Описание функций PKCS #11

Функции стандарта PKCS#11, используемые для работы с устройствами Рутокен, делятся на следующие категории:

- функции общего назначения;
- функции для работы со слотами и токенами;
- функции для работы с сессиями;
- функции для работы с объектами;
- функции шифрования;
- функции расшифрования;
- функции хеширования сообщений;
- функции создания подписи;
- функции проверки подписи;
- функции для работы с ключами;
- функции генерации случайных чисел.

Кроме того, стандартом предусмотрено использование определенных производителем функций обратного вызова для управление объектами мьютекса для безопасного многопоточного доступа к библиотеке.

Выполнение функции стандарта PKCS #11 в общем случае осуществляется по принципу "все или ничего", т.е. результатом вызова функции является или целиком выполненная задача или совсем ничего.

- Если функция была выполнена успешно, то она возвращает значение CKR_OK.
- Если функция не была выполнена успешно, то она возвращает значение, отличное от CKR_OK, и токен остается в том же состоянии, к каком был до вызова функции. Если функцией предполагалось изменение содержимого определенных ячеек памяти на ПК, то они могут оказаться измененными, несмотря на неудачное выполнение функции.
- В редких (и крайне неприятных) случаях функция при неудачном завершении может вернуть значение CKR_GENERAL_ERROR. Когда это происходит, токен и ПК могут оказаться в противоречивых состояниях, и функция выполнить задачу частично.

Существует небольшое количество стандартных функций, поведение возвращаемых значений которых не укладывается в описанные выше рамки, эти исключения задокументированы индивидуально в описании самих функций.

Библиотека PKCS #11 не должна поддерживать каждую функцию Cryptoki API. Однако даже неподдерживаемая функция должна иметь "заглушку" в библиотеке, возвращающую значение CKR_FUNCTION_NOT_SUPPORTED. Вход функции в структуру библиотеки CK_FUNCTION_LIST (полученную с помощью C_GetFunctionList) должен указывать на эту заглушку.