ООО «ФИРМА «ИНФОКРИПТ»

«Криптографические компоненты» (ICCryptoComponents 2.0)

Спецификация библиотеки

г. Москва 2025 год

Оглавление

Введение

Программный продукт ICCryptoComponents 2.0 (ICCC) является плагином для веб-браузеров семейства Chromium. Выполняемый функционал: внедрение ЭП в заранее созданный объект CMS (PKCS#7), формирование ЭП в формате CMS (присоединенная и отсоединенная ЭП). Используемое криптографическое ядро — сертифицированное СКЗИ «Бикрипт 5.0».

Программный продукт ICCryptoComponents 2.0 обеспечивает формирование ЭП в соответствии с ГОСТ Р34.10-2001 и ГОСТ Р34.10-2012 и хеширование данных в соответствии с ГОСТ Р34.11-94 и ГОСТ Р34.11-2012.

Программный продукт представляет собой исполняемый файл iccryptocomponents.exe и набор динамически загружаемых библиотек (dll), работающих в операционной системе семейства Windows.

Установка плагина ICCC 2.0

MS Windows

Установка плагина ICCC 2.0 осуществляется путем запуска установочного пакета I3C2Setup_64.msi. Предварительно необходимо установить расширение для браузера BiCrypt (инструкцию по установке нужно смотреть в описании указанного программного продукта).

Установщик распакует необходимые файлы в штатный каталог установки:
[Program Files]\InfoCrypt\BrowserPlugin\c++.

MacOS

Установка плагина ICCC 2.0 осуществляется путем запуска установочного пакета ICCryptoComponentsChrome.pkg (для браузера Chrome) или ICCryptoComponentsChromium.pkg (для браузера семейства Chromium).

Методы ICCC 2.0

1. Метод загрузки секретного ключа на ТМ носителе.

```
ICCC_LoadPrivateKeyTm()
```

Описание
Метод делает возможным веб-приложению, использующему ICCC, "отрисовать" окно в браузере с предложением приложить ТМ в визуальном стиле браузера/используемой АБС. Также, метод позволит АБС (при необходимости) применить некую логику, предшествующую выбору ключевого носителя.
Функционально метод считывает секретный ключ с носителя ТМ. Вызов метода обязателен перед вызовами методов, использующих секретный ключ. Информация о секретном ключе помещается в контекст СКЗИ Бикрипт 5.0 и используется им в дальнейшем.

Возврат
В поле **result** будет занесен числовой код ошибки. 0 - успех, 30 - ТМ не приложена, другие коды - прочие ошибки. В поле **identifier** будет занесен идентификатор Бикрипт секретного ключа. Список ошибок представлен в разделе «Список кодов возврата методов ICCC».

2. Метод внедерения ЭП в CMS объект, переданный в плагин.

```
ICCC_SignCMS(String unsignedCms)
```

Описание
Метод внедряет ЭП в заранее созданный CMS объект. Важно! Ключ для подписания ДОЛЖЕН БЫТЬ ранее загружен через метод **`LoadPrivateKeyTm.`**

Параметры
unsignedCms неподписанный CMS в кодировках PEM / Base64

Возврат
В поле **cms** подписанный CMS в формате PEM. В случае возникновения какой-либо ошибки – метод вернет ее код и текстовое описание.

3. Метод получения идентификатора Бикрипт из сертификата

```
ICCC_GetBicryptIdentifier(String userCertificate)
```

Описание
Метод получает идентификатор Бикрипт из сертификата.

Параметры
userCertificate сертификат в формате PEM.

Возврат
В параметре **result** строка с идентификатором Бикрипт.

4. Метод подписания хеш значения

```
SignDigest(String digest)
```

Описание
Метод формирует ЭП в RAW формате.

Параметры

digest	хеш в кодировке Base64.

Возврат
В параметре **sign** значение ЭП в кодировке Base64.

5. Метод формирования ЭП в формате CMS

```
Sign (
   String    data,
   String    signerCertificate,
   int       cmsType,
   int       encodingType,
   int       extensionsType,
   String[]  additionalCerts
)
```

Описание
Метод формирует ЭП в формате CMS (PKCS#7) с расширением CAdES BES.

