Программный комплекс «Блокхост-ЭЦП» 2.0 (ПК «Litoria Desktop»)

Руководство программиста

АННОТАЦИЯ

Настоящий документ содержит руководство программиста к программному комплексу «Блокхост-ЭЦП» 2.0 (в дальнейшем ПК «Litoria Desktop», ПК или комплекс).

В разделе «Назначение и условия применения ПК «Litoria Desktop» указаны назначение и функции комплекса, аппаратные и программные требования к рабочему компьютеру пользователя, на котором будет использоваться комплекс.

В разделе «Обращение к комплексу» описаны параметры командной строки, с помощью которых можно выполнить основные функции комплекса.

В разделе «Входные и выходные данные» указаны виды входных и выходных данных.

В разделе «Сообщения» приведены тексты ошибок, возникающих при работе с комплексом из командной строки, и методы их устранения.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ ПК «LITORIA DESKTOP»

1.1. НАЗНАЧЕНИЕ КОМПЛЕКСА

Основным назначением ПК «Litoria Desktop» является создание, добавление, заверка и проверка электронной подписи (ЭП), а также шифрование и расшифровывание файлов. В ПК «Litoria Desktop» реализована возможность выполнения одновременных операций создания ЭП и шифрования, расшифровывания и проверки ЭП.

Кроме того, продукт позволяет выполнить функции просмотра хранилища сертификатов и списков отзыва сертификатов; создания запроса на выпуск и перевыпуск сертификата; установки сертификата на устройство; установки сертификата из устройства в реестр; просмотра установленных криптопровайдеров и их параметров; формирования DVCS-запросов и анализа DVC-квитанций в соответствии с рекомендациями RFC3029.

1.2. ФУНКЦИИ КОМПЛЕКСА

ПК «Litoria Desktop» предоставляет возможность выполнить следующие функции:

- создание нового запроса на сертификат;
- создание запроса на основе имеющегося сертификата;
- установка сертификата на устройство;
- просмотр сертификатов в контейнерах;
- установка сертификата из устройства в хранилище «Личное»;
- управление сертификатами:
  - импорт;
  - экспорт;
  - удаление;
  - детальный просмотр;
  - проверка статуса по локальному и/или удаленному СОС и по протоколу OCSP в реальном времени;
- управление списками отзыва сертификата:
  - импорт;
  - экспорт;
  - удаление;
  - детальный просмотр;
- просмотр списка криптопровайдеров;
- удаление контейнера закрытого ключа;
- управление настройками комплекса;
- создание усовершенствованной ЭП (УЭП) для файлов произвольного типа;
- добавление УЭП для подписанных файлов;
- заверка УЭП для подписанных файлов;
- проверка УЭП для подписанных файлов с возможностью получения исходного документа;
- формирование DVCS-запросов и анализ DVC-квитанций в соответствии с рекомендациями RFC3029;
- шифрование файла произвольного типа;
- расшифровывание файла;
- гарантированное удаление файлов произвольно типа;
- универсальные операции:
  - создание УЭП и шифрование файла произвольного типа;
  - расшифровывание файла и проверка УЭП с возможностью получения исходного документа.

1.3. УСЛОВИЯ ПРИМЕНЕНИЯ КОМПЛЕКСА

Требования к рабочей станции, на которую устанавливается ПК «Litoria Desktop», обусловлены применением ОС.

ПК «Litoria Desktop» функционирует под управлением следующих ОС:

- Windows XP (32 бит/64 бит);
- Windows Sever 2003 (32 бит/64 бит);
- Windows Server 2008 (32 бит/64 бит);
- Windows Vista (32 бит/64 бит);
- Windows 7 (32 бит/64 бит);
- Windows Server 2008 R2;
- Windows 8 (32 бит/64 бит);
- Windows Server 2012 (64 бит);
- Windows 8.1 (32 бит/64 бит);
- Windows Server 2012 R2 (64 бит).

Дополнительно должно быть установлено следующее программное обеспечение:

1. Средство криптографической защиты информации, реализованное в соответствии с технологией Microsoft CSP. Например: программные СКЗИ – «ViPNet CSP» версии 3.2, «ВАЛИДАТА CSP» версии 4.0, «Крипто-Ком 3.2», «КриптоПро CSP» версии 3.6 и выше или ПК «ЛИССИ-CSP»

2. ОБРАЩЕНИЕ К КОМПЛЕКСУ

ПК «Litoria Desktop» предоставляет возможность использования его основных функций в режиме командной строки.

