Описание крипто-сервиса RRIC_CRYPTO_SERVICE

Общая информация

Крипто-сервис RRIC_CRYPTO_SERVICE является составной частью АИС «КРЭДО», разработанного ГУП «Республиканский Расчетный Информационный Центр», и предназначен для осуществления функций по созданию XML-контейнеров электронных документов, управлению электронными документами и электронно-цифровыми подписями.

В крипто-сервисе реализован полный перечень крипто-функций, позволяющих добавлять ЭЦП и проверять их подлинность, зашифровывать и расшифровывать XML-контейнеры электронных документов.

Крипто-сервис реализован как настольное приложение Windows, внутри которого задействован локальный веб-сервис. После запуска приложения, оно инициализирует http-прослушиватель (HttpListener), который осуществляет перехват POST-пакетов по следующим адресам http://localhost:57336 и http://127.0.0.1:57336. Для работы приложения необходимо, чтобы на хост-компьютере был установлен .Net Framework 4.6.

Для взаимодействия с крипто-сервисом из сторонних приложений или веб-браузеров лучше всего использовать механизмы COM-взаимодействия. В частности, можно использовать COM-объекты "Msxml2.XMLHTTP", "Microsoft.XMLHTTP" или в современных браузерах класс XMLHttpRequest.

Функции

CreateContainer

Создание нового XML-контейнера электронных документов

string CreateContainer()

Возвращает base64 строку, содержащую имя созданного XML-контейнера.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

LoadContainer

Загрузка XML-контейнера электронных документов из файла

string LoadContainer()

При вызове функции появляется диалоговое окно выбора файла.

Возвращает base64 строку, содержащую имя загруженного XML-контейнера.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

UploadContainer

Загрузка XML-контейнера электронных документов из base64-строки данных

string UploadContainer(string cntData64, string cntName64)

cntData64 – строка base64. Данные XML-контейнера.

cntName64 – строка base64. Имя XML-контейнера (не обязательный параметр).

Возвращает base64 строку, содержащую имя загруженного XML-контейнера или значение «98989898» если XML-контейнер с таким именем уже загружен в хранилище XML-контейнеров.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetContainers

Получение информации обо всех XML-контейнерах электронных документов, с которыми ведётся работа в данный момент

string GetContainers()

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root><cnt name="имя XML-контейнера" status="статус XML-контейнера" /></root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

DeleteContainer

Удаление XML-контейнера электронных документов

string DeleteContainer(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetContainerContent

Получение текстового содержимого XML-контейнера электронных документов

string GetContainerContent(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с содержимым XML-контейнера:

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

SetDocumentInfo

Добавление/редактирование общей информации об XML-контейнере(ах) электронных документов

string SetDocumentInfo(string cntName64, string docInfo64)

cntName64 – строка base64. Имя XML-контейнера.

docInfo64 – строка base64. XML-данные общей информации для записи.

Возвращает base64 строку с фразой, содержащую слово «ОК».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetDocumentInfo

Извлечение общей информации об XML-контейнере(ах) электронных документов

string GetDocumentInfo(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку, содержащую XML-данные общей информации.

В случае ошибки возвращает фразу, содержащую слово «Ошибка».

SetDocInfoParameter

Добавление элемента описания XML-контейнера электронных документов

string SetDocInfoParameter(string cntName64, string parName64, string parValue64)

cntName64 – строка base64. Имя XML-контейнера.

parName64 – строка base64. Имя параметра.

parValue64 – строка base64. Значение параметра.

Возвращает base64 строку с фразой, содержащую слово «ОК».

В случае ошибки возвращает фразу, содержащую слово «Ошибка».

GetDocInfoParameterValue

Получение эелемента описания XML-контейнера электронных документов

string GetDocInfoParameterValue(string cntName64, string parName64)

cntName64 – строка base64. Имя XML-контейнера.

parName64 – строка base64. Имя параметра.

Возвращает base64 строку со значением параметра. В случае ошибки возвращает фразу, содержащую слово «Ошибка».

SetDocInfoLogo

Добавление логотипа организации в XML-контейнер электронных документов

string SetDocInfoLogo(string cntName64, string logo_image64)

cntName64 – строка base64. Имя XML-контейнера.

logo_image64 – строка base64. Имя параметра.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает фразу, содержащую слово «Ошибка».

