**СКЗИ «KALKAN-CRYPT (COM)» v2.3.0.0**

**Общее описание СКЗИ и архитектуры построения**

**Константы криптографической библиотеки KalkanCryptCOM**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **KALKANCRYPTCOM\_STORETYPE. Константы, определяющие способ хранения ключей/сертификатов (вид хранилища/носителя).**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значение KALKANCRYPTCOM\_STORETYPE** | | **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 | |
| **KALKANCRYPTCOM\_CERTTYPE. Константы, определяющие принадлежность сертификата.**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значения KALKANCRYPTCOM\_CERTTYPE** | | **Описание** | | **KC\_CERT\_CA** | 0x00000201 | Корневой сертификат УЦ | | **KC\_CERT\_INTERMEDIATE** | 0x00000202 | Сертификат промежуточного УЦ | | **KC\_CERT\_USER** | 0x00000204 | Сертификат пользователя | |
| **KALKANCRYPTCOM\_CERTCODETYPE. Константы, определяющие тип кодировки.**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значения KALKANCRYPTCOM\_CERTCODETYPE** | | **Описание** | | **KC\_CERT\_DER** | 0x00000101 | Кодировка DER | | **KC\_CERT\_PEM** | 0x00000102 | Кодировка PEM | | **KC\_CERT\_B64** | 0x00000104 | Кодировка Base64 | |
| **KALKANCRYPTCOM\_VALIDTYPE. Константы, определяющие тип валидации.**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значения KALKANCRYPTCOM\_VALIDTYPE** | | **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 | |
| **KALKANCRYPTCOM\_CERTPROPID. Константы, определяющие значение поля/расширения в запросе/сертификате.**  **Значения:**   |  |  |  | | --- | --- | --- | | **Значения KALKANCRYPTCOM\_CERTPROPID** | | **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 серификата | | **KC\_CERTPROP\_ISSUER\_DN** | 0x0000081a | Отличительное имя издателя | | **KC\_CERTPROP\_SUBJECT\_DN** | 0x0000081b | Отличительное имя субъекта | | **KC\_CERTPROP\_SIGNATURE\_ALG** | 0x0000081c | Алгоритм подписи | |
| **KALKANCRYPTCOM\_FLAGS. 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 (не используется в текущей версии) | | **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) | |
| **KALKANCRYPTCOM\_ERRORS. Константы, определяющие подробные коды ошибок времени выполнения. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString.**  **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\_LIBRARYNOTINITIALIZED** | 0х08F00101 | Библиотека не инициализирована | | **KCR\_ENGINELOADERR** | 0х08F00200 | Ошибка подключения (загрузки) модуля (engine) | | **KCR\_PARAM\_ERROR** | 0х08F00300 | Некорректные входные данные | | **KCR\_CERT\_STATUS\_OK** | 0х08F00400 | Статус сертификата – валидный. Используется при проверке сертификата по OCSP. (не является ошибкой, делается запись в лог) | | **KCR\_CERT\_STATUS\_REVOKED** | 0х08F00401 | Статус сертификата – отозван. Используется при проверке сертификата по OCSP. | | **KCR\_CERT\_STATUS\_UNKNOWN** | 0х08F00402 | Статус сертификата – неизвестен. Используется при проверке сертификата по OCSP. Например, не удалось установить издателя сертификата. | |

**Описание Функций криптографической библиотеки KalkanCryptCOM**

|  |  |  |  |
| --- | --- | --- | --- |
| **Функция** | **Обзор** | **Описание** | **Возвращаемые значения** |
| **Init().**  Инициализация библиотеки. | HRESULT Init(); | – | При успешном завершении возвращает 0. |
| **GetTokens().**  Обеспечивает получение указателя на строку подключенных устройств типа storage и их количество. | HRESULT GetTokens([in] INT storage, [out] BSTR\* tokens, [out] INT\* tCount); | Параметры:  [in] INT storage — тип хранилища;  [out] BSTR\* tokens — указатель на строку подключенных устройств;  [out] INT\* tCount — количество подключенных устройств. | При успешном завершении возвращает 0, в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **GetCertAliases().**  Обеспечивает получение списка сертификатов в виде строки и их количество. | HRESULT GetCertAliases([out] BSTR\* certAlias, [out] INT\* count); | Параметры:  [out] BSTR\* certAlias — указатель на строку сертификатов;  [out] INT\* count — количество сертификатов. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **LoadKeyStore().**  Загрузка ключей/сертификата их хранилища. | HRESULT LoadKeyStore([in] INT storage, [in] BSTR password, [in] BSTR container, [in] BSTR alias); | Параметры:  [in] INT storage — тип хранилища;  [in] BSTR password — пароль к хранилищу;  [in] BSTR container — название хранилища;  [in] BSTR alias — label (alias) сертификата. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **X509LoadCertificateFromFile().