Синтаксис команды запуска имеет вид:

LitoriaConsole.exe <параметр запуска функции> <другие параметры> <имя обрабатываемого файла>.

Требования к командной строке:

1) Параметры запуска функций, другие параметры и имена обрабатываемых файлов могут находиться в любом месте командной строки.
2) Значения параметров должны быть расположены строго после задания параметра.
3) Значения параметров, содержащие пробелы, должны быть заключены в кавычки.
4) Имена обрабатываемых файлов должны быть заключены в кавычки, если путь к ним содержит пробелы.

Параметры запуска функций и другие параметры приведены в таблице 2.1.

Таблица 2.1.

Функции ПК «Litoria Desktop»	**Параметры запуска функции**		**Другие параметры**	
	Параметр	**Назначение**	**Задание параметра**	**Назначение**
Работа с ЭП	-c, --ceds	Создание ЭП.	-n, --serialeds <серийный номер сертификата подписчика>	Указание сертификата подписчика.
	-x, --detached	Создание отделенной подписи.	-m, --comment <текст комментария>	Комментарий к подписи.
	-u, --cades	Создание УЭП.	-y, --tsp <адрес службы штампов времени>	Указание адреса службы штампов времени.
	-a, --aeds	Добавление ЭП.		
	-v, --veds	Проверка ЭП.	-p, --detacheddir <путь к файлу-оригиналу подписи>	Задание пути к файлу-оригиналу отделенной подписи.
Работа с шифрованием	-e, --encr	Шифрование файла.	-r, --serialreceiver <серийный номер сертификата получателя>	Указание сертификатов получателей. Может быть несколько.
			-k, --filereceiver <путь к файлу сертификата получателя>	
	-d, --decr	Расшифровывание файла.		
Работа с ДТС-клиентом	-i, --dvcinvoice	Создание ДТС запроса.	-n, --serialeds <серийный номер сертификата подписчика>	Указание сертификата подписчика. Если сертификат не указан, будет создан анонимный запрос. Анонимный DVCS-запрос используется только в демонстрационных целях.

Функции ПК «Litoria Desktop»	Параметры запуска функции		Другие параметры	
	Параметр	Назначение	Задание параметра	Назначение
			-b, --dvctype <vsd, vpkc>	Тип ДТС запроса. При указании другого типа значение автоматически заменится на vpkc.
			-w, --dvchash < Y|y|yes|YES|Yes>	Хэширование данных. Если значение – ни одно из указанных, хэширование не будет произведено.
			-j, --dvcaddress <адрес сервера службы ДТС >	Адрес сервера службы ДТС.
Информация о программе	-t, --about			
Общие параметры			-f, --format64	Формат выходного файла BASE64.
			-o, --outdir <выходной каталог>	Указание каталога, куда сохранится выходной файл.

При создании ЭП любого вида из командной строки подпись всегда будет создаваться в неквалифицированном режиме (независимо от значения настройки, установленной в разделе «Настройки ЭП»).

Примеры командной строки:

1) Создание обычной ЭП:
   LitoriaConsole.exe --ceds --serialeds 497D3C2C000000000674
   «c:\comand line\test.txt»
   или
   LitoriaConsole.exe -c -n 497D3C2C000000000674 c:\test.txt
2) Создание обычной отделенной ЭП:
   LitoriaConsole.exe --ceds --detached --serialeds 497D3C2C000000000674 «c:\comand line \test.txt»
   или
   LitoriaConsole.exe -c -x -n 497D3C2C000000000674 c:\test.txt
3) Создание УЭП
   LitoriaConsole.exe --ceds --cades --serialeds 497D3C2C000000000674 --tsp tsp.gaz-is.ru/tsp/tsp.srf «c:\comand line\test.txt»
   или
   LitoriaConsole.exe -c -u -n 497D3C2C000000000674 -y tsp.gaz-is.ru/tsp/tsp.srf c:\test.txt
4) Проверка обычной ЭП
   LitoriaConsole.exe --veds «c:\comand line \test.txt.p7s»
   или
   LitoriaConsole.exe –v c:\test.txt.p7s
5) Проверка УЭП
   LitoriaConsole.exe --veds --cades --tsp tsp.gaz-is.ru/tsp/tsp.srf
   «c:\comand line \test.txt.p7s»
   или
   LitoriaConsole.exe -v -u -y www.gaz-is.ru/tsp/tsp.srf c:\test.txt.p7s