AddSigner

Добавление подписанта в XML-контейнер электронных документов

string AddSigner(string cntName64, string position64, string fio64)

cntName64 – строка base64. Имя XML-контейнера.

position64 – строка base64. Должность подписанта.

fio64 - строка base64. ФИО подписанта.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

RemoveSigner

Удаление подписанта из XML-контейнера электронных документов

string RemoveSigner(string cntName64, int index)

cntName64 – строка base64. Имя XML-контейнера.

index – индекс записи с данными подписанта.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

RemoveSigners

Удаление всех подписантов из XML-контейнера электронных документов

string RemoveSigners(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetSigners

Извлечение информации обо всех подписантах XML-контейнера электронных документов

string GetSigners(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root><signaturestextinfo><post>Должность подписанта</post><fio>ФИО подписанта</fio></signaturestextinfo></root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

AddRecipient

Добавление получателя XML-контейнера электронных документов

string AddRecipient(string cntName64, string org64, string branch64, string pos64, string fio64)

cntName64 – строка base64. Имя XML-контейнера.

org64 - строка base64. Наименование организации получателя.

branch64 - строка base64. Наименования подразделения организации получателя.

pos64 – строка base64. Должность получателя.

fio64 - строка base64. ФИО получателя.

Возвращает base64 строку с фразой, содержащую слово «ОК».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

RemoveRecipient

Удаление получателя XML-контейнера электронных документов

string RemoveRecipient(string cntName64, int index)

cntName64 – строка base64. Имя XML-контейнера.

index – индекс записи с данными получателя.

Возвращает base64 строку с фразой, содержащую слово «ОК».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

RemoveRecipients

Удаление всех получателей XML-контейнера электронных документов

string RemoveRecipients(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с фразой, содержащую слово «ОК».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetRecipients

Извлечение информации обо всех получателях XML-контейнера электронных документов

string GetRecipients(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root><destination><org>Организация получателя</org><branch>Подразделение
организации</branch><post>Должность получателя</post><fio>ФИО
получателя</fio></destination></root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

AddRawData

Добавление «голых» данных в XML-контейнер электронных документов

string AddRawData(string cntName64, string rawData64)

cntName64 – строка base64. Имя XML-контейнера.

rawData64 – строка base64. Набор «голых» данных.

Возвращает base64 строку с фразой, содержащую слово «ОК».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetRawData

Извлечение «голых» данных из XML-контейнера электронных документов

string GetRawData(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с содержимым «голых» данных.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

RemoveRawData

Удаление «голых» данных из XML-контейнера электронных документов

string RemoveRawData(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с фразой, содержащую слово «ОК».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

AddDocument

Добавление вложения в XML-контейнер электронных документов

string AddDocument(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

При вызове функции появляется диалоговое окно выбора добавляемого документа.

Возвращает base64 строку с наименованием добавленного документа.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

AddDocumentRaw

Добавление вложения в XML-контейнер электронных документов

string AddDocument(string cntName64, string docName64, string docData64)

cntName64 – строка base64. Имя XML-контейнера.

docName64 – строка base64. Имя добавляемого документа.

docData64 – строка base64. Содержимое добавляемого документа.

Возвращает base64 строку с наименованием добавленного документа.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

RemoveDocument

Удаление вложения из XML-контейнера электронных документов

string RemoveDocument(string cntName64, string docName64)

cntName64 – строка base64. Имя XML-контейнера.

docName64 – строка base64. Имя электронного документа.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

RemoveDocuments

Удаление всех вложений из XML-контейнера электронных документов

string RemoveDocuments(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetDocument

Извлечение содержимого вложения из XML-контейнера электронных документов

string RemoveDocument(string cntName64, string docName64)

cntName64 – строка base64. Имя XML-контейнера.

docName64 – строка base64. Имя электронного документа.

Возвращает base64 строку с содержимым электронного документа.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

SaveDocument

Извлечение вложения из XML-контейнера электронных документов и сохранение его в указанное место на диске

string SaveDocument(string cntName64, string docName64)

cntName64 – строка base64. Имя XML-контейнера.

docName64 – строка base64. Имя электронного документа.

При вызове функции появляется диалоговое окно сохранения файла.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

SignDocument

Подписание XML-контейнера электронных документов электронно-цифровой подписью

Возможен вызов функции четырьмя различными способами с указанием разного набора входных параметров.

Способ 1 – для подписания используется сертификат, установленный в хранилище сертификатов пользователя.

string SignDocument(string cntName64, string certFlag, string certOptions64, string tsaService64)

cntName64 – строка base64. Имя XML-контейнера.

certFlag – признак местонахождения сертификата безопасности (0 – сертификат в хранилище сертификатов).

certOptions64 - строка base64. XML-представление структуры certOptions

tsaService64 – строка base64 с адресом сервера штампов времени.

