APDU

Для взаимодействия с операционной системой Рутокен и его файловой системой имеется низкоуровневый протокол, реализующий подмножество стандарта ISO/IEC 7816-4 (Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange). Этот протокол оперирует понятием APDU (Application Protocol Data Unit) и состоит из двух видов APDU: APDU-команда и APDU-ответ. Инициирует обмен с токеном приложение, отправляя APDU-команду и ожидая получить от токена APDU-ответ.

Интерфейс уровня APDU обеспечивает приложениям доступ ко всем функциям токенов. Однако ничто не дается "бесплатно". В данном случае за широкие возможности приходится платить большим объемом программирования: приложение само должно обнаруживать токен, инициировать транзакции, обеспечивать совместный доступ и т.п.

Структура APDU

APDU-команда		
Название поля	**Длина (байт)**	**Описание**
CLA	1	Класс команды
INS	1	Код команды
P1-P2	2	Параметры команды
L_C	0,1 или 3	Длина передаваемых данных
Command Data	N_C	Набор байтов, представляющий собой передаваемые данные
L_e	0, 1, 2 или 3	Максимальное количество данных, ожидаемых в поле данных ответа

Таким образом, APDU-команда состоит из заголовка и опционально - данных:

Заголовок	**Тело**
CLA INS P1 P2	[Поле L_C][Поле данных][ПолеL_e]

APDU-ответ		
Название поля	**Длина (байт)**	**Описание**
Response data	Nr (по крайней мере Ne)	Данные ответа
SW1-SW2	2	Статус обработки команды, например 90 00 (hex) означает успешное завершение

Примеры APDU-команд

APDU-команда	**Описание**
CREATE FILE	Создать файл или каталог в текущем каталоге
SELECT FILE	Сделать текущим файл (или каталог)
READ BINARY	Прочитать текущий файл или его часть
UPDATE BINARY	Перезаписать содержимое текущего файла или его части
DELETE FILE	Удалить текущий файл или каталог
GENERATE KEY	Сгенерировать ключ шифрования
VERIFY	Установить текущие права доступа
PERFORM SECURITY OPERATION	Выполнить хэширование, зашифрование, расшифрование (и др. операции) данных

GET CHALLENGE	Сгенерировать случайное число

Несмотря на то, что APDU является базовым уровнем коммуникации с токеном, разработчику скорее всего не понадобится работать с ним напрямую - за исключением, быть может, каких-то экзотических случаев, когда пользование высокоуровневыми интерфейсами по каким-то причинам нежелательно или невозможно. По этой причине описания и примеры работы с APDU Рутокен мы не включаем в состав Комплекта разработчика.