**СКЗИ «libkalkancryptwr-64.so.1.1.1»**

**Описание флагов**

**Константы криптографической библиотеки libkalkancryptwr-64.so**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Константы, определяющие способ хранения ключей/сертификатов (вид хранилища/носителя).**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значение** | | **Описание** | | **KCST\_PKCS12** | **0x00000001** | **Файловая система (небезопасный способ хранения ключей)** | | **KCST\_KZIDCARD** | **0x00000002** | **Удостоверение личности гражданина РК** | | **KCST\_KAZTOKEN** | **0x00000004** | **Казтокен** | | **KCST\_ETOKEN72K** | **0x00000008** | **eToken 72k** | | **KCST\_JACARTA** | **0x00000010** | **JaCarta** | | **KCST\_X509CERT** | **0x00000020** | **Сертификат X509** | | **KCST\_AKEY** | **0x00000040** | **aKey** | | **KCST\_ETOKEN5110** | **0x00000080** | **eToken 5110** | |
| **Константы, определяющие принадлежность сертификата.**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значения** | | **Описание** | | **KC\_CERT\_CA** | **0x00000201** | **Корневой сертификат УЦ** | | **KC\_CERT\_INTERMEDIATE** | **0x00000202** | **Сертификат промежуточного УЦ** | | **KC\_CERT\_USER** | **0x00000204** | **Сертификат пользователя** | |
| **Константы, определяющие тип кодировки.**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значения** | | **Описание** | | **KC\_CERT\_DER** | **0x00000101** | **Кодировка DER** | | **KC\_CERT\_PEM** | **0x00000102** | **Кодировка PEM** | | **KC\_CERT\_B64** | **0x00000104** | **Кодировка Base64** | |
| **Константы, определяющие тип валидации.**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значения** | | **Описание** | | **KC\_USE\_NOTHING** | **0x00000401** | **Не делать проверок** | | **KC\_USE\_CRL** | **0x00000402** | **Проверка сертификата по списку отозванных сертификатов** | | **KC\_USE\_OCSP** | **0x00000404** | **Проверка сертификата посредством сервиса OCSP** | |
| **Константы, определяющие значение поля/расширения в запросе/сертификате.**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значения** | | **Описание** | | **KC\_CERTPROP\_ISSUER\_COUNTRYNAME** | **0x00000801** | **Страна издателя** | | **KC\_CERTPROP\_ISSUER\_SOPN** | **0x00000802** | **Название штата или провинции издателя** | | **KC\_CERTPROP\_ISSUER\_LOCALITYNAME** | **0x00000803** | **Населённый пункт издателя** | | **KC\_CERTPROP\_ISSUER\_ORG\_NAME** | **0x00000804** | **Наименование организации издателя** | | **KC\_CERTPROP\_ISSUER\_ORGUNIT\_NAME** | **0x00000805** | **Название организационного подразделения издателя** | | **KC\_CERTPROP\_ISSUER\_COMMONNAME** | **0x00000806** | **Имя Фамилия издателя** | | **KC\_CERTPROP\_SUBJECT\_COUNTRYNAME** | **0x00000807** | **Страна субъекта** | | **KC\_CERTPROP\_SUBJECT\_SOPN** | **0x00000808** | **Название штата или провинции субъекта** | | **KC\_CERTPROP\_SUBJECT\_LOCALITYNAME** | **0x00000809** | **Населенный пункт