Параметры

data	данные на подпись
signerCertificate	сертификат подписанта
cmsType	0 – отсоединенная ЭП, 1 – присоединенная ЭП
encodingType	0 – DER, 1 – PEM
extensionsType	0 – CMS (без расширенных атрибутов), 1 – CAdES-BES
additionalCerts	массив сертификатов, добавляемых в CMS (необязательный параметр)

Возврат
В параметре **cms** значение ЭП.

6. Метод расшифрования данных

```
ICCC_Decrypt (String envelopedCms, String userCertificate)
```

Описание
Метод расшифровывает данные в формате Enveloped CMS.

Параметры

envelopedCms	зашифрованные данные
userCertificate	сертификат адресата шифртекста

Возврат
В параметре **data** расшифрованные данные.

7. Метод вычисления хеш-значения

```
CalculateDigest (String data, String oid)
```

Описание
Метод вычисляет хеш-значение от данных **data** в соответствии с алгоритмом **oid**.

Параметры

data	данные, для которых вычисляется хеш
oid	строка с OID, определяющая алгоритм вычисления хеша

Возврат
В параметре **digest** вычисленный хеш в кодировке Base64.

8. Метод вычисления ЭП в формате Бикрипт

```
CreateBicryptFileSign (String data)
```

Описание
Метод вычисляет ЭП в формате Бикрипт для данных **data,** используя ранее загруженный секретный ключ.

Параметры

data	Данные в кодировке Base64, для которых вычисляется ЭП

Возврат
В параметре **sign** вычисленная ЭП в кодировке Base64. Sign включает в себя исходные данные **data** («подписанный файл»). Если требуется получить только ЭП в формате Бикрипт – см. **CreateBicryptFileSignShort**

9. Метод вычисления ЭП в формате Бикрипт

```
CreateBicryptFileSignShort (String data)
```

Описание
Метод вычисляет ЭП в формате Бикрипт для данных **data,** используя ранее загруженный секретный ключ.

Параметры

data	Данные в кодировке Base64, для которых вычисляется ЭП

Возврат
В параметре **sign** вычисленная ЭП в кодировке Base64.

Методы ICCC 2.0 по работе с токеном VPNKey-TLS

1. Метод аутентификации на токене

```
VKT_Login (int container, String pin)
```

Описание
Метод производит запуск прокси-сервера и осуществляет аутентификацию на токене.

Параметры

container	номер контейнера на токене VPNKey-TLS (1…5)
pin	пин-код доступа к контейнеру

Возврат
В параметре **token_info** детальная информация о прошивке токена.

2. Метод получения личных сертификатов ЭП из токена

```
VKT_GetCertificates()
```

Описание
Метод получает идентификаторы личных сертификатов ЭП из токена.

Возврат
В параметре **certIds** перечисление (массив) идентификаторов. В дальнейшем эти идентификаторы, действующие в рамках сессии, можно использовать для криптографических операций на токене.

3. Метод получения личного сертификата ЭП из токена

```
VKT_GetCertificate (String certId)
```

Описание
Метод получает из токена личный сертификат ЭП по его идентификатору.

Параметры

certId	идентификатор личного сертификата ЭП, полученный в рамках текущей сессии

Возврат
В параметре **certificate** сертификат ЭП.

4. Метод формирования ЭП на токене

```
VKT_Sign(String b64Data, String certId,
             int chainLen, int cmsMode)
```

Описание
Метод формирует ЭП в формате CMS под данными **b64Data**, используя секретный ключ, связанный с сертификатом под идентификатором **certId**. При этом, размер вкладываемой в CMS цепочки сертификатов, определяется параметром **chainLen**, а формат CMS определяется параметром **cmsMode**.

Параметры

b64Data	данные на подпись в кодировке Base64. **Важно!** Подписываться будут **декодированные** данные.
certID	идентификатор сертификата, секретным ключом которого будет производится подпись данных
chainLen	-1 – цепочка, исключая корневой, 1…n – количество вкладываемых сертификатов
cmsMode	0 – отсоединенная ЭП, 1 – присоединенная

Возврат
В параметре **cms** сформированная ЭП, закодированная в Base64.