6) Шифрование файла
   LitoriaConsole.exe --encr --serialreceiver 497D3C2C000000000674
   «c:\comand line\test.txt»
   или
   LitoriaConsole.exe -e -r 497D3C2C000000000674 c:\test.txt
7) Шифрование файла для нескольких получателей
   LitoriaConsole.exe -e -r 497D3C2C000000000674 -r 138F137900000000268C c:\test.txt
8) Расшифровывание файла
   LitoriaConsole.exe --decr «c:\comand line\test.txt.p7m»
   или
   LitoriaConsole.exe -d c:\test.txt.p7m
9) Создание запроса в службу ДТС
   LitoriaConsole.exe --dvcinvoice --dvctype vsd --dvcaddress http://dts.gaz-is.ru/dvc/dvc.srf C:\test.txt.p7s

3. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

3.1. ВХОДНЫЕ ДАННЫЕ

Входные данные для ПК «Litoria Desktop» отличаются друг от друга в зависимости от выполняемой операции. В таблице 3.1 приведены входные данные для функций комплекса, которые можно выполнить из командной строки.

Таблица 3.1

Функция	Входные данные	Примечание
Создание ЭП	1. Файл произвольного типа[1]; 2. Сертификат подписчика (указанный вручную); 3. Параметры подписи (указанные вручную).	Для выполнения данной функции необходимо иметь в наличии ключевой носитель с закрытым ключом сертификата подписчика.
Добавление ЭП Заверка ЭП	1. Подписанный файл; 2. Сертификат подписчика (указанный вручную); 3. Параметры подписи (указанные вручную).	Для выполнения данной функции необходимо иметь в наличии ключевой носитель с закрытым ключом сертификата подписчика.
Проверка ЭП	1. Подписанный файл; 2. Параметры проверки подписи (указанные вручную).	
Шифрование	1. Файл произвольного типа[1]; 2. Сертификаты получателей (указанные вручную).	
Расшифровывание	1. Зашифрованный файл.	
Функция ДТС-клиента	Для DVCS-запроса VSD типа: 1. Подписанный файл в формате pkcs#7 ; 2. Параметры запроса; 3. Сертификат подписчика; 4. Адрес ДТС сервера.	
	Для DVCS-запроса VPCS типа: 1. Сертификат ключа подписи; 2. Параметры запроса; 3. Сертификат подписчика; 4. Адрес ДТС сервера.	

3.2. ВЫХОДНЫЕ ДАННЫЕ

В результате выполнения операций шифрования и создания ЭП на выходе ПК «Litoria Desktop» формируются файлы с расширениями, указанными в таблице 3.2.

[1] ПК «Litoria Desktop» работает с файлами форматов, поддерживаемых ПО Microsoft Office и соответствующими приложениями, установленными в ОС. При подписании таких файлов ЭП не встраивается в сам файл, а создается в формате CAdES.

Таблица 3.2

Иконка	Тип файла	Расширение файла	Описание
	Подписанный файл	.p7s	подписан в DER-кодировке или в BASE64-кодировке
	Зашифрованный файл	.p7m	зашифрован в DER-кодировке или в BASE64-кодировке
	Подписанный и зашифрованный файл	.p7s.p7m	подписан и зашифрован в DER-кодировке или в BASE64-кодировке

Новое расширение файлу назначается в зависимости от типа операции.

Идентификатор создаваемого после выполнения операций шифрования и создания файла формируется по следующей схеме:

Идентификатор файла до выполнения операций шифрования и/или создания ЭП: **<Имя файла>.<расширение файла до выполнения операции>.**

Идентификатор файла после выполнения операций шифрования и/или создания ЭП: **<Имя файла>.<расширение файла до выполнения операции>.<Новое расширение>**.

Аналогично происходит восстановление старого идентификатора файла после выполнения обратных операций расшифровывания и снятия ЭП.

Примечание: ПК «Litoria Desktop» не встраивает ЭП в файлы форматов PDF, XML и ODF, а создает для них подпись в формате CAdES.

