

Объекты PKCS #11

Объекты стандарта PKCS #11, поддерживаемые устройствами Рутокен

Поддержка библиотекой `ртPKCS11` определённых стандартом⁽¹⁾ и производителем⁽²⁾ классов и типов классов объектов отражена в таблице ниже.

Объекты, поддерживаемые устройствами Рутокен

Классы объектов (значение атрибута CKA_CLASS)	Тип класса		
	Базовый класс	(значение атрибута CKA_KEY_TYPE)	(значение атрибута CKA_CERTIFICATE_TYPE)
CKO_DATA	+	–	–
CKO_PUBLIC_KEY	+	CKK_GOSTR3410 ¹ CKK_GOSTR3410_512 ² CKK_RSA ¹ CKK_ECDSA ¹	–
CKO_PRIVATE_KEY	+	CKK_GOSTR3410 ¹ CKK_GOSTR3410_512 ² CKK_RSA ¹ CKK_ECDSA ¹	–
CKO_SECRET_KEY	+	CKK_GENERIC_SECRET ¹ CKK_GOST ² CKK_GOST28147 ¹ CKK_KUZNECHIK ² CKK_MAGMA ² CKK_KUZNECHIK_TWIN_KEY ² CKK_MAGMA_TWIN_KEY ²	–
CKO_CERTIFICATE	+	–	CKC_X_509 ¹ CKC_X_509_ATTR_CERT ¹

¹ тип класса, определенный стандартом

² тип класса, определенный производителем

При работе с объектами поддерживаются стандартные и расширенные (определенные производителем) атрибуты, перечисленные в таблице ниже и отмеченные знаком «+» для поддерживаемого объекта. Под поддержкой атрибута понимается его любое использование, например, инициализация при создании, изменение после создания, чтение, поиск по атрибуту и др. Подробную информацию по стандартным атрибутам можно найти в [стандарте](#) (английский язык) или в [данном разделе](#) (стандартные и определенные производителем атрибуты, русский язык).

Атрибуты объектов, поддерживаемые устройствами Рутокен

Название атрибута	Класс объекта (значение атрибута CKA_CLASS)				
	CKO_DATA	CKO_PUBLIC_KEY	CKO_PRIVATE_KEY	CKO_SECRET_KEY	CKO_CERTIFICATE
Общие атрибуты объектов (Common Object Attributes)					
CKA_CLASS	+	+	+	+	+
Общие атрибуты объектов хранения (Common Storage Object Attributes)					
CKA_TOKEN	+	+	+	+	+
CKA_PRIVATE	+	+	+	+	+

CKA_MODIFIABLE	+	+	+	+	+
CKA_LABEL	+	+	+	+	+
CKA_COPYABLE	+	+	+	+	+
Атрибуты объектов данных (Data Object Attributes)					
CKA_APPLICATION	+	-	-	-	-
CKA_OBJECT_ID	+	-	-	-	-
CKA_VALUE	+	-	-	-	-
Общие атрибуты объектов ключей (Common Key Attributes)					
CKA_KEY_TYPE	-	+	+	+	-
CKA_ID	-	+	+	+	-
CKA_START_DATE	-	+	+	+	-
CKA_END_DATE	-	+	+	+	-
CKA_DERIVE	-	+	+	+	-
CKA_LOCAL	-	+	+	+	-
CKA_KEY_GEN_MECHANISM	-	+	+	+	-
CKA_ALLOWED_MECHANISMS	-	+	+	+	-
Общие атрибуты открытых ключей (Common Public Key Attributes)					
CKA_SUBJECT	-	+	-	-	-
CKA_ENCRYPT	-	+	-	-	-
CKA_VERIFY	-	+	-	-	-
CKA_VERIFY_RECOVER	-	+	-	-	-
CKA_WRAP	-	+	-	-	-
CKA_TRUSTED	-	+	-	-	-
CKA_WRAP_TEMPLATE	-	+	-	-	-
Атрибуты открытых ключей, определенные производителем (Rutoken Vendors Defined Public Key Attributes)					
CKA_CAP1_ID	-	+	-	-	-
CKA_PUBLIC_KEY_RSF_ID	-	+	-	-	-
CKA_PRIVATE_KEY_RSF_ID	-	+	-	-	-
CKA_VENDOR_KEY_JOURNAL	-	+	-	-	-
Общие атрибуты закрытых ключей (Common Private Key Attributes)					
CKA_SUBJECT	-	-	+	-	-
CKA_SENSITIVE	-	-	+	-	-
CKA_DECRYPT	-	-	+	-	-
CKA_SIGN	-	-	+	-	-
CKA_SIGN_RECOVER	-	-	+	-	-
CKA_UNWRAP	-	-	+	-	-
CKA_EXTRACTABLE	-	-	+	-	-
CKA_ALWAYS_SENSITIVE	-	-	+	-	-
CKA_NEVER_EXTRACTABLE	-	-	+	-	-
CKA_WRAP_WITH_TRUSTED	-	-	+	-	-
CKA_UNWRAP_TEMPLATE	-	-	+	-	-
CKA_ALWAYS_AUTHENTICATE	-	-	+	-	-
Атрибуты закрытых ключей, определенные производителем (Rutoken Vendors Defined Private Key Attributes)					

CKA_CAPI_ID	-	-	+	-	-
CKA_PUBLIC_KEY_RSF_ID	-	-	+	-	-
CKA_PRIVATE_KEY_RSF_ID	-	-	+	-	-
CKA_VENDOR_KEY_PIN_ENTER	-	-	+*	-	-
CKA_VENDOR_KEY_CONFIRM_OP	-	-	+*	-	-
CKA_VENDOR_KEY_JOURNAL	-	-	+*	-	-
Общие атрибуты секретных ключей (Common Secret Key Attributes)					
CKA_SENSITIVE	-	-	-	+	-
CKA_ENCRYPT	-	-	-	+	-
CKA_DECRYPT	-	-	-	+	-
CKA_SIGN	-	-	-	+	-
CKA_VERIFY	-	-	-	+	-
CKA_WRAP	-	-	-	+	-
CKA_UNWRAP	-	-	-	+	-
CKA_EXTRACTABLE	-	-	-	+	-
CKA_ALWAYS_SENSITIVE	-	-	-	+	-
CKA_NEVER_EXTRACTABLE	-	-	-	+	-
CKA_CHECK_VALUE	-	-	-	+	-
CKA_WRAP_WITH_TRUSTED	-	-	-	+	-
CKA_TRUSTED	-	-	-	+	-
CKA_WRAP_TEMPLATE	-	-	-	+	-
CKA_UNWRAP_TEMPLATE	-	-	-	+	-
Атрибуты секретных ключей, определенные производителем (Rutoken Vendors Defined Secret Key Attributes)					
CKA_SECRET_KEY_RSF_ID	-	-	-	+	-
Общие атрибуты объектов сертификатов ключей (Common Certificate Object Attributes)					
CKA_CERTIFICATE_TYPE	-	-	-	-	+
CKA_TRUSTED	-	-	-	-	+
CKA_CERTIFICATE_CATEGORY	-	-	-	-	+
CKA_CHECK_VALUE	-	-	-	-	+
CKA_START_DATE	-	-	-	-	+
CKA_END_DATE	-	-	-	-	+
Атрибуты сертификатов, определенные производителем (Rutoken Vendors Defined Certificate Object Attributes)					
CKA_CAPI_ID	-	-	-	-	+

* - атрибуты, доступные только для Рутокен PINPad