Механизмы PKCS#11

Механизмы строго определяют, как должен выполняться тот или иной криптографический процесс.

Библиотеки rtPKCS11 и rtPKCS11ECP поддерживают как стандартные механизмы, так и механизмы расширения стандарта PKCS#11 для реализации работы устройств Рутокен с российскими криптографическими алгоритмами.

В таблице ниже приведен список механизмов PKCS#11, работу которых поддерживают устройства Рутокен, знаком «+» отмечено соответствие поддержки конкретного механизма конкретной библиотекой и устройством Рутокен, знаком «−» – отсутствие реализации в текущей версии библиотеки. Подробное описание любого поддерживаемого механизма можно найти в стандарте (английский язык) или в приложении для механизмов расширения (русский язык).

Механизмы PKCS#11, поддерживаемые устройствами Рутокен

Поддерживаемые механизмы PKCS#11	rtPKCS11			rtPKCS11ECP		
	Рутокен S	Рутокен Lite	Рутокен ЭЦП 2.0 /3.0	Рутокен Lite	Рутокен ЭЦП 2.0	Рутокен ЭЦП 3.0
Механизмы стандарта						
CKM_RSA_PKCS_KEY_PAIR_GEN	+	+	+	−	+	+
CKM_RSA_PKCS	+	+	+	−	+	+
CKM_RSA_PKCS_OAEP	-	-	-	-	+	+
CKM_EC_KEY_PAIR_GEN	-	-	-	-	-	+
CKM_ECDSA	-	-	-	-	-	+
CKM_GENERIC_SECRET_KEY_GEN	+	+	+	−	−	−
CKM_MD2	+	+	−	−	−	−
CKM_MD5	+	+	+	−	+	+
CKM_SHA_1	+	+	+	−	+	+
CKM_SHA256	+	+	+	-	+	+
CKM_SHA512	+	+	+	-	+	+
CKM_SHA512_RSA_PKCS	−	−	−	−	+	+
CKM_SHA384_RSA_PKCS	−	−	−	−	+	+
CKM_SHA256_RSA_PKCS	−	−	−	−	+	+
CKM_SHA224_RSA_PKCS	−	−	−	−	+	+
CKM_SHA1_RSA_PKCS	−	−	−	−	+	+
CKM_MD5_RSA_PKCS	−	−	−	−	+	+
CKM_GOSTR3410_KEY_PAIR_GEN	−	−	−	−	+	+
CKM_GOSTR3410	−	−	−	−	+	+
CKM_GOSTR3410_WITH_GOSTR3411	−	−	−	−	+	+
CKM_GOSTR3410_KEY_WRAP	−	−	−	−	−	−
CKM_GOSTR3410_DERIVE	−	−	−	−	+	+
CKM_GOSTR3411	−	−	−	−	+	+
CKM_GOSTR3411_HMAC	−	−	−	−	+	+
CKM_GOST28147_KEY_GEN	−	−	−	−	+	+
CKM_GOST28147_ECB	−	−	−	−	+	+
CKM_GOST28147	−	−	−	−	+	+
CKM_GOST28147_MAC	−	−	−	−	+	+
CKM_GOST28147_KEY_WRAP	−	−	−	−	+	+
Механизмы расширения						

CKM_GOST_KEY_GEN	+	–	–	–	–	–
CKM_GOST	+	–	–	–	–	–
CKM_GOSTR3410_512_KEY_PAIR_GEN	–	–	–	–	+*	+
CKM_GOSTR3410_512	–	–	–	–	+*	+
CKM_GOSTR3410_12_DERIVE	–	–	–	–	+*	+
CKM_GOSTR3410_WITH_GOSTR3411_12_256	–	–	–	–	+*	+
CKM_GOSTR3410_WITH_GOSTR3411_12_512	–	–	–	–	+*	+
CKM_GOSTR3411_12_256	–	–	–	–	+*	+
CKM_GOSTR3411_12_512	–	–	–	–	+*	+
CKM_GOSTR3411_12_256_HMAC	–	–	–	–	+*	+
CKM_GOSTR3411_12_512_HMAC	–	–	–	–	+*	+
CKM_KUZNECHIK_KEY_GEN	–	–	–	–	–	+
CKM_MAGMA_KEY_GEN	–	–	–	–	–	+
CKM_KUZNECHIK_ECB	–	–	–	–	–	+
CKM_MAGMA_ECB	–	–	–	–	–	+
CKM_KUZNECHIK_CTR_ACPKM	–	–	–	–	–	+
CKM_MAGMA_CTR_ACPKM	–	–	–	–	–	+
CKM_KUZNYECHIK_MAC	–	–	–	–	–	+
CKM_MAGMA_MAC	–	–	–	–	–	+
CKM_KUZNECHIK_MGM	–	–	–	–	–	+
CKM_MAGMA_MGM	–	–	–	–	–	+
CKM_KUZNECHIK_KEXP_15_WRAP	–	–	–	–	–	+
CKM_MAGMA_KEXP_15_WRAP	–	–	–	–	–	+
CKM_VENDOR_GOST_KEG	–	–	–	–	–	+
CKM_KDF_TREE_GOSTR3411_2012_256	–	–	–	–	–	+
CKM_KDF_HMAC3411_2012_256	–	–	–	–	–	+

* начиная с прошивки версии 20.