Способ 2 – для подписания используется файл сертификата в формате PKCS #12 (файлы с расширением .pfx). При вызове функции последовательно появляются диалоговые окна выбора файла сертификата и ввода пароля.

string SignDocument(string cntName64, string certFlag, string tsaService64)

cntName64 – строка base64. Имя XML-контейнера.

certFlag – признак местонахождения сертификата безопасности (1 – сертификат в файле на носителе информации).

tsaService64 – строка base64 с адресом сервера штампов времени.

Способ 3 – для подписания используется считанное содержимое сертификата в формате PKCS #12 (из файла с расширением .pfx) и указывается пароль сертификата.

string SignDocument(string cntName64, string certFlag, string certData64, string certPass64, string tsaService64)

cntName64 – строка base64. Имя XML-контейнера.

certFlag – признак местонахождения сертификата безопасности (2 – используется содержимое сертификата).

certData64 – строка base64 содержимого сертификата.

certPass64 – строка base64 пароля (ПИН-кода) сертификата.

tsaService64 – строка base64 с адресом сервера штампов времени.

Способ 4 – для подписания используется сертификат, установленный в хранилище сертификатов пользователя, имеющий указанный отпечаток.

string SignDocument(string cntName64, string certFlag, string thumbPrint64, string tsaService64)

cntName64 – строка base64. Имя XML-контейнера.

certFlag – признак местонахождения сертификата безопасности (3 – используется отпечаток сертификата).

thumbPrint64 – строка base64 с отпечатком сертификата.

tsaService64 – строка base64 с адресом сервера штампов времени.

Возвращает base64 строку с идентификатором подписи.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

SignSignature

Подписание электронно-цифровой подписи – визирование

Возможен вызов функции четырьмя различными способами с указанием разного набора входных параметров.

Способ 1 – для подписания используется сертификат, установленный в хранилище сертификатов пользователя.

string SignSignature(string cntName64, string sigId64, string certFlag, string certOptions64, string tsaService64)

cntName64 – строка base64. Имя XML-контейнера..

sigId64 - строка base64. ID заверяемой ЭЦП.

certFlag – признак местонахождения сертификата безопасности (0 – сертификат в хранилище сертификатов).

certOptions64 - строка base64. XML-представление структуры certOptions

tsaService64 – строка base64 с адресом сервера штампов времени.

Способ 2 – для подписания используется файл сертификата в формате PKCS #12 (файлы с расширением .pfx). При вызове функции последовательно появляются диалоговые окна выбора файла сертификата и ввода пароля.

string SignSignature(string cntName64, string sigId64, string certFlag, string tsaService64)

cntName64 – строка base64. Имя XML-контейнера.

sigId64 - строка base64. ID заверяемой ЭЦП.

certFlag – признак местонахождения сертификата безопасности (1 – сертификат в файле на носителе информации).

tsaService64 – строка base64 с адресом сервера штампов времени.

Способ 3 – для подписания используется считанное содержимое сертификата в формате PKCS #12 (из файла с расширением .pfx) и указывается пароль сертификата.

string SignSignature (string cntName64, string sigId64, string certFlag, string certData64, string certPass64, string tsaService64)

cntName64 – строка base64. Имя XML-контейнера.

sigId64 - строка base64. ID заверяемой ЭЦП.

certFlag – признак местонахождения сертификата безопасности (2 – используется содержимое сертификата).

certData64 – строка base64 содержимого сертификата.

certPass64 – строка base64 пароля (ПИН-кода) сертификата.

tsaService64 – строка base64 с адресом сервера штампов времени.

Способ 4 – для подписания используется сертификат, установленный в хранилище сертификатов пользователя, имеющий указанный отпечаток.

string SignSignature (string cntName64, string sigId64, string certFlag, string thumbPrint64, string tsaService64)

cntName64 – строка base64. Имя XML-контейнера.

sigId64 - строка base64. ID заверяемой ЭЦП.

certFlag – признак местонахождения сертификата безопасности (3 – используется отпечаток сертификата).

thumbPrint64 – строка base64 с отпечатком сертификата.

tsaService64 – строка base64 с адресом сервера штампов времени.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

RemoveSignature

Удаление электронно-цифровой подписи XML-контейнера электронных документов

Возможен вызов функции тремя различными способами с указанием разного набора входных параметров.