субъекта** | | **KC\_CERTPROP\_SUBJECT\_COMMONNAME** | **0x0000080a** | **Общее имя субъекта** | | **KC\_CERTPROP\_SUBJECT\_GIVENNAME** | **0x0000080b** | **Имя субъекта** | | **KC\_CERTPROP\_SUBJECT\_SURNAME** | **0x0000080c** | **Фамилия субъекта** | | **KC\_CERTPROP\_SUBJECT\_SERIALNUMBER** | **0x0000080d** | **Серийный номер субъекта** | | **KC\_CERTPROP\_SUBJECT\_EMAIL** | **0x0000080e** | **e-mail субъекта** | | **KC\_CERTPROP\_SUBJECT\_ORG\_NAME** | **0x0000080f** | **Наименование организации субъекта** | | **KC\_CERTPROP\_SUBJECT\_ORGUNIT\_NAME** | **0x00000810** | **Название организационного подразделения субъекта** | | **KC\_CERTPROP\_SUBJECT\_BC** | **0x00000811** | **Бизнес категория субъекта** | | **KC\_CERTPROP\_SUBJECT\_DC** | **0x00000812** | **Доменный компонент субъекта** | | **KC\_CERTPROP\_NOTBEFORE** | **0x00000813** | **Дата действителен с** | | **KC\_CERTPROP\_NOTAFTER** | **0x00000814** | **Дата действителен по** | | **KC\_CERTPROP\_KEY\_USAGE** | **0x00000815** | **Использование ключа** | | **KC\_CERTPROP\_EXT\_KEY\_USAGE** | **0x00000816** | **Расширенное использование ключа** | | **KC\_CERTPROP\_AUTH\_KEY\_ID** | **0x00000817** | **Идентификатор ключа центра сертификации** | | **KC\_CERTPROP\_SUBJ\_KEY\_ID** | **0x00000818** | **Идентификатор ключа субъекта** | | **KC\_CERTPROP\_CERT\_SN** | **0x00000819** | **Серийный номер сертификата** | | **KC\_CERTPROP\_ISSUER\_DN** | **0x0000081a** | **Отличительное имя издателя** | | **KC\_CERTPROP\_SUBJECT\_DN** | **0x0000081b** | **Отличительное имя субъекта** | | **KC\_CERTPROP\_SIGNATURE\_ALG** | **0x0000081c** | **Алгоритм подписи** | | **KC\_CERTPROP\_PUBKEY** | **0x0000081d** | **Получение открытого ключа** | | **KC\_CERTPROP\_POLICIES\_ID** | **0x0000081e** | **Получение идентификатора политики сертификата** | | **KC\_CERTPROP\_OCSP** | **0x0000081f** | **Получение URL-адреса OCSP** | | **KC\_CERTPROP\_GET\_CRL** | **0x00000820** | **Получение URL-адреса CRL** | | **KC\_CERTPROP\_GET\_DELTA\_CRL** | **0x00000821** | **Получение URL-адреса delta CRL** | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Константы, определяющие дополнительные условия выполнения операций. Используется как параметр в функциях.**  **Значения:**   |  |  |  | | --- | --- | --- | | **KC\_SIGN\_DRAFT** | **0x00000001** | **Сырая подпись (draft sign)** | | **KC\_SIGN\_CMS** | **0x00000002** | **Подпись в формате CMS** | | **KC\_IN\_PEM** | **0x00000004** | **Входные данные в формате PEM** | | **KC\_IN\_DER** | **0x00000008** | **Входные данные в кодировке DER** | | **KC\_IN\_BASE64** | **0x00000010** | **Входные данные в кодировке BASE64** | | **KC\_IN2\_BASE64** | **0x00000020** | **Дополнительные входные данные в кодировке BASE64** | | **KC\_DETACHED\_DATA** | **0x00000040** | **Отсоединенная подпись** | | **KC\_WITH\_CERT** | **0x00000080** | **Вложить сертификат в подпись** | | **KC\_WITH\_TIMESTAMP** | **0x00000100** | **Добавить в подпись метку времени** | | **KC\_OUT\_PEM** | **0x00000200** | **Выходные данные в формате PEM** | | **KC\_OUT\_DER** | **0x00000400** | **Выходные данные в кодировке DER** | | **KC\_OUT\_BASE64** | **0x00000800** | **Выходные данные в кодировке BASE64** | | **KC\_PROXY\_OFF** | **0x00001000** | **Отключить использование прокси-сервера и стереть настройки.