4. СООБЩЕНИЯ

В ходе работы с ПК «Litoria Desktop» из командной строки могут появляться сообщения. Полный список сообщений приведен в Приложении 1. При появлении сообщения, сгенерированного комплексом, попытайтесь решить проблему самостоятельно. Если не получается, обратитесь в службу технической поддержки.

ПРИЛОЖЕНИЕ 1

Полный список сообщений пользователю:

№	Сообщение
1.	"Ошибки нет"
2.	"Ошибка, библиотека не загружена"
3.	"Ошибка открытия входного файла"
4.	"Ошибка процесса подписи"
5.	"Ошибка получения сертификатов"
6.	"Ошибка получения сертификата"
7.	"Ошибка преобразования файла из der кодировки в base64"
8.	"Ошибка в процессе проверки подписи"
9.	"Ошибка открытия присоединенного файла"
10.	"Ошибка добавления подписи"
11.	"Ошибка открытия временного файла"
12.	"Ошибка в процессе шифрования"
13.	"Ошибка в процессе расшифрования"
14.	"Ошибка в процессе безопасного удаления"
15.	"Ошибка проверки сертификата"
16.	"Ошибка создания нового запроса на сертификат"
17.	"Ошибка установки личного сертификата"
18.	"Ошибка получения списка криптопровайдеров"
19.	"Ошибка удаления сертификата"
20.	"Ошибка получения информации о криптопровайдере"
21.	"Ошибка получения детальной информации о сертификате"
22.	"Ошибка получения сертификата из контейнера"
23.	"Ошибка получения цепочки сертификата"
24.	"Ошибка кэширования контейнера"
25.	"Ошибка получения списков отзыва"
26.	"Ошибка удаления контейнера"
27.	"Ошибка создания самоподписанного сертификата"
28.	"Ошибка создания сертификата пользователя"
29.	"Ошибка удаления СОС"
30.	"Ошибка установки СОС"
31.	"Ошибка получения СОС из данных"
32.	"Ошибка инициализации параметров создания ЭП"
33.	"Неверный набор данных сертификата подписчика"
34.	"Сертификат подписчика отсутствует в хранилище ‘Личные’"
35.	"Алгоритм хэширования не определен"
36.	"Ошибка формирования атрибута SignerCertReferenseV2"
37.	"Ошибка формирования атрибута SignerCertReferense"
38.	"Ошибка инициализации параметров функции. Неверный параметр"
39.	"Подходящий криптографический алгоритм не определен"
40.	"Ошибка в функции кэширования контейнера"
41.	"Ошибка в функции отмены кэширования контейнера"
42.	"Ошибка вычисления хэш-значения"
43.	"Не удалось найти подходящий криптопровайдер"
44.	"Не удалось получить подходящий алгоритм хэширования"
45.	"Ошибка инициализации данных для хэширования файла"
46.	"Ошибка хэширования файла"
47.	"Ошибка получения результата хэширования файла"