Способ 1 – для удаления необходимо указать сертификат, установленный в хранилище сертификатов пользователя.

string RemoveSignature(string cntName64, string sigId64, string certFlag, string certOptions64)

cntName64 – строка base64. Имя XML-контейнера.

sigId64 – строка base64. ID электронно-цифровой подписи.

certFlag – признак местонахождения сертификата безопасности (0 – сертификат в хранилище сертификатов).

certOptions64 - строка base64. XML-представление структуры certOptions

Способ 2 – для удаления необходимо выбрать сертификат в формате PKCS #12 (файлы с расширением .pfx). При вызове функции последовательно появляются диалоговые окна выбора файла сертификата и ввода пароля.

string RemoveSignature(string cntName64, string sigId64, string certFlag)

cntName64 – строка base64. Имя XML-контейнера.

sigId64 – строка base64. ID электронно-цифровой подписи.

certFlag – признак местонахождения сертификата безопасности (1 – сертификат в файле на носителе информации).

Способ 3 – для удаления используется считанное содержимое сертификата в формате PKCS #12 (из файла с расширением .pfx) и указывается пароль сертификата.

string RemoveSignature(string cntName64, string sigId64, string certFlag, string certData64, string certPass64)

cntName64 – строка base64. Имя XML-контейнера.

sigId64 – строка base64. ID электронно-цифровой подписи.

certFlag – признак местонахождения сертификата безопасности (1 – сертификат в файле на носителе информации).

certData64 – строка base64 содержимого сертификата.

certPass64 – строка base64 пароля (ПИН-кода) сертификата.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

Validate

Проверка всех электронно-цифровых подписей, добавленных в XML-контейнер электронных документов - валидация

string Validate(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

В случае положительной проверки возвращает base64 строку с xml-структурой, содержащей данные подписей и их проверки.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

ValidateSignature

Проверка заданной электронно-цифровой подписи, добавленной в XML-контейнер электронных документов - валидация

string Validate(string cntName64, string sigId64)

cntName64 – строка base64. Имя XML-контейнера.

sigId64 – строка base64. ID электронно-цифровой подписи.

В случае положительной проверки возвращает base64 строку с фразой, содержащую слово «Valid».

В случае отрицательной проверки возвращает base64 строку с фразой, содержащую слово «Invalid».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

EncryptContainer

Зашифрование XML-контейнера электронных документов

Возможен вызов функции тремя различными способами с указанием разного набора входных параметров.

Способ 1 – для зашифрования необходимо указать сертификат, установленный в хранилище сертификатов пользователя.

string EncryptContainer(string cntName64, string certFlag, string certOptions64)

cntName64 – строка base64. Имя XML-контейнера.

certFlag – признак местонахождения сертификата безопасности (0 – сертификат в хранилище сертификатов).)

certOptions64 - строка base64. XML-представление структуры certOptions

Способ 2 – для зашифрования используется файл сертификата в формате DER (файлы с расширением .cer). При вызове функции появляется диалоговое окно выбора файла сертификата.

string EncryptContainer(string cntName64, string certFlag)

cntName64 – строка base64. Имя XML-контейнера.

certFlag – признак местонахождения сертификата безопасности (1 – сертификат в файле на носителе информации).

Способ 3 – для зашифрования используется содержимое файла сертификата в формате DER (файлы с расширением .cer).

string EncryptContainer(string cntName64, string certFlag, string certRaw64)

cntName64 – строка base64. Имя XML-контейнера.

certFlag – признак местонахождения сертификата безопасности (2 – сертификат в raw-формате).

certRaw64 – строка base64. Строка с описанием массива сертификатов безопасности следующего вида:

```
<root><cert data="base64 строка байтового массива сертификата" /></root>
```

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

DecryptContainer

Расшифрование XML-контейнера электронных документов

Возможен вызов функции двумя различными способами с указанием разного набора входных параметров.