5. Завершение сессии на токене VPN-Key-TLS

```
VKT_Logout ()
```

Описание
Метод завершает текущую сессию на токене.

Методы ICCC 2.0 по работе с форматом DSig

1. Метод формирования ЭП для XML в формате DSig.

```
DSIGN_Sign (String xml, String xmlElementNameInsertSign,
            int xmlElementNameInsertSignIndex, String
            xmlElementIDToSign, String canonicalizationUrl,
            String signerCert, String signatureID)
```

Описание
Метод формирует подписанную XML с ЭП в формате DSig.

Параметры

xml	XML, для которой формируется ЭП, в формате Base64
xmlElementNameInsertSign	наименование элемента, куда будет помещен контейнер с ЭП
xmlElementNameInsertSignIndex	индекс элемента, куда будет помещен контейнер с ЭП. 0 – если первый элемент, далее по порядку.
xmlElementIDToSign	идентификатор подписываемого элемента (тэга)
canonicalizationUrl	алгоритм каноникализации
signerCert	сертификат подписанта
signatureID	идентификатор элемента ЭП

Возврат
В параметре **signedXml** подписанная XML в формате Base64.

2. Метод проверки ЭП для XML в формате DSIG.

```
DSIGN_Check (String xml, int signToCheckNumber)
```

Описание
Метод проверяет ЭП в формате DSig.

xml	подписанная XML в формате Base64
signToCheckNumber	порядковый номер проверяемой ЭП (1…n)

Возврат
В параметре **checkStatus** результат проверки. 0 – успешно, иначе код ошибки.

Список кодов возврата методов ICCC

Код	Текстовое описание
0	Ошибок нет
1	Недостаточно памяти
2	Подпись неверна
3	Длина буфера неверна
4	Данные пользователя не соответствуют ожидаемым
5	Ошибка внутреннего тестирования криптоопераций
6	Ошибка декодирования мастер-ключа
8	Не поддерживаемая функция
9	Ошибка контрольной суммы файла с закрытым ключом
11	Нет подписи
12	Ошибка открытия файла
14	Ошибка открытия файла БОК
16	Количество носителей ключа превысило максимально допустимый предел
18	Ошибка чтения файла с мастер-ключом
19	Идентификатор подписи не зарегистрирован в БОК
20	Внутренние тесты библиотеки проведены с ошибкой
21	Ошибка чтения главного ключа
22	Ошибка чтения узла замены
23	Ошибка контрольной суммы главного ключа
24	Главный ключ требует ввода пароля
25	Не найден ДСЧ
26	Ошибка контрольной суммы при чтении TM
27	Ошибка загрузки зависимых библиотеки
28	Процесс инициализации ПДСЧ прерван пользователем
29	Ошибка использования TM-устройства - нет драйвера TMDRV
30	Идентификатор TouchMemory не приложен к считывателю
31	Ошибка чтения TM
32	Ошибка в параметрах функции
33	Ошибка дескриптора (например, происходит обращение к закрытому ранее дескриптору или вместо валидного дескриптора используется случайное значение)
34	Неправильный тип дескриптора (например, вместо типа H_USER в соответствующий параметр функции передается дескриптор типа H_PKEY)
35	Ошибка работы с программным датчиком - требуется инициализация
37	Ошибка чтения файла сетевых ключей
39	Ошибка инициализации библиотеки, не был вызван cr_init
40	Ошибка загрузки ключа
42	Ошибка сетевого ключа
43	Буфер не был зашифрован
44	Ошибка расшифрования буфера
45	Ошибка файлового ключа
46	Ошибка чтения файла
47	Ошибка записи файла
48	Ошибка архивации данных
49	Длина выделенного буфера недостаточна
101	Ошибка сервера ЭП. Устройство не найдено
102	Ошибка сервера ЭП. Нет сокета
103	Ошибка сервера ЭП. ERR_NO_RESOLVE
104	Ошибка сервера ЭП. Нет отклика
105	Ошибка сервера ЭП. Неверная структура пакета
106	Ошибка сервера ЭП. Не поддерживается протокол TCPIP
107	Ошибка сервера ЭП. Ключ не найден
108	Ошибка сервера ЭП. Некорректный параметр
109	Ошибка сервера ЭП. Внутренняя ошибка драйвера
110	Ошибка сервера ЭП. Превышено время ожидания
111	Ошибка сервера ЭП. Некорректная версия
11110	Ошибка драйвера TM
11111	Ошибка ПДСЧ
11112	Отсутствуют ГК и УЗ