№	Сообщение
48.	"Для инициализации механизма хэширования передан алгоритм, не являющийся алгоритмом хэширования"
49.	"Ошибка создания ЭЦП"
50.	"Для инициализации механизма подписи передан алгоритм, не являющийся алгоритмом подписи"
51.	"Ошибка определения параметров создания ЭЦП"
52.	"Не удалось определить комбинированный алгоритм вычисления хэш-значения и подписи"
53.	"Формат создаваемой подписи задан некорректно"
54.	"Ошибка добавления ЭЦП"
55.	"Не удалось получить значения подписей из сообщения"
56.	"Неверный дескриптор сообщения"
57.	"Ошибка получения индекса добавленной подписи"
58.	"Ошибка заверения подписи"
59.	"Не удалось сформировать данные для удаленной подписи хэш-значения"
60.	"Разделение подписанного документа на составляющие не произведено"
61.	"Не удалось обновить подпись необходимой дополнительной информацией"
62.	"Произошла ошибка в процессе объединения компонент механизма добавления подписи через удаленную подпись хэш-значения"
63.	"Ошибка объединения 2-х отделенных ЭЦП"
64.	"Ошибка подписи хэш-значения"
65.	"Не удалось сформировать CMS"
66.	"Некорректно осуществлять заверение или добавление подписи, если сообщение содержит одну или несколько подписей с архивными штампами времени"
67.	"Ошибка усовершенствования ЭЦП"
68.	"Не удалось получить значение подписи"
69.	"Не удалось получить информацию о сертификате подписавшего лица"
70.	"Не удалось получить информацию из сети"
71.	"Цепочка сертификата подписавшего лица составлена некорректно"
72.	"Цепочка сертификата TSA-оператора составлена некорректно"
73.	"Цепочка сертификата OCSP-оператора составлена некорректно"
74.	"Ошибка формирования атрибутов RevocationValues и CompleteRevocationRefs"
75.	"Ошибка формирования атрибутов CompleteCertificateRefs и CertificateValues"
76.	"Ошибка проверки используемых сертификатов на действительность относительно времени внешнего штампа"
77.	"Один или несколько сертификатов цепочки сертификата подписавшего лица недействительны"
78.	"Один или несколько сертификатов цепочки сертификата TSA-оператора недействительны"
79.	"Один или несколько сертификатов цепочки сертификата OCSP-оператора недействительны"
80.	"Ошибка добавления неподписанного атрибута в подпись"
81.	"Ошибка получения результата операции"
82.	"Ошибка получения результата операции"
83.	"Ошибка получения информации об отзыве сертификата"
84.	"Ошибка формирования ссылки на значение отзыва"
85.	"Ошибка формирования ссылки на значение сертификата"
86.	"Ошибка формирования манифеста для квитанции в XAdES"
87.	"Ошибка формирования служебной информации о проверке для квитанции в XAdES"
88.	"Ошибка извлечения квитанции и документа"
89.	"Ошибка подписи XAdES"
90.	"Ошибка создания подписанной квитанции XAdES"
91.	"Ошибка добавления подписанной квитанции в ЭЦП, на которую эта квитанция создавалась"
92.	"Ошибка проверки подписи XAdES"

№	Сообщение
93.	"Ошибка проверки манифеста"
94.	"Ошибка получения информации по квитанции"
95.	"Ошибка получения сертификата подписчика XAdES"
96.	"Ошибка добавления узла с готовой подписью в документ"
97.	"Не удалось создать soap конверт с технологическим сообщением об ошибке"
98.	"Ошибка преобразования буфера xml данных в DOM объект"
99.	"Ошибка сериализации объекта подписи в буфер"
100.	"Ошибка разбора блока данных квитанции из буфера"
101.	"Ошибка разбора манифеста из буфера"
102.	"Ошибка анализа секции QualifyingProperties xml подписи из потока"
103.	"Ошибка разбора подписи из потока"
104.	"В подписи отсутствует сертификат подписчика"
105.	"В подписи присутствует больше одного сертификата"
106.	"Ошибка анализа входного документа"
107.	"Не удалось получить штамп времени на значение подписи или он некорректен"
108.	"Не удалось получить штамп времени на доказательства подписи или он некорректен"
109.	"Статус ответа службы штампов времени некорректен"
110.	"Полученный штамп времени содержит ошибки"
111.	"Не удалось получить информацию о сертификате TSA-оператора"
112.	"Сертификат службы штампов времени не предназначен для установки отметки времени"
113.	"Подпись штампа времени математически некорректна"
114.	"Ошибка получения времени создания внутреннего штампа времени"
115.	"Ошибка получения времени создания внешнего штампа времени"
116.	"Не удалось собрать доказательства действительности внутреннего штампа времени"
117.	"В запросе указан неизвестный системе алгоритм"
118.	"Указанный в запросе алгоритм не является алгоритмом хэширования"
119.	"Указанный алгоритм поддерживается системой, однако длина хэш-значения не соответствует требуемой"
120.	"Ошибка создания TSP-запроса"
121.	"Алгоритм хэширования, указанный в запросе, не поддерживается для обработки"
122.	"Необходимый CRL не найден"
123.	"Ошибка получения CRL из хранилища"
124.	"Ошибка получения CRL из сети"
125.	"Для проверки передан пустой сертификат"
126.	"Ошибка доступа к хранилищу промежуточных центров сертификации"
127.	"Ошибка доступа к хранилищу корневых центров сертификации"
128.	"Проверяемый сертификат отозван по CRL"
129.	"Ошибка получения точек распространения CRL"
130.	"Сертификат не содержит ни одной точки распространения CRL"
131.	"Не удалось определить формат CDP"
132.	"Полученный CRL недействителен по времени"
133.	"Не удалось установить CRL в хранилище сертификатов"
134.	"Цепочка проверяемого сертификата составлена некорректно"
135.	"Ошибка создания OCSP-запроса"
136.	"Ошибка получения точек распространения OCSP"
137.	"Сертификат не содержит ни одной точки распространения OCSP"
138.	"Не удалось определить формат OCSP CDP"
139.	"Поставщик сертификата не определен"
140.	"Не удалось получить OCSP-ответ"
141.	"Сертификат OCSP-оператора не определен"