Способ 1 – для расшифрования используется сертификат в формате PKCS #12 (с приватным ключом), установленный в хранилище сертификатов пользователя и принадлежащий получателю документа.

string DecryptContainer(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Способ 2 – для расшифрования используется считанное содержимое сертификата в формате PKCS #12 (из файла с расширением .pfx) и указывается пароль сертификата.

string DecryptContainer(string cntName64, string certData64, string certPass64)

cntName64 – строка base64. Имя XML-контейнера.

certData64 – строка base64 содержимого сертификата.

certPass64 – строка base64 пароля (ПИН-кода) сертификата.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

Compress

Архивирование XML-контейнера электронных документов

Необходимо использовать перед записью XML-контейнера в базу данных АИС «КРЭДО».

string Compress(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

Decompress

Разархивирование XML-контейнера электронных документов

Необходимо использовать после извлечения XML-контейнера из базы данных АИС «КРЭДО».

string DecompressFile(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetDocCount

Получение количества вложений XML-контейнера электронных документов

string GetDocCount(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку количества электронных документов в XML-контейнере.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetDocList

Получение списка вложений XML-контейнера электронных документов

string GetDocList(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<docs><doc name="имя документа" size="размер документа" /></docs>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetSigCount

Получение количества электронно-цифровых подписей XML-контейнера электронных документов

string GetSigCount(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку количества ЭЦП в XML-контейнере.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetSigList

Получение списка электронно-цифровых подписей XML-контейнера электронных документов

string GetSigList(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root><signature id="Идентификатор подписи" sign_type="Тип подписи"
child_id="Идентификатор дочерней подписи" digest="Хэш подписи" createtime="Дата создания"
timestamp="Штамп сервера времени" hash_algo="Алгоритм хэширования" hash_algo_oid="OID
алгоритма хэширования" sig_algo="Алгоритм подписи" sig_algo_oid="OID алгоритма подписи"
cert="Сертификат подписи" /></root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

IsEncrypted

Проверка XML-контейнера электронных документов, является ли он зашифрованным

string IsEncrypted(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает возвращает base64 строку со значением «0», если XML-контейнер не зашифрован, или base64 строку со значением «1», если XML-контейнер зашифрован.

GetDocSigCount

Проверка количества ЭЦП во вложении XML-контейнера электронных документов

string GetDocSigCount(string cntName64, string docName64)

cntName64 – строка base64. Имя XML-контейнера.

docName64 – строка base64. Имя файла вложения.

Возвращает base64 строку количества ЭЦП в файле вложения XML-контейнера.

GetDocSigners

Возвращает список подписантов файла вложения XML-контейнера электронных документов

string GetDocSigners(string cntName64, string docName64)

cntName64 – строка base64. Имя XML-контейнера.

docName64 – строка base64. Имя файла вложения.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root><signer>Данные подписанта</signer></root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetStatus

Получение признака текущего состояния XML-контейнера электронных документов

string GetStatus(string cntName64)

cntName64 – строка base64. Имя XML-контейнера.

Возвращает base64 строку с текущим статусом XML-контейнера: NotDefined (не определенный статус), Clean (контейнер без документов и подписей), Filled (в контейнере присутствуют документы), Signed (в контейнере есть электронно-цифровые подписи), Crypted (контейнер зашифрован), Compressed (контейнер сжат).

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

ShowDialog

Вызов диалогового окна

string ShowDialog(string dlgOptions64)

dlgOptions64 - строка base64. XML-представление структуры dlgOptions

ClearAll

Очистка временного хранилища XML-контейнеров

string ClearAll()

Возвращает base64 строку с фразой, содержащую слово «OK».

GetCertificate

Поиск и извлечение содержимого пользовательского сертификата безопасности

string GetCertificate(string certFlag, string certOptions64)

certFlag – признак местонахождения сертификата безопасности (0 – сертификат в хранилище сертификатов)

certOptions64 - строка base64. XML-представление структуры certOptions

string GetCertificate (string certFlag)

certFlag – признак местонахождения сертификата безопасности (1 – сертификат в файле на носителе информации).

string GetCertificate (string cntName64, string sigId64)

certFlag – признак местонахождения сертификата безопасности (2 – сертификат в подписи XML-контейнера).

cntName64 – строка base64. Имя XML-контейнера..

sigId64 - строка base64. ID заверяемой ЭЦП.

Возвращает base64 строку с содержимым сертификата безопасности.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetStampInfo

Извлечение информации из штампа времени

string GetStampInfo(string timeStamp64)

timeStamp64 - строка base64. Содержимое токена штампа времени.

string GetStampInfo(string cntName64, string sigId64)

cntName64 – строка base64. Имя XML-контейнера..

sigId64 - строка base64. ID заверяемой ЭЦП.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root><timestamp serial_number="серийный номер штампа" created="дата и время"
data_hash="хэш заверенных штампом времени данных"><TSA issuer_name="имя заверителя
сертификата сервера штампов времени" issuer_serial="серийный номер заверителя сертификата
сервера штампов времени" tsa_name="имя сертификата сервера штампов времени"
tsa_from_date="действителен с" tsa_to_date="действителен до"/></timestamp></root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

GetStampDate

Извлечение значения даты и времени из штампа времени

string GetStampDate(string timeStamp64)

timeStamp64 - строка base64. Содержимое токена штампа времени.

