Функции PKCS #11, поддерживаемые устройствами Рутокен

Реализация стандарта PKCS #11 в библиотеках Рутокен связана с некоторыми ограничениями, обусловленными аппаратными характеристиками устройства. Некоторые функции, определенные стандартом, не поддерживаются текущими версиями библиотек rtPKCS11 или rtPKCSECP, но, тем не менее, остаются доступными, и при их вызове возвращается код ошибки CKR_FUNCTION_NOT_SUPPORTED. Наличие подобных ограничений допускается стандартом PKCS #11.

В таблице 2.24 приведен полный список определенных стандартом PKCS #11 функций, знаком «+»отмечено соответствие поддержки конкретной функции конкретной библиотекой и устройством Рутокен, знаком «−» – отсутствие реализации в текущей версии библиотеки.

Подробное описание любой поддерживаемой функции можно найти в стандарте (английский язык) или в данном разделе (русский язык).

Таблица 2.24. Список поддерживаемых библиотеками Рутокен функций стандарта PKCS #11

Функции стандарта PKCS #11			rtPKCS11			rtPKCS11ECP	
Категория	Функция	Описание	Рутокен	Рутокен Lite	Рутокен ЭЦП / 2.0 / PKI	Рутокен Lite	Рутокен ЭЦП / 2.0 / 3.0 / PKI
Функции общего назначения	C_Initialize	инициализирует библиотеку	+	+	+	+	+
	C_Finalize	деинициализирует библиотеку	+	+	+	+	+
	C_GetInfo	получает информацию о библиотеке	+	+	+	+	+
	C_GetFunctionList	получает список всех функций в библиотеке	+	+	+	+	+
Функции для работы со слотами и токенами	C_GetSlotList	получает список слотов в системе	+	+	+	+	+
	C_GetSlotInfo	получает информацию о конкретном слоте	+	+	+	+	+
	C_GetTokenInfo	получает информацию о Рутокен в конкретном слоте	+	+	+	+	+
	C_WaitForSlotEvent	ожидает событие в любом слоте	+	+	+	+	+
	C_GetMechanismList	получает список механизмов, поддерживаемых Рутокен	+	+	+	−	+
	C_GetMechanismInfo	получает информацию о конкретном механизме	+	+	+	−	+
	C_InitToken	инициализирует память Рутокен	+	+	+	+	+
	C_InitPIN	инициализирует PIN-код Пользователя Рутокен	+	+	+	+	+
	C_SetPIN	изменяет PIN-код в пользователя Рутокен, выполнившего вход	+	+	+	+	+
Функции для работы с сессиями	C_OpenSession	открывает новую сессию с Рутокен	+	+	+	+	+
	C_CloseSession	закрывает сессию	+	+	+	+	+
	C_CloseAllSessions	закрывает все сессии	+	+	+	+	+
	C_GetSessionInfo	получает информацию о конкретной сессии	+	+	+	+	+
	C_GetOperationState	получает информацию о состоянии выполнения криптографической операции	−	−	−	−	−
	C_SetOperationState	изменяет состояние выполнения криптографической операции	−	−	−	−	−
	C_Login	выполняет вход пользователя / администратора	+	+	+	+	+
	C_Logout	выполняет выход пользователя / администратора	+	+	+	+	+
Функции для работы с объектами	C_CreateObject*	создает объект	+	+	+	+	+
	C_CopyObject	создает копию объект	−	−	−	−	−
	C_DestroyObject	уничтожает объект	+	+	+	+	+
	C_GetObjectSize	получает информацию о размере объекта в байтах	−	−	−	−	−
	C_GetAttributeValue	получает информацию об атрибутах объекта	+	+	+	+	+
	C_SetAttributeValue	изменяет значение атрибута объекта	+	+	+	+	+
	C_FindObjectsInit	инициализирует процесс поиска объекта	+	+	+	+	+