** | | **KC\_PROXY\_ON** | **0x00002000** | **Включить и установить настройки прокси-сервера (адрес и порт)** | | **KC\_PROXY\_AUTH** | **0x00004000** | **Прокси-сервер требует авторизацию (логин/пароль)** | | **KC\_IN\_FILE** | **0x00008000** | **Использовать, если параметр inData/outData содержит абсолютный путь к файлу.** | | **KC\_NOCHECKCERTTIME** | **0x00010000** | **Не проверять срок действия сертификата при построении цепочки до корневого (для проверки старых подписей с просроченным сертификатом)** | | **KC\_HASH\_SHA256** | **0x00020000** | **Алгоритм хеширования sha256** | | **KC\_HASH\_GOST95** | **0x00040000** | **Алгоритм хеширования Gost34311\_95** | | **KC\_GET\_OCSP\_RESPONSE** | **0x00080000** | **Получить ответ от OCSP-сервиса** | |
| **Константы, определяющие подробные коды ошибок времени выполнения. Код ошибки и подробный текст можно получить с помощью функции GetLastError.**  **Значения:**   |  |  |  | | --- | --- | --- | | **KCR\_OK** | **0x00000000** | **Нет ошибки** | | **KCR\_ERROR\_READ\_PKCS12** | **0x08F00002** | **Невозможно прочитать файл формата pkcs#12** | | **KCR\_ERROR\_OPEN\_PKCS12** | **0x08F00003** | **Невозможно открыть файл формата pkcs12** | | **KCR\_INVALID\_PROPID** | **0x08F00004** | **Недопустимый идентификатор расширения сертификата** | | **KCR\_BUFFER\_TOO\_SMALL** | **0x08F00005** | **Размер буфера слишком мал** | | **KCR\_CERT\_PARSE\_ERROR** | **0x08F00006** | **Невозможно разобрать (распарсить) сертификат** | | **KCR\_INVALID\_FLAG** | **0x08F00007** | **Недопустимый флаг** | | **KCR\_OPENFILEERR** | **0x08F00008** | **Невозможно открыть файл** | | **KCR\_INVALIDPASSWORD** | **0x08F00009** | **Неправильный пароль** | | **KCR\_MEMORY\_ERROR** | **0x08F0000d** | **Невозможно выделить память** | | **KCR\_CHECKCHAINERROR** | **0x08F0000e** | **Не найден сертификат УЦ или сертификат пользователя при проверки цепочки** | | **KCR\_VALIDTYPEERROR** | **0x08F00010** | **Недопустимый тип валидации сертификата** | | **KCR\_BADCRLFORMAT** | **0x08F00011** | **Некорректный формат CRL** | | **KCR\_LOADCRLERROR** | **0x08F00012** | **Невозможно загрузить CRL** | | **KCR\_LOADCRLSERROR** | **0x08F00013** | **Невозможно загрузить CRL-ы** | | **KCR\_UNKNOWN\_ALG** | **0x08F00015** | **Неизвестный алгоритм подписи** | | **KCR\_KEYNOTFOUND** | **0x08F00016** | **Не найден приватный ключ пользователя** | | **KCR\_SIGN\_INIT\_ERROR** | **0x08F00017** | **Невозможно инициализировать менеджера подписи** | | **KCR\_SIGN\_ERROR** | **0x08F00018** | **Не удалось сгенерировать цифровую подпись** | | **KCR\_ENCODE\_ERROR** | **0x08F00019** | **Ошибка