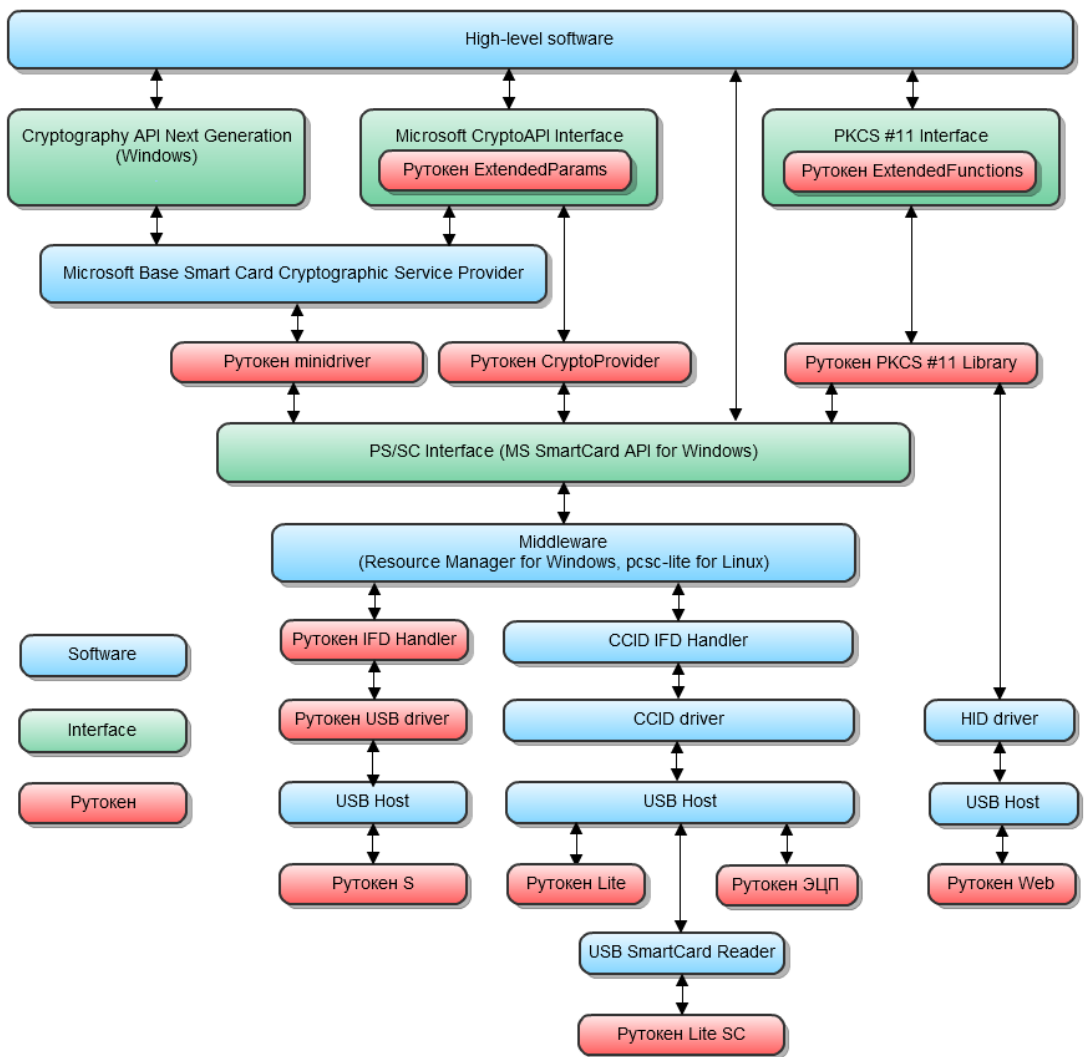


Рекомендации по выбору интерфейса

По мере развития технологий смарт-карт было создано множество технологий, описывающих правила взаимодействия различных систем с ними. Самые удачные технологии реализовались в международные стандарты ISO или общепризнанные отраслевые стандарты.