№	Сообщение
142.	"Цепочка проверяемого сертификата составлена некорректно"
143.	"Издатель сертификата не определен, либо сертификат самоподписанный"
144.	"Не удалось проверить сертификат по CRL"
145.	"Не удалось проверить сертификат по OCSP"
146.	"Не удалось сформировать список отзыва сертификатов"
147.	"Ошибка формирования структуры информации списка отзыва сертификатов"
148.	"Ошибка подписи информации списка отзыва сертификатов"
149.	"Проверяемый сертификат отозван по OCSP"
150.	"Ошибка разбора OCSP-запроса"
151.	"Ошибка проверки целостности CRL. CRL поврежден либо некорректен"
152.	"Издатель CRL не определен"
153.	"В проверяемом списке отзыва сертификатов отсутствует информация об издателе"
154.	"Ошибка проверки целостности OCSP-запроса"
155.	"Статус ответа некорректен"
156.	"Ошибка построения цепочки сертификата OCSP-службы"
157.	"Ошибка проверки целостности OCSP-ответа"
158.	"Ошибка инициализации преобразования отделенной ЭЦП в присоединенную"
159.	"Ошибка преобразования отделенной ЭЦП в присоединенную"
160.	"Ошибка записи заголовка подписи в результирующий файл"
161.	"Ошибка записи данных в результирующий файл"
162.	"Ошибка записи данных подписи в результирующий файл"
163.	"Необходимые имя пользователя и пароль для прокси заданы неверно"
164.	"Ошибка сетевого обращения"
165.	"Ошибка определения типа подписи"
166.	"Ошибка инициализации данных для проверки ЭЦП"
167.	"Ошибка проверки математической целостности подписи"
168.	"Ошибка определения типа данных в файле"
169.	"Ошибка определения типа сообщения"
170.	"Ошибка проверки ЭЦП подписанного сообщения"
171.	"Невозможно получить исходные данные подписанного сообщения"
172.	"Подпись отделенная"
173.	"Ни один из алгоритмов хэширования, представленных в структуре подписанного файла, не поддерживается в системе"
174.	"Алгоритм хэширования не содержится в списке используемых алгоритмов подписанного сообщения"
175.	"Не определен сертификат открытого ключа"
176.	"Ошибка декодирования атрибутов УЭЦП"
177.	"Ошибка кодирования атрибутов УЭЦП"
178.	"Отсутствуют значения сертификатов в атрибуте CertificateValues"
179.	"Ошибка создания дополнительного хранилища сертификатов"
180.	"Ошибка проверки доказательств УЭЦП для сертификата подписчика"
181.	"Один или несколько сертификатов из цепочки сертификата подписчика являлись недействительными на момент получения внешнего штампа времени"
182.	"В атрибут подписи включены не все сертификаты из цепочки"
183.	"Целостность подписи нарушена. Возможно, произошла подмена сертификата подписчика"
184.	"Ссылки на значения сертификатов были собраны не для всех сертификатов из цепочки, либо они недействительны"
185.	"Значения отзывов были собраны не для всех сертификатов из цепочки, либо они недействительны"
186.	"Проверяемый сертификат на момент создания УЭЦП был отозван"