	C_FindObjects	осуществляет поиск объекта по заданным условиям	+	+	+	+	+
	C_FindObjectsFinal	завершает процесс поиска объекта	+	+	+	+	+
Функции шифрования	C_EncryptInit	инициализирует процесс шифрования	+	+	+	–	+
	C_Encrypt	шифрует данные целиком	+	+	+	–	+
	C_EncryptUpdate	продолжает шифрование данных по частям	–	–	–	+	+
	C_EncryptFinal	завершает шифрование данных по частям	–	–	–	+	+
Функции расшифрования	C_DecryptInit	инициализирует процесс расшифрования	+	+	+	–	+
	C_Decrypt	расшифровывает данные целиком	+	+	+	–	+
	C_DecryptUpdate	продолжает расшифрование данных по частям	–	–	–	+	+
	C_DecryptFinal	завершает расшифрование данных по частям	–	–	–	+	+
Функции хеширования сообщений	C_DigestInit	инициализирует процесс хеширования	+	+	+	–	+
	C_Digest	хеширует данные целиком	+	+	+	–	+
	C_DigestUpdate	продолжает хеширование данных по частям	–	–	–	+	+
	C_DigestKey	хеширует ключ	–	–	–	–	–
	C_DigestFinal	завершает хеширование данных по частям	–	–	–	+	+
Функции создания подписи	C_SignInit	инициализирует процесс подписи	+	+	+	–	+
	C_Sign	подписывает данные целиком	+	+	+	–	+
	C_SignUpdate	продолжает подпись данных по частям	–	–	–	–	–
	C_SignFinal	завершает подпись данных по частям	–	–	–	–	–
	C_SignRecoverInit	инициализирует процесс подписи с восстановлением	–	–	–	–	–
	C_SignRecover	подписывает данные целиком подписью с восстановлением	–	–	–	–	–
Функции проверки подписи	C_VerifyInit	инициализирует процесс проверки подписи	+	+	+	–	+
	C_Verify	проверяет подпись данных, подписанных целиком	+	+	+	–	+
	C_VerifyUpdate	продолжает проверку подписи данных, подписанных по частям	–	–	–	–	–
	C_VerifyFinal	завершает проверку подписи данных, подписанных по частям	–	–	–	–	–
	C_VerifyRecoverInit	инициализирует операцию проверки подписи с восстановлением	–	–	–	–	–
	C_VerifyRecover	проверяет подпись с восстановлением подписанных целиком данных	–	–	–	–	–
Совмещенные функции	C_DigestEncryptUpdate	продолжает одновременное хеширование и шифрование данных по частям	–	–	–	–	–
	C_DecryptDigestUpdate	продолжает одновременное расшифрование и хеширование данных по частям	–	–	–	–	–
	C_SignEncryptUpdate	продолжает одновременную подпись и шифрование данных по частям	–	–	–	–	–
	C_DecryptVerifyUpdate	продолжает одновременное расшифрование и проверку подписи данных, подписанных по частям	–	–	–	–	–
Функции для работы с ключами	C_GenerateKey	генерирует секретный ключ на Рутокен	+	+	+	–	+
	C_GenerateKeyPair	генерирует пару «открытый/закрытый ключ»	+	+	+	–	+
	C_WrapKey	шифрует ключ	–	–	–	–	+
	C_UnwrapKey	расшифровывает ключ	–	–	–	–	+
	C_DeriveKey	вырабатывает ключ из основного ключа	–	–	–	–	+
Функции генерации случайных чисел	C_SeedRandom	задает инициализирующее значение для генератора случайных чисел	–	–	–	–	–
	C_GenerateRandom	генерирует случайное число	+	+	+	+	+
Параллельные функции управления функциями	C_GetFunctionStatus	устаревшая функция, всегда возвращает CKR_FUNCTION_NOT_PARALLEL	–	–	–	–	–
	C_CancelFunction	устаревшая функция, всегда возвращает CKR_FUNCTION_NOT_PARALLEL	–	–	–	–	–

* Устройства Рутокен, сертифицированные ФСБ, не поддерживают создание (импорт) ключей функцией `C_CreateObject` по алгоритмам ГОСТ 28147-89, ГОСТ 34.10-2001 и ГОСТ 34.10-2012 в долговременную память (с флагом `CKA_TOKEN = TRUE`).