Коды ошибок PKCS #11

- Стандартные коды ошибок
- Специальные коды ошибок

Все функции из реализации стандарта PKCS#11 возвращают различные коды ошибок. Все возвращаемые коды ошибок делятся на две большие группы:

- **стандартные коды ошибок**, которые описаны в стандарте. Для каждого кода ошибки есть разъяснение, в каких ситуациях он может быть возвращен.
- **специальные коды ошибок**, которые определяются каждым разработчиком реализации стандарта PKCS#11. Ситуации, в которых могут быть возвращены специальные коды ошибок разработчик реализации стандарта определяет самостоятельно.

Все функции из реализации стандарта PKCS#11 возвращают специальные коды ошибок (определяются производителем).

Все функции из реализации расширения стандарта PKCS#11 возвращают специальные коды ошибок (определяются производителем).

Стандартные коды ошибок

В силу особенностей реализации библиотек rtPKCS11 и rtPKCS11ECP некоторые стандартные функции могут вернуть стандартный код ошибки PKCS#11, не входящий в список допустимых для данной функции. Подобная ситуация является исключением. Стандартные коды ошибок, возвращаемые каждой функцией в исключительных ситуациях, перечислены в описании для каждой функции отдельно.

В таблице ниже приведен список кодов ошибок стандарта PKCS#11 и их описаний, поддерживаемых устройствами Рутокен. Подробную информацию по каждому коду ошибки можно найти в стандарте (английский язык).

Коды ошибок стандарта PKCS #11, поддерживаемые устройствами Рутокен

Код ошибки	Описание
CKR_ARGUMENTS_BAD	Недопустимый аргумент
CKR_ATTRIBUTE_READ_ONLY	Невозможно установить или изменить значение атрибута приложением
CKR_ATTRIBUTE_SENSITIVE	Атрибут недоступен для чтения
CKR_ATTRIBUTE_TYPE_INVALID	Некорректный тип атрибута
CKR_ATTRIBUTE_VALUE_INVALID	Некорректное значение атрибута
CKR_BUFFER_TOO_SMALL	Размер заданного буфера является недостаточным для вывода результатов выполнения функции
CKR_CANT_LOCK	Библиотека не поддерживает блокировку для защиты потоков; возвращается только при вызове функции **C_Initialize**
CKR_CRYPTOKI_ALREADY_INITIALIZED	Библиотека уже инициализирована (предыдущий вызов функции **C_Initialize** не был сопровожден соответствующим вызовом функции **C_Finalize**); возвращается только при вызове функции **C_Initialize**
CKR_CRYPTOKI_NOT_INITIALIZED	Выполнение функции невозможно, так как библиотека не инициализирована; возвращается только при вызове любой функции, за исключением **C_Initialize** и **C_Finalize**
CKR_DATA_INVALID	Некорректные входные данные для выполнения криптографической операции
CKR_DATA_LEN_RANGE	Входные данные имеют некорректный размер для выполнения криптографической операции
CKR_DEVICE_ERROR	Ошибка при обращении к токену или слоту
CKR_DEVICE_MEMORY	Недостаточно памяти токена для выполнения запрошенной функции
CKR_DEVICE_REMOVED	Токен был удален из слота во время выполнения функции
CKR_DOMAIN_PARAMS_INVALID	Функции переданы некорректные или не поддерживаемые параметры домена

CKR_ENCRYPTED_DATA_INVALID	Для операции расшифрования переданы некорректно зашифрованные данные
CKR_ENCRYPTED_DATA_LEN_RANGE	Для операции расшифрования переданы зашифрованные данные некорректного размера
CKR_FUNCTION_CANCELED	Выполнение функции было прервано
CKR_FUNCTION_FAILED	При выполнении функции возник сбой
CKR_FUNCTION_NOT_SUPPORTED	Запрашиваемая функция не поддерживается библиотекой
CKR_FUNCTION_REJECTED	Запрос на подпись был отклонен пользователем
CKR_GENERAL_ERROR	Критическая ошибка, связанная с аппаратным обеспечением
CKR_HOST_MEMORY	Недостаточно памяти для выполнения функции на рабочей станции, где установлена библиотека
CKR_KEY_FUNCTION_NOT_PERMITTED	Атрибуты ключа не позволяют выполнить операцию
CKR_KEY_HANDLE_INVALID	Функции передан некорректный идентификатор (хэндл) ключа
CKR_KEY_NOT_WRAPPABLE	Невозможно зашифровать ключ
CKR_KEY_SIZE_RANGE	Недопустимый размер ключа
CKR_KEY_TYPE_INCONSISTENT	Тип ключа не соответствует данному механизму
CKR_KEY_UNEXTRACTABLE	Невозможно зашифровать ключ, так как атрибут CKA_UNEXTRACTABLE установлен в значение CK_TRUE
CKR_MECHANISM_INVALID	Указан неправильный механизм для выполнения криптографической операции
CKR_MECHANISM_PARAM_INVALID	Указаны неправильные параметры механизма для выполнения криптографической операции
CKR_NEED_TO_CREATE_THREADS	Программа не поддерживает внутренних методов операционной системы для создания новых потоков
CKR_OBJECT_HANDLE_INVALID	Функции передан некорректный идентификатор (хэндл) объекта
CKR_OPERATION_ACTIVE	Выполнение операции невозможно, поскольку такая операция уже выполняется
CKR_OPERATION_NOT_INITIALIZED	Невозможно выполнить операцию в этой сессии
CKR_PIN_EXPIRED	Срок действия PIN-кода истек
CKR_PIN_INCORRECT	Функции передан PIN-код, который не соответствует тому, который сохранен на токене
CKR_PIN_INVALID	Значение PIN-кода содержит недопустимые символы
CKR_PIN_LEN_RANGE	Недопустимая длина PIN-кода
CKR_PIN_LOCKED	Авторизация по данному PIN-коду невозможна (превышен допустимый предел последовательного ввода неправильных значений PIN-кода)
CKR_RANDOM_NO_RNG	Данный токен не поддерживает генерацию случайных чисел
CKR_SESSION_CLOSED	Сессия была закрыта во время выполнения функции
CKR_SESSION_COUNT	Достигнуто предельное количество открытых сессий для данного токена
CKR_SESSION_EXISTS	Сессия с токеном уже открыта и поэтому токен не может быть инициализирован