> *Версию прошивки Рутокен можно узнать в панели управления Рутокен, нажав на кнопку* Информация... *Третья пара цифр в разделенном точками поле* Версия *означает номер прошивки.*

В таблице ниже представлены механизмы, поддерживающие разные криптографические операции устройствами Рутокен.

Поддержка криптографических операций устройствами Рутокен

Поддерживаемые механизмы PKCS#11	Функции						
	Шифрование/ Расшифрование	Подпись/ Проверка подписи	Подпись с восстановлением/ Проверка подписи с восстановлением	Хэширование	Генерация ключа/ ключевой пары	Шифрование ключа/ Расшифрование ключа	Извлечение ключа из ключа
Механизмы стандарта							
CKM_RSA_PKCS_KEY_PAIR_GEN	–	–	–	–	+	–	–
CKM_RSA_PKCS	+*	+*	–	–	–	–	–
CKM_EC_KEY_PAIR_GEN	–	–	–	–	+	–	–
CKM_ECDSA	–	+*	–	–	–	–	–
CKM_SHA512_RSA_PKCS	+*	+*	–	–	–	–	–

CKM_SHA384_RSA_PKCS	+*	+*	–	–	–	–	–
CKM_SHA256_RSA_PKCS	+*	+*	–	–	–	–	–
CKM_SHA224_RSA_PKCS	+*	+*	–	–	–	–	–
CKM_SHA1_RSA_PKCS	+*	+*	–	–	–	–	–
CKM_MD5_RSA_PKCS	+*	+*	–	–	–	–	–
CKM_MD2	–	–	–	+	–	–	–
CKM_MD5	–	–	–	+	–	–	–
CKM_SHA_1	–	–	–	+	–	–	–
CKM_SHA_256	–	–	–	+	–	–	–
CKM_SHA_512	–	–	–	+	–	–	–
CKM_GENERIC_SECRET_KEY_GEN	–	–	–	–	+	–	–
CKM_GOSTR3410_KEY_PAIR_GEN	–	–	–	–	+	–	–
CKM_GOSTR3410	–	+**	–	-	–	–	–
CKM_GOSTR3410_WITH_GOSTR3411	–	+	–	–	–	–	–
CKM_GOSTR3410_KEY_WRAP	–	–	–	–	–	–	-
CKM_GOSTR3410_DERIVE	–	–	–	–	–	–	+
CKM_GOSTR3411	–	–	–	+	–	–	–
CKM_GOSTR3411_HMAC	–	+	–	–	–	–	–
CKM_GOST28147_KEY_GEN	–	–	–	–	+	–	–
CKM_GOST28147_ECB	+	–	–	–	–	–	–
CKM_GOST28147	+	–	–	–	–	–	–
CKM_GOST28147_MAC	–	+	–	–	–	–	–
CKM_GOST28147_KEY_WRAP	–	–	–	–	–	+	–
Механизмы расширения							
CKM_GOST_KEY_GEN	–	–	–	–	+	–	–
CKM_GOST	+	–	–	–	–	–	–
CKM_GOSTR3410_512_KEY_PAIR_GEN	–	–	–	–	+	–	–
CKM_GOSTR3410_512	–	+**	–	-	–	–	–
CKM_GOSTR3410_12_DERIVE	–	–	–	–	–	–	+
CKM_GOSTR3410_WITH_GOSTR3411_12_256	–	+	–	–	–	–	–
CKM_GOSTR3410_WITH_GOSTR3411_12_512	–	+	–	–	–	–	–
CKM_GOSTR3411_12_256	–	–	–	+	–	–	–
CKM_GOSTR3411_12_512	–	–	–	+	–	–	–
CKM_GOSTR3411_12_256_HMAC	–	+	–	–	–	–	–
CKM_GOSTR3411_12_512_HMAC	–	+	–	–	–	–	–
CKM_KUZNECHIK_KEY_GEN	–	–	–	–	+	–	–
CKM_MAGMA_KEY_GEN	–	–	–	–	+	–	–
CKM_KUZNECHIK_ECB	+	–	–	–	–	–	–
CKM_MAGMA_ECB	+	–	–	–	–	–	–
CKM_KUZNECHIK_CTR_ACPKM	+	–	–	–	–	–	–
CKM_MAGMA_CTR_ACPKM	+	–	–	–	–	–	–
CKM_KUZNYECHIK_MAC	–	+	–	–	–	–	–

CKM_MAGMA_MAC	–	+	–	–	–	–	–
CKM_KUZNECHIK_MGM	+	+	–	–	–	–	–
CKM_MAGMA_MGM	+	+	–	–	–	–	–
CKM_KUZNECHIK_KEXP_15_WRAP	–	–	–	–	–	+	–
CKM_MAGMA_KEXP_15_WRAP	–	–	–	–	–	+	–
CKM_VENDOR_GOST_KEG	–	–	–	–	–	–	+
CKM_KDF_TREE_GOSTR3411_2012_256	–	–	–	–	–	–	+
CKM_KDF_HMAC3411_2012_256	–	–	–	–	–	–	+

* - только целиком

** – не правильно передавать в C_Sign