Функции расширения PKCS #11

Библиотеки rtPKCS11 и rtPKCS11ECP реализуют функции расширения стандарта PKCS#11 для поддержки специфической функциональности устройств Рутокен.

Функции расширения предоставляют разработчику дополнительные возможности по работе с Рутокен, а именно:

- получение расширенной информации о токене;
- выполнение расширенной инициализации памяти токена;
- разблокирование PIN-кода пользователя;
- задание и считывание имени токена произвольной длины;
- запись и чтение информации для лицензирования приложений;
- создание запроса на сертификат и чтение информации о сертификате;
- подпись и проверка подписи сообщения в формате PKCS#7;
- управление флеш-памятью;
- управление беспроводным каналом связи;
- получение записи журнала операций;
- работу с сеансовыми ключами в оперативной памяти.

Функции расширения стандарта, не поддерживающие работу с каким-либо типом устройств Рутокен, при вызове возвращают код ошибки `CKR_FUNCTION_NOT_SUPPORTED`.

Ниже приведен список всех функций расширения стандарта PKCS #11. Поддерживаемые микропрограммой функции отмечены знаком «+». Подробная информацию по каждой функции находится здесь.

Функции расширения стандарта PKCS#11 для библиотеки rtPKCS11ECP

Функции расширения стандарта PKCS#11		**Библиотека rtPKCS11ECP**				
		Модель Рутокен				
Функция	**Описание**	Рутокен Lite	Рутокен ЭЦП PKI / ЭЦП SC	Рутокен ЭЦП Bluetooth	Рутокен ЭЦП 2.0 и 3.0	Рутокен ЭЦП 2.0 Flash / ЭЦП 2.0 Touch
Функции общего назначения						
C_EX_GetFunctionListExtended	получает список функций расширения библиотеки	+	+	+	+	+
Функции для работы со слотами и токенами						
C_EX_GetTokenInfoExtended	получает расширенную информацию о Рутокен	+	+	+	+	+
C_EX_InitToken	выполняет расширенную инициализацию памяти Рутокен	+	+	+	+	+
C_EX_UnblockUserPIN	разблокирует PIN-код пользователя	+	+	+	+	+
C_EX_SetTokenName	задает имя Рутокен произвольной длины	+	+	+	+	+
C_EX_GetTokenName	считывает имя Рутокен произвольной длины	+	+	+	+	+
C_EX_SetLicense	записывает информацию о лицензировании приложения	–	+	+	+	+
C_EX_GetLicense	считывает информацию о лицензировании приложения	–	+	+	+	+
C_EX_SetLocalPIN	устанавливает локальный PIN-код	–	+	+	+	+
C_EX_TokenManage*	выполняет настройку по принудительному сбросу PIN-кода пользователя	–	+	+	+	+
	Работа с кастомизированными PIN-кодами по-умолчанию	–	+	+	+	+
C_EX_SlotManage*	выполняет расширенную инициализацию токена	–	–	–	+	+
	возвращает информацию о локальных PIN-кодах	–	+	+	+	+
	возвращает информацию об установленной опции принудительной смены PIN-кода	–	+	+	+	+
Вспомогательные функции						

C_EX_FreeBuffer	освобождает память, выделенную другими функциями расширения	–	+	+	+	+
Функции для работы с сертификатами						
C_EX_CreateCSR	создает запрос на выпуск сертификата и упаковывает его в PKCS#10 (поддерживаемые ключи: CKK_GOSTR3410, CKK_RSA)	–	+	+	+	+
C_EX_GetCertificateInfoText	получает информацию о сертификате из токена в текстовом виде	–	+	+	+	+
Функции подписи и проверки подписи CMS/PKCS#7 сообщений						
C_EX_PKCS7Sign	подписывает данные в формате PKCS#7 (поддерживаемые механизмы: CKM_GOSTR3410)	–	+	+	+	+
C_EX_PKCS7VerifyInit	инициализирует процесс проверки подписи в формате PKCS#7	–	+	+	+	+
C_EX_PKCS7Verify	проверяет присоединенную подпись в формате PKCS#7	–	+	+	+	+
C_EX_PKCS7VerifyUpdate	проверяет отсоединенную подпись в формате PKCS#7	–	+	+	+	+
C_EX_PKCS7VerifyFinal	завершает проверку отсоединенноń подпись в формате PKCS#7	–	+	+	+	+
Функции для работы с журналом						
C_EX_GetJournal	возвращает содержимое журнала операций	–	–	–	+	+
Функции для работы с флеш-памятью (поддерживаются только устройствами Рутокен Flash)						
C_EX_GetVolumesInfo	получает информацию о существующих на флеш-памяти разделах	–	–	–	–	+
C_EX_GetDriveSize	получает весь объем внешней флеш-памяти	–	–	–	–	+
C_EX_ChangeVolumeAttributes	изменяет атрибуты доступа к разделу	–	–	–	–	+
C_EX_FormatDrive	разбивает флеш-память на разделы	–	–	–	–	+
Функции для работы с беспроводным каналом связи (поддерживаются только устройствами Рутокен Bluetooth)						
C_EX_LoadActivationKey (устарела)	активирует защищенный канал связи с токеном с использованием пароля (поддерживается только в 20-й версии прошивки)	–	–	–	–	–
C_EX_SetActivationPassword	активирует защищенный канал связи с токеном с использованием пароля	–	–	+	–	–
C_EX_GenerateActivationPassword	генерирует пароль для защищенного канала связи	–	–	+	–	–
C_EX_TokenManage*	управляет режимом работы токена и таймаутом беспроводного соединения	–	–	+	–	–
Функции системного назначения						
C_EX_SlotManage*	выполняет контроль целостности (поддерживается только в Рутокен SC 2.0)	–	–	–	–	–

* – функция используется в нескольких секциях

Функции расширения стандарта PKCS#11 для библиотеки rtPKCS11

Функции расширения стандарта PKCS#11	Библиотека rtPKCS11
	Версия Рутокен
	Модель Рутокен

Функция	Описание	≤ #11 Рутокен S Рутокен Lite	≥ #18 Все остальные модели Рутокен
Функции общего назначения			
C_EX_GetFunctionListExtended	получает список функций расширения библиотеки	+	+
Функции для работы со слотами и токенами			
C_EX_GetTokenInfoExtended	получает расширенную информацию о Рутокен	+	+
C_EX_InitToken	выполняет расширенную инициализацию памяти Рутокен	+	+
C_EX_UnblockUserPIN	разблокирует PIN-код пользователя	+	+
C_EX_SetTokenName	задает имя Рутокен произвольной длины	+	+
C_EX_GetTokenName	считывает имя Рутокен произвольной длины	+	+
C_EX_SetLicense	записывает информацию о лицензировании приложения	–	+
C_EX_GetLicense	считывает информацию о лицензировании приложения	–	+