Возвращает строку base64, содержащую значение даты и времени.

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

CertVerify

Проверка сертификата подписи

string StampVerify(string cntData64, string sigId64)

cntData64 – строка base64. Данные XML-контейнера.

sigId64 - строка base64. Идентификатор подписи.

При положительной проверке возвращает base64 строку с фразой «Valid».

При отрицательной проверке возвращает base64 строку с фразой «Invalid».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

CertVerify2

Проверка сертификата

string CertVerify2(string certData64, string certPass64)

certData64 – строка base64. Содержимое файла сертификата.

certPass64 - строка base64. Пароль (ПИН-код) сертификата.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root><error>Описание ошибки сертификата</error></root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

CertView

Отображение диалогового окна свойств сертификата

string CertView(string certData64, string certPass64)

certData64 – строка base64. Содержимое файла сертификата.

certPass64 - строка base64. Пароль (ПИН-код) сертификата.

Возвращает base64 строку с фразой, содержащую слово «OK».

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

SignatureInfo

Данные электронно-цифровой подписи

string SignatureInfo(string cntName64, string sigId64)

cntName64 – строка base64. Имя XML-контейнера..

sigId64 - строка base64. ID заверяемой ЭЦП.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root>
        <!-- информация о подписи -->
        <signature>
                <id>идентификатор подписи</id>
                <sign_type>тип подписи</sign_type>
                <sign_value>подпись в base64</sign_value>
                <hasstamp>флаг наличия штампа времени (true/false)</hasstamp>
                <hash_algo>алгоритм хэширования</hash_algo>
                <hash_algo_oid>OID алгоритма хэширования</hash_algo_oid>
                <sig_algo>алгоритм подписи</sig_algo>
                <sig_algo_oid>OID алгоритма подписи</sig_algo_oid>
```

```
                <!-- информация о сертификате подписи -->
                <certificate>
                        <version>версия</version>
                        <serial>серийный номер</serial>
                        <subject>кому выдан</subject>
                        <validity_from>действует с</validity_from>
                        <validity_till>действует по</validity_till>
                        <issuer>издатель</issuer>
                </certificate>
        </signature>
        <!-- заверяющие подписи -->
        <counter_signatures>
                <counter_signature
                        id="идентификатор подписи"
                        serial="серийный номер сертификата"
                        thumbprint="отпечаток сертификата"
                        subject="принадлежность сертификата"/>
                ...
        </counter_signatures>
</root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

CertificateInfo

Данные сертификата безопасности

string CertificateInfo(string certData64, string certPass64)

certData64 – строка base64. Данные сертификата в RAW формате.

certPass64 - строка base64. Пароль (ПИН-код) сертификата.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root>
        <version>версия</version>
        <serial>серийный номер</serial>
        <thumbprint>отпечаток</thumbprint>
        <subject>кому выдан</subject>
        <validity_from>действует с</validity_from>
        <validity_till>действует по</validity_till>
        <issuer>издатель</issuer>
        <key_usage>Ключи использования сертификата</key_usage>
        <clientId>идентификатор владельца в ЦС АПБ</clientId>
        <clientMvdId>идентификатор владельца в БД МВД</clientMvdId>
        <clientBirthDate>дата рождения владельца в БД МВД</clientBirthDate>
        <clientOrgRegNum>регистрационный номер ЕГРЮЛ организации владельца</clientOrgRegNum>
        <clientOrgFiscalCode>фискальный код организации владельца</clientOrgFiscalCode>
</root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

CertificateInfo2

Данные сертификата безопасности

string CertificateInfo2(string cntName64, string sigId64)

cntData64 – строка base64. Данные XML-контейнера.

sigId64 - строка base64. Идентификатор подписи.