Список кодов возврата методов ICCC по работе с VPN-Key TLS

0	"Функция не выполнена"
2	"Указаны неверные аргументы (несоответствие алфавита; выход за явно указанные в документе границы; недопустимые символы в base64, итд) или обязательный аргумент отсутствует"
3	"Недостаточное число подписей контейнера корневого сертификата"
4	"Не удалось проверить подлинность подписи"
6	"Попытка загрузки корневого сертификата без безопасного контейнера"
7	"Ошибка классификации корневого сертификата"
8	"Ошибка классификации сертификата УЦ"
9	"Ошибка классификации сертификата ЭП"
10	"Ошибка классификации сертификата TLS"
11	"Класс сертификата определить не удалось"
12	"Дубликат (сертификата)"
13	"Ошибка ФС при сохранении сертификата"
14	"Прочая ошибка при обработке входящего сертификата"
15	"Ошибка парсинга формата CMS"
16	"Функция получила недостаточно данных, или больше чем допустимо, или больше, чем было обещано, или неожиданный номер блока данных"
21	"В хранилище объектов недостаточно места"
24	"Пользователь уже выполнил вход"
25	"Пользователь заблокирован"
26	"Не инициализирован ДСЧ"
27	"Израсходованы попытки ввода PUK"
28	"Израсходованы попытки ввода PIN"
29	"Введен некорректный PIN"
32	"Пользователь не выполнил вход"
33	"Операция не проинициализирована"
35	"Введен некорректный идентификатор объекта"
42	"Устройство не в режиме инициализации"
44	"Устройство не в активном режиме"
47	"Введен некорректный идентификатор бизнес-системы"
48	"Введен некорректный PUK"
51	"Шаблон не применяется на данном устройстве"
52	"Ошибка формата CMS при разборе шаблона"
53	"Ошибка подписи под шаблоном"
54	"Ошибка формата при разборе документа"
55	"Прочая ошибка при разборе документа"
56	"Синтаксическая ошибка в документе"
57	"Документ нельзя подписать как визуализированный"
58	"Невозможно отобразить документ т.к. не был загружен шаблон"
59	"Ошибка формата шаблона"
60	"Версия документа и шаблона не совместимы"
61	"Недостаточно памяти для визуализации всех документов"
62	"Ошибка парсинга XML-шаблона"
63	"Превышение квоты документов на подписание"
90	"Введен некорректный SID"
95	"Нераспознанная/неподдерживаемая команда"
96	"Таймаут сессии"
97	"Операция (подписания; проверки подписи; шифрования) не выполнена"
200	"Ошибка соединения с HTTP прокси. Проверьте настройки"
210	"Ошибка аутентификации на HTTP прокси. Проверьте ваши логин и пароль"
220	"Ошибка работы с HTTP прокси"
700	"Ошибка ядра 0"
701	"Ошибка инициализации устройства"
702	"Ошибка выделения защищённой памяти на устройстве"
703	"Ошибка выделения внешней памяти на устройстве"
705	"Ошибка выделения памяти"
713	"Исполняемые модули для ПК на внешнем носителе повреждены"
714	"Происходит проверка исполняемых модулей для ПК на внешнем носителе устройства. Операцию следует повторить через несколько секунд"
720	"Файл не найден"
722	"Ошибка записи файла на устройство"
723	"Ошибка чтения файла с устройства"
724	"Недостаточно полномочий для файловой операции на устройстве"
725	"Недопустимая файловая операция"
726	"Ошибка защищённой памяти"
727	"Ошибка инициализации файловой системы"
728	"Внутренняя ошибка файловой системы"

