

# Объекты PKCS #11

## Объекты стандарта PKCS #11, поддерживаемые устройствами Рутокен

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

### Объекты, поддерживаемые устройствами Рутокен

| Классы объектов<br>(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 <sup>1</sup><br>CKK_GOSTR3410_512 <sup>2</sup><br>CKK_RSA <sup>1</sup><br>CKK_ECDSA <sup>1</sup>                                                                                                           | –                                                          |
| CKO_PRIVATE_KEY                                  | +             | CKK_GOSTR3410 <sup>1</sup><br>CKK_GOSTR3410_512 <sup>2</sup><br>CKK_RSA <sup>1</sup><br>CKK_ECDSA <sup>1</sup>                                                                                                           | –                                                          |
| CKO_SECRET_KEY                                   | +             | CKK_GENERIC_SECRET <sup>1</sup><br>CKK_GOST <sup>2</sup><br>CKK_GOST28147 <sup>1</sup><br>CKK_KUZNECHIK <sup>2</sup><br>CKK_MAGMA <sup>2</sup><br>CKK_KUZNECHIK_TWIN_KEY <sup>2</sup><br>CKK_MAGMA_TWIN_KEY <sup>2</sup> | –                                                          |
| CKO_CERTIFICATE                                  | +             | –                                                                                                                                                                                                                        | CKC_X_509 <sup>1</sup><br>CKC_X_509_ATTR_CERT <sup>1</sup> |

<sup>1</sup> тип класса, определенный стандартом

<sup>2</sup> 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                                                                                                  | + | + | + | + | + |
| <b>Атрибуты объектов данных (Data Object Attributes)</b>                                                      |   |   |   |   |   |
| CKA_APPLICATION                                                                                               | + | - | - | - | - |
| CKA_OBJECT_ID                                                                                                 | + | - | - | - | - |
| CKA_VALUE                                                                                                     | + | - | - | - | - |
| <b>Общие атрибуты объектов ключей (Common Key Attributes)</b>                                                 |   |   |   |   |   |
| CKA_KEY_TYPE                                                                                                  | - | + | + | + | - |
| CKA_ID                                                                                                        | - | + | + | + | - |
| CKA_START_DATE                                                                                                | - | + | + | + | - |
| CKA_END_DATE                                                                                                  | - | + | + | + | - |
| CKA_DERIVE                                                                                                    | - | + | + | + | - |
| CKA_LOCAL                                                                                                     | - | + | + | + | - |
| CKA_KEY_GEN_MECHANISM                                                                                         | - | + | + | + | - |
| CKA_ALLOWED_MECHANISMS                                                                                        | - | + | + | + | - |
| <b>Общие атрибуты открытых ключей (Common Public Key Attributes)</b>                                          |   |   |   |   |   |
| CKA_SUBJECT                                                                                                   | - | + | - | - | - |
| CKA_ENCRYPT                                                                                                   | - | + | - | - | - |
| CKA_VERIFY                                                                                                    | - | + | - | - | - |
| CKA_VERIFY_RECOVER                                                                                            | - | + | - | - | - |
| CKA_WRAP                                                                                                      | - | + | - | - | - |
| CKA_TRUSTED                                                                                                   | - | + | - | - | - |
| CKA_WRAP_TEMPLATE                                                                                             | - | + | - | - | - |
| <b>Атрибуты открытых ключей, определенные производителем (Rutoken Vendors Defined Public Key Attributes)</b>  |   |   |   |   |   |
| CKA_CAPI_ID                                                                                                   | - | + | - | - | - |
| CKA_PUBLIC_KEY_RSF_ID                                                                                         | - | + | - | - | - |
| CKA_PRIVATE_KEY_RSF_ID                                                                                        | - | + | - | - | - |
| CKA_VENDOR_KEY_JOURNAL                                                                                        | - | + | - | - | - |
| <b>Общие атрибуты закрытых ключей (Common Private Key Attributes)</b>                                         |   |   |   |   |   |
| 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                                                                                       | - | - | + | - | - |
| <b>Атрибуты закрытых ключей, определенные производителем (Rutoken Vendors Defined Private Key Attributes)</b> |   |   |   |   |   |

|                                                                                                                   |   |   |    |   |   |
|-------------------------------------------------------------------------------------------------------------------|---|---|----|---|---|
| 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                                                                                            | - | - | +* | - | - |
| <b>Общие атрибуты секретных ключей (Common Secret Key Attributes)</b>                                             |   |   |    |   |   |
| 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                                                                                               | - | - | -  | + | - |
| <b>Атрибуты секретных ключей, определенные производителем (Rutoken Vendors Defined Secret Key Attributes)</b>     |   |   |    |   |   |
| CKA_SECRET_KEY_RSF_ID                                                                                             | - | - | -  | + | - |
| <b>Общие атрибуты объектов сертификатов ключей (Common Certificate Object Attributes)</b>                         |   |   |    |   |   |
| CKA_CERTIFICATE_TYPE                                                                                              | - | - | -  | - | + |
| CKA_TRUSTED                                                                                                       | - | - | -  | - | + |
| CKA_CERTIFICATE_CATEGORY                                                                                          | - | - | -  | - | + |
| CKA_CHECK_VALUE                                                                                                   | - | - | -  | - | + |
| CKA_START_DATE                                                                                                    | - | - | -  | - | + |
| CKA_END_DATE                                                                                                      | - | - | -  | - | + |
| <b>Атрибуты сертификатов, определенные производителем (Rutoken Vendors Defined Certificate Object Attributes)</b> |   |   |    |   |   |
| CKA_CAPI_ID                                                                                                       | - | - | -  | - | + |

\* - атрибуты, доступные только для Рутокен PINPad