шифрования** | | **KCR\_INVALID\_FLAGS** | **0x08F0001a** | **Недопустимые флаги** | | **KCR\_CERTNOTFOUND** | **0x08F0001b** | **Не найден сертификат пользователя** | | **KCR\_VERIFYSIGNERROR** | **0x08F0001c** | **Ошибка верификации подписи xml** | | **KCR\_BASE64\_DECODE\_ERROR** | **0x08F0001d** | **Ошибка дешифровки из Base 64** | | **KCR\_UNKNOWN\_CMS\_FORMAT** | **0x08F0001e** | **Неизвестный формат CMS** | | **KCR\_CA\_CERT\_NOT\_FOUND** | **0x08F00020** | **Не найден сертификат УЦ** | | **KCR\_XMLSECINIT\_ERROR** | **0x08F00021** | **Ошибка инициализации xmlsec** | | **KCR\_LOADTRUSTEDCERTSERR** | **0x08F00022** | **Ошибка загрузки доверенных сертификатов** | | **KCR\_SIGN\_INVALID** | **0x08F00023** | **Недопустимая подпись xml** | | **KCR\_NOSIGNFOUND** | **0x08F00024** | **Не найдена подпись во входных данных** | | **KCR\_DECODE\_ERROR** | **0x08F00025** | **Ошибка дешифрования** | | **KCR\_XMLPARSEERROR** | **0x08F00026** | **Невозможно разобрать (распарсить) xml** | | **KCR\_XMLADDIDERROR** | **0x08F00027** | **Не удалось добавить атрибут ID** | | **KCR\_XMLINTERNALERROR** | **0x08F00028** | **Ошибка при работе с xml** | | **KCR\_XMLSETSIGNERROR** | **0x08F00029** | **Не удалось подписать xml** | | **KCR\_OPENSSLERROR** | **0x08F0002a** | **Ошибка openssl** | | **KCR\_NOTOKENFOUND** | **0x08F0002c** | **Не найден токен** | | **KCR\_OCSP\_ADDCERTERR** | **0x08F0002d** | **Не удалось добавить сертификат в ocsp** | | **KCR\_OCSP\_PARSEURLERR** | **0x08F0002e** | **Не удалось разобрать url** | | **KCR\_OCSP\_ADDHOSTERR** | **0x08F0002f** | **Не удалось добавить хост** | | **KCR\_OCSP\_REQERR** | **0x08F00030** | **Не удалось добавить текущее время в запрос** | | **KCR\_OCSP\_CONNECTIONERR** | **0x08F00031** | **Ошибка подключения к OCSP респондеру** | | **KCR\_VERIFY\_NODATA** | **0x08F00032** | **Нет входных данных для верификации** | | **KCR\_IDATTR\_NOTFOUND** | **0x08F00033** | **Не найден атрибут ID** | | **KCR\_IDRANGE** | **0x08F00034** | **Некорректный идентификатор** | | **KCR\_READERNOTFOUND** | **0x08F00037** | **Не найден ридер** | | **KCR\_GETCERTPROPERR** | **0x08F00038** | **Не удалось получить значение атрибута** | | **KCR\_SIGNFORMMAT** | **0x08F00039** | **Неизвестный формат подписи** | | **KCR\_INDATAFORMAT** | **0x08F0003a** | **Неизвестный формат входных данных** | | **KCR\_OUTDATAFORMAT** | **0x08F0003b** | **Неизвестный формат выходных данных** | | **KCR\_VERIFY\_INIT\_ERROR** | **0x08F0003c** | **Невозможно инициализировать менеджера верификации подписи** | | **KCR\_VERIFY\_ERROR** | **0x08F0003d** | **Не удалось верифицировать цифровую подпись** | | **KCR\_HASH\_ERROR** | **0x08F0003e** | **Не удалось хэшировать данные** | | **KCR\_SIGNHASH\_ERROR** | **0x08F0003f** | **Не удалось подписать хэшированные данные** | | **KCR\_CACERTNOTFOUND** | **0x08F00040** | **Не найден сертификат УЦ в хранилище сертификатов** | | **KCR\_CERTTIMEINVALID** | **0x08F00042** | **Срок