**  Загрузка сертификата из файла для дальнейшей работы с ним. | HRESULT X509LoadCertificateFromFile([in] BSTR certPath, [in] INT certType); | Параметры:  [in] BSTR certPath — путь до файла сертификата;  [in] INT certType) — тип сертификата (см. KalkanCrypt Cert Types). | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **X509LoadCertificateFromBuffer().**  Загрузка сертификата из памяти. | HRESULT X509LoadCertificateFromBuffer([in] BSTR inCert, [in] INT flag); | Параметры:  [in] BSTR inCert — сертификат в виде строки;  [in] INT flag — флаги. Указывается кодировка сертификата (см. Кодировка сертификатов). | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **X509ExportCertificateFromStore().**  Экспорт сертификата из хранилища. | HRESULT X509ExportCertificateFromStore([in] BSTR alias, [in] INT flag, [out] BSTR \*outCert); | Параметры:  [in] BSTR alias — label (alias) сертификата;  [in] INT flag — флаги;  [out] BSTR\* outCert — указатель на начало сертификата. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **X509CertificateGetInfo().**  Обеспечивает получение значений полей/расширений из сертификата. Сертификат должен быть предварительно загружен с помощью одной из функций: LoadKeyStore(), X509LoadCertificateFromFile(),X509LoadCertificateFromBuffer(). | HRESULT X509CertificateGetInfo([in] BSTR inCert, [in] INT propId, [out] BSTR\* outData); | Параметры:  [in] BSTR inCert — сертификат в виде строки;  [in] INT propId — идентификатор полей/расширений сертификата (см. KalkanCrypt CertPropID); [out] BSTR\* outData — указатель на значение указанного поля/расширения. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **X509ValidateCertificate().**  Осуществляет проверку сертификата: проверка срока действия, построение цепочки сертификатов, проверка отозванности по OCSP или CRL. | HRESULT X509ValidateCertificate([in] BSTR inCert, [in] INT validType, [in] BSTR validPath, [in] \_\_int64 checkTime, [out] BSTR\* outInfo); | Параметры:  [in] BSTR inCert — сертификат в виде строки;  [in] INT validType — тип проверки (OCSP/CRL) (см. KalkanCrypt ValidType);  [in] BSTR validPath — путь до CRL или URL OCSP;  [in] \_\_int64 checkTime — дата и время, на момент которого необходимо провести проверку (зарезервировано, в текущей версии не используется);  [out] BSTR\* outInfo — выходная подробная информация о результате проверки. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Если сертификат действителен, то GetLastError вернет 0, иначе, если сертификат недействителен, вернет код ошибки 0x00000017 (23). Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **SignData().**  Подписывает данные. | HRESULT SignData([in] BSTR alias, [in] INT flags, [in] BSTR inData, [out] BSTR\* outSign); | Параметры:  [in] BSTR alias — label (alias) сертификата;  [in] INT flags — флаги. Устанавливают формат входных/выходных данных, тип подписи (см. KalkanCrypt flags);  [in] BSTR inData — входные данные;  [out] BSTR\* outSign — выходные данные (подписи). | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **SignXML().**  Подписывает данные в формате XML. | HRESULT SignXML([in] BSTR alias, [in] INT flags, [in] BSTR signNodeId, [in] BSTR parentSignNode, [in] BSTR parentNameSpace, [in] BSTR inData, [out] BSTR\* outSign); | Параметры:  [in] BSTR alias — label (alias) сертификата;  [in] INT flags — флаги;  [in] BSTR signNodeId — идентификатор тэга, который необходимо подписать. Не указывается, если необходимо подписать все содержимое документа;  [in] BSTR parentSignNode — идентификатор тэга, в который необходимо поместить значение подписи;  [in] BSTR parentNameSpace — пространство имен тэга, в который необходимо поместить значение подписи. Если пространство имен есть, но не будет указано - то тег не найдется;  [in] BSTR inData — входные данные;  [out] BSTR\* outSign — выходные данные (подписи). | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **VerifyData().**  Обеспечивает проверку подписи. | HRESULT VerifyData([in] BSTR alias, [in] INT flags, [in] INT inCertID, [in] BSTR inData, [in] BSTR inSign, [out] BSTR\* outData, [out] BSTR\* outVerifyInfo, [out] BSTR\* outCert); | Параметры:  [in] BSTR alias — label (alias) сертификата;  [in] INT flags — флаги;  [in] INT inCertID — идентификатор (порядковый номер) сертификата (начинается с 0);  [in] BSTR inData — входные данные;  [in] BSTR inSign — подписанные входные данные;  [out] BSTR\* outData — выходные данные;  [out] BSTR\* outVerifyInfo — выходная подробная информация о результате проверки подписи;  [out] BSTR\* outCert — указатель на начало сертификата с подробной информацией. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **VerifyXML().**  Обеспечивает проверку подписи данных в формате XML. | HRESULT VerifyXML([in] BSTR alias, [in] INT flags, [in] BSTR inData, [out] BSTR\* outVerifyInfo); | Параметры:  [in] BSTR alias — label (alias) сертификата;  [in] INT flags — флаги;  [in] BSTR inData — входные данные;  [out] BSTR\* outVerifyInfo — выходная подробная информация о результате проверки подписи. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **GetLastError().**  Обеспечивает получение подробного кода ошибки, возникшей в процессе выполнения функций криптопровайдера KalkanCryptCOM. | HRESULT GetLastError([out, retval] ULONG\* rv); | Параметры:  [out, retval] ULONG\* rv — возвращаемый код последней ошибки. | Возвращает 0, если не найдена ошибка, иначе — значение > 0 (см. KalkanCryptCOM Errors).  При вызове очищается протокол работы криптопровайдера и значение кода последней ошибки. |
