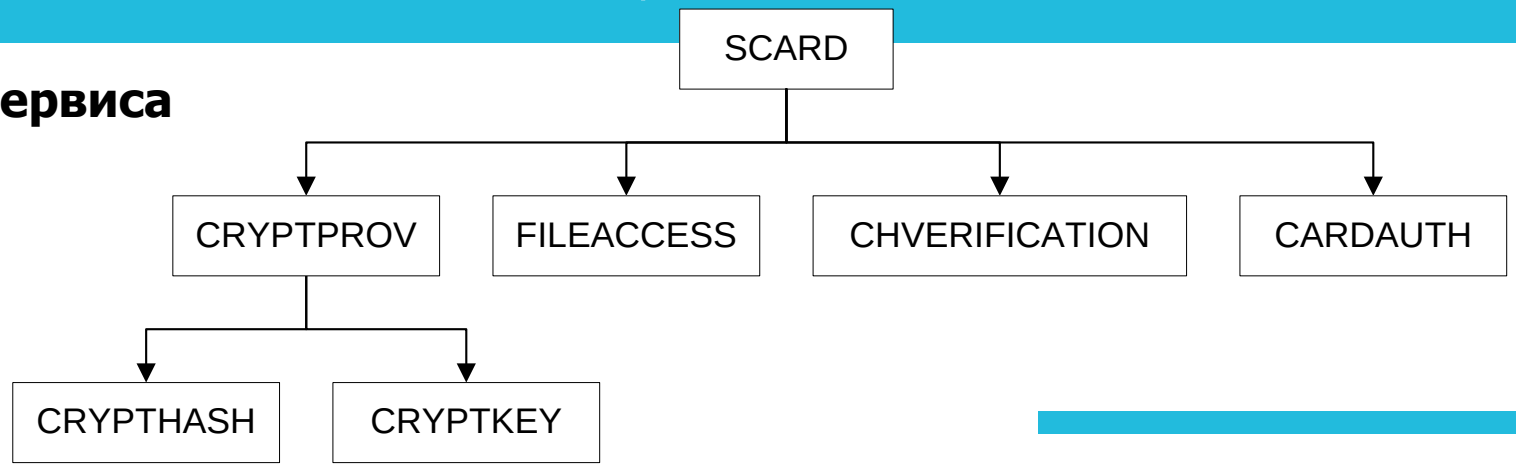
Основные категории функций:

- функции работы с файлами;
- функции аутентификации;
- криптографические функции (могут быть выделены в отдельный криптопровайдер).

Должен иметь графический интерфейс, предоставляющий, как минимум, следующие возможности:

- настроек параметров аутентификации и выполнения аутентификации пользователей;
- управления паролями и PIN-кодами.

Классы провайдера сервиса смарт-карт:



Часть 6: Требования к провайдеру сервиса смарт-карт

SCARD
- CreateFileAccess
- CreateCHVerification
- CreateCardAuth
- CreateCryptProv
- AttachByHandle
- AttachByIFD
- Detach
- Reconnect
- Lock
- Unlock

CHVERIFICATION
- Verify
- ChangeCode
- Unblock
- ResetSecurityState

FILEACCESS
- ChangeDir
- GetCurrentDir
- Directory
- Опциональные функции работы с данными

CARDAUTH
- GetChallenge
- ICC_Auth
- APP_Auth
- User_Auth

CRYPTPROV
- CreateHash
- DeriveKey
- GenKey
- GenRandom
- GetParam
- GetUserKey
- Cancel
- ImportKey
- SetParam

CRYPTHASH
- GetParam
- HashData
- HashSessionKey
- SetParam
- SignHash
- VerifySignature

CRYPTKEY
- Decrypt
- Encrypt
- Export
- GetParam
- SetParam

Часть 7: Рекомендации по разработке приложений для смарт-карт

Основные рекомендации:

- взаимодействовать с провайдером сервиса смарт-карт, обращаться к другим компонентам (менеджеру ресурсов или провайдеру сервиса считывателя) только при отсутствии требуемых возможностей у провайдера сервиса смарт-карт;
- динамически определять доступные ресурсы: считыватели и их группы, поддерживаемые типы смарт-карт;
- не использовать вкомпилированные константы, соответствующие именам считывателей, групп считывателей и типов смарт-карт;
- не использовать ресурсы эксклюзивно;
- не выполнять сброс смарт-карты без необходимости;
- использовать возможности смарт-карт в части безопасности и криптографии;
- отслеживать события, относящиеся к смарт-картам интересующих приложение типов;
- восстанавливать взаимодействие со смарт-картой и работу приложения после возникновения некритичных ошибок;
- минимизировать использование транзакций.

Часть 8: Рекомендации по применению смарт-карт в приложениях, обеспечивающих безопасность

Криптографические смарт-карты должны реализовывать следующие алгоритмы:

- хеширования;
- вычисления и проверки подписи;
- обмена ключами;
- симметричного шифрования (опционально);
- генерации случайных последовательностей;
- генерации ключевых пар;
- экспорта открытых ключей;
- защищенного хранения секретных ключей без возможности их экспорта.

Поддержка возможностей по аутентификации:

- пользователя в удаленных системах;
- пользователя смарт-картой;
- приложения смарт-картой и наоборот.

Поддержка механизмов разграничения доступа к файлам и каталогам; минимум вариантов доступа (для чтения/записи/дополнения/удаления):

- доступ всегда разрешен / всегда запрещен;
- для получения доступа требуется успешная аутентификация пользователя;
- для получения доступа требуется успешная аутентификация приложения.