CKR_SESSION_HANDLE_INVALID	Функции передан некорректный идентификатор (хэндл) сеанса
CKR_SESSION_PARALLEL_NOT_SUPPORTED	Данный токен не поддерживает параллельные сессии
CKR_SESSION_READ_ONLY	Невозможно выполнить действие, поскольку это сессия R/O
CKR_SESSION_READ_WRITE_SO_EXISTS	Уже открыта сессия R/W, поэтому открыть сессию R/O невозможно
CKR_SIGNATURE_INVALID	Неверное значение ЭЦП
CKR_SIGNATURE_LEN_RANGE	Значение ЭЦП неверно по длине
CKR_SLOT_ID_INVALID	Слота с данным ID не существует
CKR_TEMPLATE_INCOMPLETE	Для создания объекта недостаточно атрибутов
CKR_TEMPLATE_INCONSISTENT	Заданные атрибуты противоречат друг другу
CKR_TOKEN_NOT_PRESENT	Токен отсутствует в слоте во время вызова функции
CKR_UNWRAPPING_KEY_HANDLE_INVALID	Функции передан некорректный идентификатор (хэндл) ключа дешифрования
CKR_UNWRAPPING_KEY_SIZE_RANGE	Недопустимый размер ключа дешифрования
CKR_UNWRAPPING_KEY_TYPE_INCONSISTENT	Тип ключа дешифрования не соответствует данному механизму
CKR_USER_ALREADY_LOGGED_IN	Данный пользователь уже авторизован
CKR_USER_ANOTHER_ALREADY_LOGGED_IN	Другой пользователь уже авторизован
CKR_USER_NOT_LOGGED_IN	Соответствующий пользователь не авторизован
CKR_USER_PIN_NOT_INITIALIZED	Не инициализирован PIN-код пользователя
CKR_USER_TOO_MANY_TYPES	Невозможно выполнить авторизацию Администратора и Пользователя одновременно
CKR_USER_TYPE_INVALID	Задан некорректный тип пользователя
CKR_WRAPPED_KEY_INVALID	Задан некорректный зашифрованный ключ
CKR_WRAPPED_KEY_LEN_RANGE	Задана некорректная длина зашифрованного ключа
CKR_WRAPPING_KEY_HANDLE_INVALID	Функции передан некорректный идентификатор (хэндл) ключа шифрования
CKR_WRAPPING_KEY_SIZE_RANGE	Недопустимый размер ключа шифрования
CKR_WRAPPING_KEY_TYPE_INCONSISTENT	Тип ключа шифрования не соответствует данному механизму

Специальные коды ошибок

В таблице 2.30 приведен список всех расширенных кодов ошибок стандарта PKCS #11 вместе с их описанием. Расширенные коды ошибок могут возвращать как стандартные функции, так и функции расширения.

Таблица 2.30. Коды ошибок стандарта PKCS #11, поддерживаемые устройствами Рутокен

Код ошибки		Описание
CKR_CORRUPTED_MAPFILE	0x80000001	MAP-файл поврежден (при считывании MAP-файла было обнаружено, что тег заголовка MAP-файла (2 байта) является недопустимым)
CKR_RTPKCS11_DATA_CORRUPTED	0x80000002	Обнаружено нарушение целостности данных на токене (при считывании файла, содержащего объект PKCS#11, было обнаружено, что тег заголовка объекта (2 байта) является недопустимым)
CKR_WRONG_VERSION_FIELD	0x80000003	Файл, содержащий объект PKCS#11, имеет некорректную версию (при считывании MAP-файла или файла, содержащего объект PKCS#11, было обнаружено, что версия заголовка (4 байта) является недопустимой)
CKR_WRONG_PKCS1_ENCODING	0x80000004	Расшифрованное сообщение имеет некорректную форму
CKR_RTPKCS11_RSF_DATA_CORRUPTED	0x80000005	Попытка использовать RSF-файл завершилась неудачей