Возвращает base64 строку, содержащую xml со следующей структурой:

```
<root>
        <version>версия</version>
        <serial>серийный номер</serial>
        <thumbprint>отпечаток</thumbprint>
        <subject>кому выдан</subject>
        <validity_from>действует с</validity_from>
        <validity_till>действует по</validity_till>
        <issuer>издатель</issuer>
        <key_usage>Ключи использования сертификата</key_usage>
        <clientId>идентификатор владельца в ЦС АПБ</clientId>
        <clientMvdId>идентификатор владельца в БД МВД</clientMvdId>
        <clientBirthDate>дата рождения владельца в БД МВД</clientBirthDate>
        <clientOrgRegNum>регистрационный номер ЕГРЮЛ организации владельца</clientOrgRegNum>
        <clientOrgFiscalCode>фискальный код организации владельца</clientOrgFiscalCode>
</root>
```

В случае ошибки возвращает base64 строку с фразой, содержащую слово «Ошибка».

Base64Encode

Кодирование текста в строку base64

string Base64Encode(string data)

data – строка, подлежащая кодированию в base64.

Возвращает base64 строку.

В случае ошибки возвращает пустую строку.

Base64Decode

Декодирование текста из строки base64

string Base64Decode(string data64)

data64 – base64 строка, подлежащая декодированию.

Возвращает строку декодированного текста.

В случае ошибки возвращает пустую строку.

Структуры

dlgOptions

Структура элементов диалоговых окон открытия и сохранения файлов

```
struct dlgOptions
{
  string Type;
  string Title;
  string Filter;
  int FilterIndex;
  string InitDir;
  bool Multy;
  bool RestoreDir;
  bool CheckFileExist;
  bool CheckPathExist;
  string DefaultExt;
  string FileName;
  bool BinaryFile;}
```

Type – тип диалогового окна (OpenFileDialog (диалоговое окно открытия файла), SaveFileDialog(диалоговое окно сохранения файла), InnerDialog (диалоговое окно ввода пароля), MessageDialog (диалоговое окно сообщений), AnswerDialog (диалоговое окно подтверждения).
Title – заголовок диалогового окна.
Filter – список типов и расширений файлов.
FilterIndex – индекс выбранного элемента списка Filter.
InitDir – каталог по умолчанию.
Multy – признак возможности множественного выбора.
RestoreDir – признак возможности сохранения ранее выбранного каталога.
CheckFileExist – встроенная проверка на наличие файла.
CheckPathExist – встроенная проверка на наличие каталога.
DefaultExt – расширение файла по умолчанию.
FileName – имя файла (действительно только для SaveFileDialog).
BinaryFile – признак типа файла (True – двоичный, False – текстовый).

certOptions

Структура данных о хранилище сертификатов и диалогового окна выбора сертификата

```
struct certOptions
{
  string storeLocation;
  string storeName;
  int flag;
  int multy;}
```

storeLocation – хранилище сертификатов (LocalMachine или CurrentUser).
storeName – каталог сертификатов (My, TrustedPeople, AddressBook и т.п.)
flag – комбинация значений перечисления OpenFlags.
multy – признак возможности множественного выбора сертификатов в системном диалоговом окне выбора сертификатов.

Перечисления

OpenFlags

IncludeArchived	8	Open the X.509 certificate store and include archived certificates.
MaxAllowed	2	Open the X.509 certificate store for the highest access allowed.
OpenExistingOnly	4	Opens only existing stores; if no store exists, the Open(OpenFlags) method will not create a new store.
ReadOnly	0	Open the X.509 certificate store for reading only.
ReadWrite	1	Open the X.509 certificate store for both reading and writing.

CntStat

NotDefined	0	Не определено
Clean	1	Без документов и подписей
Filled	2	Есть документы
Signed	3	Есть подписи
Crypted	4	Зашифрован
Compressed	5	Сжат