Поддержка спец. файлов для следующих данных:

- списков поддерживаемых криптоалгоритмов;
- кодов аутентификации пользователей/приложений, ключей/паролей для удаленной аутентификации;
- секретных/открытых ключей для подписи, обмена ключами и аутентификации карты и их параметров.

Часть 8: Рекомендации по применению смарт-карт в приложениях, обеспечивающих безопасность

Криптографические команды
LOAD PUB KEY
LOAD PRI KEY
GENERATE KEY
GET PUBLIC KEY
DELETE KEY
LOAD DATA
SIGN DATA
LOAD VERIFY KEY
VERIFY SIGNATURE
LOAD EXPORT KEY
EXPORT KEY
IMPORT KEY
HASH DATA

Команды аутентификации и прочие
VERIFY
CHANGE CODE
UNBLOCK
GET CHALLENGE
INTERNAL AUTH
EXTERNAL AUTH
USER AUTH
INVALIDATE
REHABILITATE

Часть 9: Применение считывателей смарт-карт с дополнительными возможностями

Дополнительные возможности считывателя:

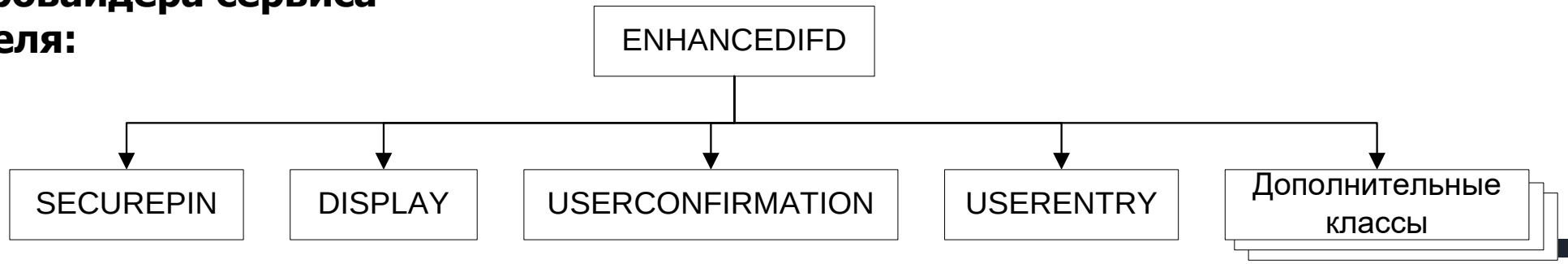
- наличие дисплея и/или клавиатуры;
- возможность ввода и проверки PIN-кода;
- наличие биометрических считывателей;
- наличие криптографических функций и др.

Если приложению требуются дополнительные возможности, то ему следует взаимодействовать со считывателем через провайдер сервиса считывателя.

Считыватель с дополнительными возможностями может представляться в архитектуре PC/SC как несколько логических устройств.

Расширенные требования к устройствам ввода PIN-кода задаются в части 10.

Классы провайдера сервиса считывателя:



Часть 9: Применение считывателей смарт-карт с дополнительными возможностями

Функции провайдера сервиса считывателя (только класс ENHANCEDIFD является обязательным):

ENHANCEDIFD
AttachByReader
AttachByHandle
Detach
SelectContext
ReleaseContext
Cancel
CreateSecurePIN
CreateDisplay
CreateUserConfirmation
CreateUserEntry
CreateInterface

SECUREPIN
GetCapabilities
SetFeedback
Verify
Change
Cancel

USERENTRY
GetString
Cancel

USERCONFIRMATION
GetConfirmation
Cancel

DISPLAY
ClearDisplay
GetCharacterDisplayResolution
DisplayMessage

Заключение

1. Спецификации PC/SC описывают набор требований к компонентам систем, использующих смарт-карты, на всех уровнях: от самих смарт-карт до пользовательских приложений.

2. Данные спецификации дополняют существующие стандарты, относящиеся к смарт-картам, с целью обеспечения совместимости компонентов таких систем (считывателей, смарт-карт и программного обеспечения) и их предсказуемого поведения.

3. Спецификации PC/SC поддерживаются в операционных системах Windows, Linux и Mac OS.

4. Спецификации являются устоявшимися и проверенными временем.

КОМПАНИЯ АКТИВ

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Сергей Панасенко, компания «Актив»,
panasenko@guardant.ru

КОМПАНИЯ АКТИВ

Компания «Актив» — крупнейший в России производитель аппаратных средств электронной подписи и решений для защиты программного обеспечения. Компания на рынке уже 30 лет.

Сейчас в компании работает более 230 человек. Из них около трети — разработчики, тестировщики и технические аналитики.

Средний возраст IT специалистов в компании — менее 30 лет. Компания активно нанимает в том числе студентов старших курсов. Многие руководители и лиды групп приходили работать в «Актив» студентами на позиции младших разработчиков, тестировщиков.

Компания «Актив» славится своим коллективом: здесь всегда готовы помочь разобраться в трудной проблеме, дать совет, подставить плечо. Каждый участник команды имеет право голоса, будет выслушан и может влиять на процессы. Именно за счёт новых идей, участия молодых сотрудников компания идёт в ногу со временем и применяет современные методы и технологии в процессах разработки.

Если у Вас возник интерес к нашей компании,
и Вы хотите стать ее частью, проходите по ссылке
в QR-коде и присылайте резюме!