[blocked URL](#)

Интерфейсы высокого уровня

Интерфейсы высокого уровня предназначены для разработчиков программ и программных комплексов прикладного уровня. Они абстрагируют программиста от такого понятия, как файловая система, особенностей работы смарт-карточной операционной системы. Наиболее распространенными интерфейсами высокого уровня, подходящими для разработчиков прикладных приложений являются стандарты RSALabs PKCS#11 и Microsoft CryptoAPI.

RSALabs PKCS#11 (CryptoKi)

Стандарт разработан исследовательской группой RSALabs как попытка стандартизовать высокоуровневый кроссплатформенный программный интерфейс доступа к функциональности смарт-карт и usb-токенов.

PKCS#11 благодаря своей логичности и относительной простоте получил широкое распространение и в настоящий момент является де-факто индустриальным стандартом для приложений работающих со смарт-картами.

Ответственность за реализацию интерфейса в виде динамически подгружаемой библиотеки лежит на производителях смарт-карт (usb-токенов).

Рекомендуется к использованию при разработке приложений прикладного уровня для различных платформ, в том числе кроссплатформенных приложений, **кроме** случаев, когда требуется глубокая интеграция приложения в операционные системы Windows.

Достоинства

- Кроссплатформенность (Windows, Mac OS X, Linux, UNIX, Java и т.п)
- Простой интерфейс для языка Си
- Широкая распространенность (кроме Windows)
- Достаточно высокий уровень абстракции
- Легкая портируемость программного обеспечения

Недостатки

- Недостаточная поддержка в Windows и в прикладных приложениях для Windows

Microsoft CryptoAPI

Microsoft CryptoAPI можно рассматривать как расширение обширного Windows API в части касающейся криптографии и инфраструктуры открытых ключей.

Функции предоставляются либо встроенными криптопровайдерами, входящими в состав Windows, либо внешними поставляемыми производителями смарт-карт или usb-токенов.

Microsoft CryptoAPI глубоко интегрирован в операционные системы Windows и другое прикладное программное обеспечение от Microsoft и является стандартом для Windows-платформы.

Рекомендуется к использованию при разработке приложений прикладного уровня для Windows, когда требуется глубокая интеграция приложения в операционную систему и программное обеспечение Microsoft.

Достоинства

- Глубокая интеграция в Windows и прикладное программное обеспечение
- Достаточно простой интерфейс
- Высокий уровень абстракции
- Легкая портируемость программного обеспечения (в пределах платформы)

Недостатки

- Совершенно не используется вне Windows
- Установка криптопровайдера требует наличия административных прав в системе

Интерфейсы низкого уровня

Программный интерфейс PC/SC

Низкоуровневый программный интерфейс описывает процесс взаимодействия прикладного программного обеспечения и оборудования смарт-карт.

Общение прикладной программы и смарт-карт (usb-токенов) по большей части представляет собой обмен особыми массивами данных в режиме запрос-ответ.

Интерфейс первоначально был разработан компанией Microsoft, однако получился настолько удачным, что был портирован и на другие операционные системы.

Реализация взаимодействия на уровне протокола PC/SC довольно трудоемка и требует знания достаточно большого количества специфических аспектов, которые могут довольно сильно отличаться у разных производителей.

Рекомендуется к использованию только для разработчиков встраиваемых систем, при доработке уже существующего программного обеспечения, либо при острой необходимости использования функций, специфичных только для устройств Рутокен.

Достоинства

- Кроссплатформенность
- Широкая распространённость
- Позволяет задействовать специфичный для конкретной модели смарт-карты (usb-токена) функционал

Недостатки

- Высокая сложность реализации
- Требуется большое количество специфичных для каждого производителя знаний
- Чрезвычайно высокая сложность портирования

Аппаратный уровень ISO/IEC 7816

На наиболее низком уровне (ближайшем к смарт-карте или токену) обосновалось семейство стандартов [ISO/IEC 7816](#).

Различные части этого стандарта описывают физические параметры карт, расположение и назначение контактов, электрические параметры интерфейса и принципы установления связи, протокол обмена и механизм действия команд.

Практически все выпускаемые смарт-карты так или иначе поддерживают этот стандарт с некоторыми вариациями.

Рекомендуется к использованию только для разработчиков аппаратных систем (не совместимых с PC).