HashAlgo

SHA256	0
SHA384	1
SHA512	2

Примеры

1. Пример вызова функций крипто-сервиса на языке JavaScript

```
// Создание документа
var d = CreateCnt();
console.log(b64Decode(d));
// Заполнение документа
var res = FillCnt(d);
// Вывод содержимого документа
var content = GetCnt(d);
console.log(b64Decode(content));

function CreateCnt(cntName) {
        return RequestSrv("proc=CreateContainer");
}

function FillCnt(cntName) {
  // Добавление наименования организации
  RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
    "&parName64=" + b64Encode("nameru") +
    "&parValue64=" + b64Encode("ООО Ивушка"));
  // Добавление наименования вида документа
  RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
    "&parName64=" + b64Encode("nameviewdoc") +
    "&parValue64=" + b64Encode("Письмо"));
   // Добавление почтового адреса, номеров телефона и факса, адреса эл.почты
   RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
     "&parName64=" + b64Encode("referencedataorg/postaladdress") +
     "&parValue64=" + b64Encode("г.Каменка, ул.Ленина, д.2"));
   RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
     "&parName64=" + b64Encode("referencedataorg/phonenumber") +
     "&parValue64=" + b64Encode("216-12345"));
   RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
     "&parName64=" + b64Encode("referencedataorg/faxnumber") +
     "&parValue64=" + b64Encode("216-56879"));
   RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
     "&parName64=" + b64Encode("referencedataorg/emailaddress") +
     "&parValue64=" + b64Encode("ivushka@idknet.com"));
   // Добавление номера и даты исходящего документа
   RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
     "&parName64=" + b64Encode("reg/datareg") +
     "&parValue64=" + b64Encode("15.01.2021"));
   RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
     "&parName64=" + b64Encode("reg/regnumber") +
     "&parValue64=" + b64Encode("12/23-3434"));
   // Добавление данных получателя (адресата) документа
   RequestSrv("proc=AddRecipient&cnt=" + cntName +
     "&org64=" + b64Encode("ООО Колокольчик") +
     "&branch64=" +
     "&pos64=" + b64Encode("Директору") +
     "&fio64=" + b64Encode("Зыкиной А.А."));
   // Добавление текста документа
   RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
     "&parName64=" + b64Encode("content") +
     "&parValue64=" + b64Encode("<p>Это <span style='color:red'>первый параграф</span> текста
документа, содержащий какую-то информацию.</p><p>Это <b>Второй параграф</b> текста
документа</p>"));
   // Добавление данных руководителей и исполнителя организации-отправителя
   RequestSrv("proc=AddSigner&cnt=" + cntName +
     "&position64=" + b64Encode("Директор") +
     "&fio64=" + b64Encode("Артамонов И.А."));
   RequestSrv("proc=AddSigner&cnt=" + cntName +
     "&position64=" + b64Encode("Зам. директора") +
     "&fio64=" + b64Encode("Васильев Г.Г."));
   RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
     "&parName64=" + b64Encode("executor/executorname") +
     "&parValue64=" + b64Encode("О.А.Васильева"));
   RequestSrv("proc=SetDocInfoParameter&cnt=" + cntName +
     "&parName64=" + b64Encode("executor/executorphone") +
     "&parValue64=" + b64Encode("216-55555"));
   // Добавление электронно-цифровой подписи
   var certOptions =
"<root><StoreLocation>CurrentUser</StoreLocation><StoreName>My</StoreName><Flag>0</Flag><Multy>
0</Multy></root>";
   var sign_id = RequestSrv("proc=SignDocument&cnt=" + cntName +
     "&certFlag=0" +
     "&certOptions64=" + b64Encode(certOptions) +
     "&tsaService64=" + b64Encode("http://ca.agroprombank.com/tsa"));
   console.log("Signature ID: " + b64Decode(sign_id));
```

```
   // Проверка ЭЦП
   var res = RequestSrv("proc=ValidateSignature&cnt=" + cntName +
     "&sigId64=" + sign_id);
   console.log("Signature is: " + b64Decode(res));
}

function GetCnt(cntName) {
   return RequestSrv("proc=GetContainerContent&cnt=" + cntName);
}

function RequestSrv(command) {
   var url = "http://localhost:57336";
   var RetVal = "";
   try {
     var objHttp = getXmlHttp();
     objHttp.open("POST", url, false);
     objHttp.onreadystatechange = handleReadyStateChange;
     objHttp.setRequestHeader("Content-Type", "text/plain");
     objHttp.send(command);

     function handleReadyStateChange() {
        if(objHttp.readyState == 4) {
           if(objHttp.status == 200) {
              RetVal = objHttp.responseText;
           }
        }
     }
   }
   catch (e) {
     console.log("Локальный крипто-сервер не запущен");
   }
   return RetVal;
}

function getXmlHttp() {
   var xmlhttp=false;
   try {
     xmlhttp=new XMLHttpRequest();
   }
   catch(e) {
     try {
        xmlhttp= new ActiveXObject("Microsoft.XMLHTTP");
     }
     catch(e) {
        try {
           req = new ActiveXObject("Msxml2.XMLHTTP");
        }
        catch(e1) {
           xmlhttp=false;
        }
     }
   }
   return xmlhttp;
}

function b64Encode(str) {
    return RequestSrv("proc=Base64Encode&data="+str);
}

function b64Decode(str) {
    return RequestSrv("proc=Base64Decode&data="+str);
}
```