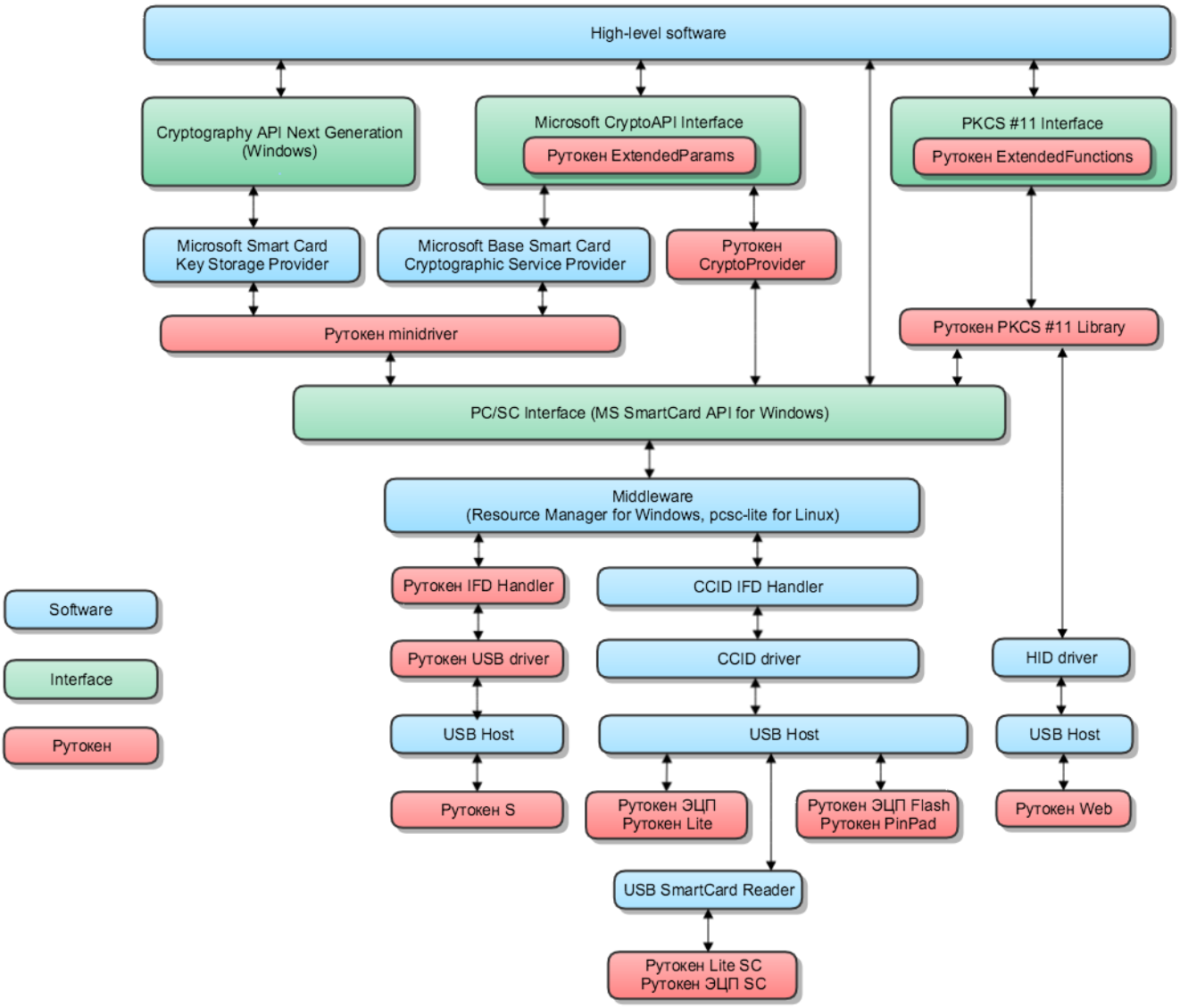
Архитектура Рутокен

Архитектура решений Рутокен выработана в соответствии с требованиями общепринятых индустриальных стандартов.

Общепринято деление интерфейсов на высокий, низкий и аппаратный уровни.



Интерфейсы высокого уровня

Интерфейсы высокого уровня ориентированы на разработчиков высокоуровневого клиентского программного обеспечения и используются для встраивания поддержки идентификаторов Рутокен.

Общепринятые стандартизованные интерфейсы:

- PKCS#11 версии 2.30 или новее,
- Microsoft CryptoAPI версии 2.0,
- Microsoft Crypto Next Generation Key Storage Provider (minidriver).

в полной мере реализованы в виде подгружаемых системных библиотек, которые легко интегрируются в любые системы.

Интерфейсы низкого уровня

Под интерфейсами высокого уровня находятся интерфейсы, обеспечивающие представление идентификаторов Рутокен в качестве смарт-карты, которая вставлена в считыватель.

За этот слой отвечают USB-драйвер идентификаторов Рутокен, системные CCID-драйверы идентификаторов Рутокен ЭЦП, а также промежуточное программное обеспечение, которое реализует стандартный протокол взаимодействия PC/SC (также известен как Microsoft SmartCard API).

В операционных системах семейства Windows - это Microsoft Resource Manager (системный сервис Смарт-карт), а в операционных системах, основанных на UNIX (в том числе и macOS), - это программное обеспечение проекта M.U.S.C.L.E. (также известное как pcsc-lite).

Взаимодействие этих интерфейсов с интерфейсом аппаратного уровня происходит путем передачи команд с использованием Transport Protocol Data Units (TPDU) по протоколу T=0|1.

Аппаратный уровень

Самый нижний уровень представлен двумя физическими устройствами:

- персональным идентификатором Рутокен;
- USB хост-контроллером клиентского компьютера.

Взаимодействие между токеном и хост-контроллером осуществляется по протоколу USB Control Transfer Protocol, который использует Vendor Specific Requests (VSR).

Основным аппаратным элементом идентификаторов Рутокен является защищенный микроконтроллер, который реализует функции интерфейса USB, поддержку файловой системы и команд по ISO/IEC 7816 (ГОСТ Р ИСО/МЭК 7816).