| **GetLastErrorString().**  Обеспечивает получение подробного протокола работы функций криптопровайдера KalkanCryptCOM. | HRESULT GetLastErrorString([out] BSTR\* errorString, [out] ULONG\* rv); | Параметры:  [out] BSTR\* errorString — подробный протокол работы функций криптопровайдера;  [out] ULONG\* rv — код последней ошибки. | При успешном завершении возвращает 0,в противном случае – 1.  При вызове очищается протокол работы криптопровайдера и значение кода последней ошибки. |
| **GetSigAlgFromXML().**  Обеспечивает получение алгоритма подписи из XML. | HRESULT GetSigAlgFromXML([in] BSTR inXML, [out] BSTR\* outSigAlg); | Параметры:  [in] BSTR inXML — входные данные в формате XML;  [out] BSTR\* outSigAlg — алгоритм подписи. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **GetCertFromXML().**  Обеспечивает получение сертификата из XML. | HRESULT GetCertFromXML([in] BSTR inXML, [in] INT inSignID, [out] BSTR\* outCert); | Параметры:  [in] BSTR inXML — входные данные в формате XML;  [in] INT inSignID — идентификатор сертификата;  [out] BSTR\* outCert — указатель на начало сертификата. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **XMLFinalize().**  Освобождает память и завершает работу библиотеки с модулями, отвечающие за парсинг, подпись и проверку данных в формате XML. | XMLFinalize(); | – | Не надо вызывать каждый раз при подписи. Можно только один раз после цикла подписания xml файлов. |
| **Finalize().**  Освобождает ресурсы криптопровайдера KalkanCryptCOM и завершает работу библиотеки. | Finalize(); | – | — |
| **HashData().**  Хэширует данные. | HashData([in] BSTR algorithm, [in] INT flags, [in] BSTR inData, [out] BSTR\* outData); | [in] BSTR algorithm –алгоритм хэширования (строка “sha256” или “Gost34311\_95”);  [in] INT flags – флаги;  [in] BSTR inData – входные данные;  [out] BSTR\* outData – выходные хэшированные данные. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **SignHash().**  Подписывает входные хэшированные данные. | SignHash([in] BSTR alias, [in] INT flags, [in] BSTR inHash, [out] BSTR\* outSign). | [in] BSTR alias - label (alias) сертификата;  [in] INT flags – флаги;  [in] BSTR inData – входные хэшированные данные;  [out] BSTR\* outData – выходные данные. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **TSASetUrl().**  Установка адреса сервиса TSA. | HRESULT TSASetUrl([in] BSTR tsaurl); | [in] BSTR tsaurl – адрес сервиса TSA | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString.  Значение по умолчанию http://tsp.pki.gov.kz:80 |
| **TSAGetTimeFromSig()**  Получить время подписи. | HRESULT TSAGetTimeFromSig([in] BSTR inData, [in] INT flags, [in] INT sigId, [out] LONGLONG\* outDateTime); | [in] BSTR inData – входные данные (подпись, в текущей версии только формата CAdES);  [in] INT flags – флаги  [in] INT sigId – идентификатор подписи (в текущей версии не используется)  [out] LONGLONG\* outDateTime – выходные данные, время подписи UTC в Unix формате (отсчет от 01/01/1970) | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **SignDataBytes()**  Подписать бинарные данные. | HRESULT SignDataBytes([in] BSTR alias, [in] INT flags, [in] BYTE\* inData, [in] INT inDataLength, [out] BSTR\* outSign); | [in] BSTR alias - label (alias) сертификата;  [in] INT flags – флаги;  [in] BYTE\* inData - входные данные;  [in] INT inDataLength – длина входных данных;  [out] BSTR\* outSign – выходные данные (подпись); | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |
| **SetProxy()**  Установить настройки прокси-сервера. | HRESULT SetProxy([in] INT flags, [in] BSTR inProxyAddr, [in] BSTR inPort, [in] BSTR inUserName, [in] BSTR inUserPass); | [in] INT flags – флаги;  [in] BSTR inProxyAddr – адрес прокси-сервера;  [in] BSTR inPort – порт;  [in] BSTR inUserName – имя пользователя;  [in] BSTR inUserPass – пароль. | При успешном завершении возвращает 0,в противном случае – 1. Код ошибки можно получить с помощью функции GetLastError. Подробный текст ошибки можно получить с помощью функции GetLastErrorString. |