750 "Внутренняя ошибка внешней файловой системы"
760 "Попытка инициализировать хранилище дважды"
770 "Ошибка чтения файла, записанного в неподдерживаемом формате"
771 "Ошибка миграции защищённой памяти"
780 "Неверный идентификатор криптооперации"
781 "Нет свободных слотов для криптооперации"
782 "Интерфейс занят другой интерактивной операцией"
783 "Операция отменена пользователем"
784 "Ожидание выбора пользователя"
785 "Истёк таймаут согласия пользователя на операцию"
786 "Не удалось найти указанный сертификат в списке получателей зашифрованного документа"
787 "Не указан сертификат, в адрес которого выполняется шифрование"
788 "Цепочка сертификатов указанной длины не может быть выгружена"
789 "На устройстве не установлено время"
790 "Попытка загрузить более старую версию встроенного ПО"
791 "Неверный заголовок в файле встроенного ПО"
792 "Подпись под обновлением неверна"
793 "Загрузка обновления завершена"
794 "Неверный ключ шифрования встроенного ПО"
795 "Обновление не найдено"
796 "Обновление не совместимо с текущей программно-аппаратной конфигурацией"
797 "Недостаточно места для загрузки обновления"
798 "Блок обновления поврежден или зашифрован на другом ключе"
799 "Ключи защиты обновлений не были загружены или были повреждены"
800 "Неверный номер ключа для загрузки обновления"
801 "Ошибка при записи в program flash"
802 "Прочая ошибка обновления"
803 "Некорректный серийный номер"
820 "Учётная запись с таким номером отсутствует на устройстве"
821 "PIN пользователя заблокирован (ещё можно восстановить с помощью PUK)"
822 "Введенные PIN-коды не совпадают"
823 "Введен неверный текущий PIN-код при смене PIN"
824 "Введенные PUK-коды не совпадают"
825 "Введен неверный текущий PUK-код при смене PUK-кода"
830 "Ошибка загрузки личного сертификата TLS"
831 "TLS-сертификат не загружен"
832 "Преждевременная попытка использования PUK"
833 "Команда не предназначена для активных учётных записей"
834 "Для разрешения доступа к функции необходимо сменить транспортный PIN-код"
835 "Команда не поддерживается для учётных записей, инициализированных в соответствии с новым протоколом"
850 "Сертификат отозван"
851 "Испорчен файл со списком отозванных сертификатов. Продолжение операции невозможно."
852 "Сертификат просрочен"
855 "На устройстве установлен более новый список отзыва сертификатов"
856 "Неверное использование объекта (например, сертификата TLS для ЭП и т.п.)"
857 "Внутренняя ошибка при создании PKCS10-RequestInfo"
863 "Структура с данными пользователя не соответствует формату"
864 "Структура с атрибутами пользователя не соответствует формату"
865 "Нет свободных слотов для создания пары Закрытый ключ - Сертификат"
866 "Превышение допустимого числа личных сертификатов на один запрос"
867 "Не найден запрос для входящего сертификата"
868 "Действие сертификата приостановлено"
869 "Совместный доступ к объекту, принадлежащему другому интерфейсу"
870 "CRL отсутствует"
900 "Функция не реализована в этой версии прошивки"
901 "Встроенное ПО устройства и используемое на ПК ПО несовместимы"
902 "На устройстве отсутствует сертификат первичного TLS подключения или транспортный"
950 "Софт-криптофункция выполнена успешно, результат не выгружен"
951 "Софт-криптофункция получила неверные параметры"
952 "Софт-криптофункция завершилось неуспешно"
953 "Внутренняя ошибка хранилища сертификатов"
999 "Ошибка формата одного или нескольких полей запроса"
1030 "Не удаётся открыть сокет на TLS-сервере"
1300 "Не удалось построить цепочку доверия"

0x9999 префикс ошибок с сокетом // 39321

601 Не удается прочитать файл sslgate.url
602 SID0 не обнаружен

603	SID2 не обнаружен
604	Не удается получить значение узла сети по имени
605	Создание сокета завершилось неудачно
606	ошибка обращения к банковскому ключу
607	Не удается полностью отправить данные
608	Задано необрабатываемое свойство сертификата
609	указанное поле не найдено в ответе от токена
610	ошибка в процедуре logout
611	выделенный буфер слишком маленький
612	не удается запустить ICS app

Приложение №1

Инструкция по работе с тестовым приложением