действия сертификата истек либо еще не наступил** | | **KCR\_CONVERTERROR** | **0x08F00043** | **Ошибка записи сертификата в структуру X509** | | **KCR\_TSACREATEQUERY** | **0x08F00044** | **Ошибка генерации запроса timestamp** | | **KCR\_CREATEOBJ** | **0x08F00045** | **Ошибка записи OID в ASN1 структуру** | | **KCR\_CREATENONCE** | **0x08F00046** | **Ошибка генерации уникального числа** | | **KCR\_HTTPERROR** | **0x08F00047** | **Ошибка протокола http** | | **KCR\_CADESBES\_FAILED** | **0x08F00048** | **Ошибка проверки расширения CADESBES в CMS** | | **KCR\_CADEST\_FAILED** | **0x08F00049** | **Ошибка проверки подписи токена TSA** | | **KCR\_NOTSATOKEN** | **0x08F0004a** | **В подписи не присутствует метка TSA** | | **KCR\_INVALID\_DIGEST\_LEN** | **0x08F0004b** | **Неправильная длина хэша** | | **KCR\_GENRANDERROR** | **0x08F0004c** | **Ошибка генерации случайного числа** | | **KCR\_SOAPNSERROR** | **0x08F0004d** | **Не найдены заголовки SOAP-сообщений** | | **KCR\_GETPUBKEY** | **0x08F0004e** | **Ошибка экспорта публичного ключа** | | **KCR\_GETCERTINFO** | **0x08F0004f** | **Ошибка получения информации о сертификате** | | **KCR\_FILEREADERROR** | **0x08F00050** | **Ошибка чтения файла** | | **KCR\_CHECKERROR** | **0x08F00051** | **Хэш не совпадает** | | **KCR\_ZIPEXTRACTERR** | **0x08F00052** | **Невозможно открыть архив** | | **KCR\_NOMANIFESTFILE** | **0x08F00053** | **Не найден MANIFEST** | | **KCR\_VERIFY\_TS\_HASH** | **0x08F00054** | **не удалось проверить Хэш подписи TS** | | **KCR\_XADEST\_FAILED** | **0x08F00055** | **XAdES-T: Ошибка проверки подписи** | | **KCR\_OCSP\_RESP\_STAT\_MALFORMEDREQUEST** | **0x08F00056** | **Неправильный запрос** | | **KCR\_OCSP\_RESP\_STAT\_INTERNALERROR** | **0x08F00057** | **Внутренняя ошибка** | | **KCR\_OCSP\_RESP\_STAT\_TRYLATER** | **0x08F00058** | **Попробуйте позже** | | **KCR\_OCSP\_RESP\_STAT\_SIGREQUIRED** | **0x08F00059** | **Должны подписать запрос** | | **KCR\_OCSP\_RESP\_STAT\_UNAUTHORIZED** | **0x08F0005a** | **Запрос не авторизован** | | **KCR\_VERIFY\_ISSUERSERIALV2** | **0x08F0005b** | **не удалось проверить IssuerSerialV2 в XAdES** | | **KCR\_OCSP\_CHECKCERTFROMRESP** | **0x08F0005c** | **Ошибка проверки сертификата OCSP-респондера** | | **KCR\_CRLEXPIRED** | **0x08F0005d** | **CRL-файл просрочен** | | **KCR\_LIBRARYNOTINITIALIZED** | **0x08F00101** | **Библиотека не инициализирована** | | **KCR\_ENGINELOADERR** | **0x08F00200** | **Ошибка подключения (загрузки) модуля (engine)** | | **KCR\_PARAM\_ERROR** | **0x08F00300** | **Некорректные входные данные** | | **KCR\_CERT\_STATUS\_OK** | **0x08F00400** | **Статус сертификата – валидный. (не является ошибкой, делается запись в лог)** | | **KCR\_CERT\_STATUS\_REVOKED** | **0x08F00401** | **Статус сертификата – отозван.** | | **KCR\_CERT\_STATUS\_UNKNOWN** | **0x08F00402** | **Статус сертификата – неизвестен. Например, не удалось установить издателя сертификата.** | |