№	Сообщение
187.	"Не удалось сформировать CRL"
188.	"Ошибка проверки доказательств УЭЦП для сертификата TSA-оператора"
189.	"Один или несколько сертификатов из цепочки сертификата TSA-оператора являются недействительными на текущий момент времени"
190.	"Ошибка проверки корректности значений отзывов"
191.	"Ошибка получения времени формирования OCSP-ответа"
192.	"Ошибка проверки корректности OCSP-ответа"
193.	"В сертификате OCSP отсутствует необходимое расширение szOID_PKIX_OCSP_NOCHECK"
194.	"Подпись OCSP-ответа математически некорректна"
195.	"Ссылки на значения отзывов были собраны не для всех значений отзывов, либо они недействительны"
196.	"Ошибка проверки доказательств УЭЦП для сертификата OCSP-оператора"
197.	"Один или несколько сертификатов из цепочки сертификата OCSP-оператора являлись недействительными на момент получения внешнего штампа времени"
198.	"Ошибка проверки внутреннего штампа времени и соответствия хэш-значений"
199.	"Хэш-значение подписи не соответствует хэш-значению во внутреннем штампе времени"
200.	"Ошибка проверки внешнего штампа времени и соответствия хэш-значений"
201.	"Хэш-значение доказательств подписи не соответствует хэш-значению во внешнем штампе времени"
202.	"Не удалось определить сертификат OCSP-оператора"
203.	"Время в OCSP-ответе опережает время во внешнем штампе. Время серверов OCSP и TSP не было синхронизировано"
204.	"Сертификат службы OCSP не предназначен для подписи OCSP-ответов"
205.	"Ошибка получения атрибута подписи"
206.	"Атрибут с заданным типом отсутствует в подписи"
207.	"Ошибка добавления атрибута в подпись"
208.	"Статус проверяемого сертификата не определен"
209.	"Ошибка получения информации о штампах времени внутри подписи"
210.	"Ошибка получения информации об отзыве сертификата"
211.	"Ошибка получения информации о списке(-ах) отзыва"
212.	"Хэш-значение отзыва не найдено, либо оно недействительно"
213.	"Ошибка инициализации данных для шифрования сообщения"
214.	"Неверный набор данных сертификата получателя"
215.	"Сертификат получателя не определен"
216.	"Не найден подходящий алгоритм шифрования"
217.	"Не найден закрытый ключ, соответствующий сертификату открытого ключа"
218.	"Набор ключей не существует. Возможно, вы ввели неверный ПИН-код"
219.	"Ошибка инициализации данных для расшифровывания сообщения"
220.	"Ошибка расшифровывания сообщения"
221.	"Ошибка шифрования сообщения"
222.	"Ошибка гарантированного удаления данных"
223.	"Криптопровайдер не указан"
224.	"Не удалось определить тип криптопровайдера"
225.	"Ошибка создания контейнера ключей"
226.	"Ошибка генерации пары ключей"
227.	"Ошибка получения длины структуры под экспортируемый открытый ключ"
228.	"Ошибка экспортирования открытого ключа"
229.	"Ошибка кодирования информации о владельце сертификата"
230.	"Возникла ошибка в процессе подписания и кодирования запроса на сертификат"
231.	"Ошибка кодирования информации в base64"

№	Сообщение
232.	"Неверный набор данных используемого сертификата"
233.	"Не удалось получить контекст криптопровайдера"
234.	"Ошибка при получении размера имени контейнера секретного ключа"
235.	"Ошибка при получении имени контейнера секретного ключа"
236.	"Имя контейнера ключа не задано и не определено"
237.	"Ошибка создания в сертификате ссылки на закрытый ключ"
238.	"Не удалось установить сертификат в хранилище сертификатов"
239.	"Ошибка декодирования информации из base64"
240.	"Ошибка создания запроса на сертификат"
241.	"Ошибка установки сертификата и создания связки открытый-закрытый ключ"
242.	"Ошибка получения сертификата из хранилища"
243.	"Ошибка получения списка сертификатов из заданного хранилища"
244.	"Ошибка получения расширенной информации о сертификате"
245.	"Не удалось получить цепочку сертификации для выбранного сертификата"
246.	"Цепочка сертификации составлена некорректно"
247.	"Неверный набор данных используемого списка отзыва сертификатов"
248.	"Не удалось установить список отзыва сертификатов в хранилище"
249.	"Ошибка создания самоподписанного сертификата"
250.	"Ошибка формирования структуры информации о самоподписанном сертификате"
251.	"Ошибка подписи информации о самоподписанном сертификате"
252.	"Ошибка выпуска сертификата пользователя"
253.	"Ошибка определения информации для доступа к закрытому ключу"
254.	"Ошибка формирования структуры информации о пользовательском сертификате"
255.	"Ошибка подписи информации о пользовательском сертификате"
256.	"Соответствие открытого ключа устанавливаемого сертификата и открытого ключа в контейнере не установлено"
257.	"Данные запроса на сертификат имеют некорректный формат"
258.	"Ошибка формирования структуры информации о запросе на сертификат"
259.	"Не удалось рассчитать значение ЭЦП на данные запроса на сертификат"
260.	"Значение подписи запроса на сертификат математически некорректно"
261.	"Не удалось установить сертификат на устройство"
262.	"Ошибка декодирования структуры данных"
263.	"Ошибка кодирования информации в структуру данных"
264.	"Ошибка декодирования объектного идентификатора"
265.	"Имя файла не задано"
266.	"Ошибка создания DVCS-запроса"
267.	"Неверный набор данных проверяемого сертификата"
268.	"Тип DVCS-запроса некорректен"
269.	"Ошибка подписи данных протокола DVCS"
270.	"Ошибка проверки подписи данных протокола DVCS"
271.	"Ошибка разбора DVC-квитанции"
272.	"Ошибка создания DVC-квитанции"
273.	"Ошибка замены значения серифного номера в DVC-квитанции"
274.	"Ошибка получения криптографических алгоритмов из DVCS-запроса"
275.	"Не удалось выполнить операцию пролонгации квитанции"
276.	"Ошибка определения типа DVCS-запроса"
277.	"Ошибка получения информации из структуры DVCS-запроса"
278.	"Ошибка получения 'подзапроса' из структуры DVCS-запроса"
279.	"Индекс запрашиваемого компонента находится вне границ массива"
280.	"Ошибка получения алгоритмов подписи из подписанного сообщения"

№	Сообщение
281.	"Ошибка объединения нескольких DVCS-ответ в результирующий DVCS-ответ"
282.	"Ошибка проверки соответствия DVCS-ответа DVCS-запросу"
283.	"Ответ не соответствует запросу, произошла подмена ответа"
284.	"Ошибка удаления аутентификационной информации из DVCS-запроса"
285.	"Сертификат или один из сертификатов в цепочке недействителен на текущий момент времени"
286.	"Сертификат или один из сертификатов в цепочке отозван"
287.	"Сертификат или один из сертификатов в цепочке искажен (содержит недействительную цифровую подпись)"
288.	"Сертификат или один из сертификатов в цепочке не предназначен для данного использования"
289.	"Сертификат или один из сертификатов в цепочке издан недоверенным центром сертификации"
290.	"Один из сертификатов в цепочке издан центром, сертифицированным проверяемым сертификатом (циклическая цепочка)"
291.	"Построение цепочки сертификации не завершено (неполная цепочка)"
292.	"Ошибка проверки отзыва промежуточного сертификата цепочки"
293.	"Ошибка получения имен криптопровайдеров в системе"
294.	"Ошибка получения параметров криптопровайдера"
295.	"Ошибка получения сертификата ключа подписи из контейнера"
296.	"Ошибка удаления контейнера ключей"
297.	"Ошибка простановки архивного штампа времени"
298.	"Подпись недействительна"
299.	"Подпись не является усовершенствованной"
300.	"Заверяющий подпись штамп времени не определен"
301.	"Не удалось собрать доказательства действительности заверяющего штампа времени"
302.	"Ошибка замены заверяющего штампа в подписи"
303.	"Не удалось рассчитать хэш-значение для формирования запроса в TSP-службу"
304.	"Не удалось сформировать архивный штамп времени и добавить его в обрабатываемую подпись"
305.	"Подпись уже является усовершенствованной"
306.	"Не удалось проверить исходную подпись, либо разделить подпись и данные"
307.	"Ошибка проверки корректности архивных штампов времени"
308.	"Не удалось получить данные из файла-подписи"
309.	"Ошибка проверки наличия и корректности доказательств действительности цепочки сертификата TSA-оператора внешнего штампа времени на момент формирования первого архивного штампа"
310.	"Не удалось рассчитать хэш-значение для проверки корректности архивного штампа"
311.	"Хэш-значение в архивном штампе времени не соответствует вновь вычисленному"
312.	"Ошибка проверки наличия и корректности доказательств действительности цепочки сертификата TSA-оператора архивного штампа времени на момент формирования последующего архивного штампа"
313.	"Цепочка сертификата TSA-оператора последнего архивного штампа времени составлена некорректно"
314.	"Ошибка проверки корректности последнего архивного штампа"
315.	"Не удалось получить расширения сертификата из запроса на сертификат"
316.	"Расширение Enhanced Key Usage имеет некорректный формат"
317.	"Расширение Key Usage имеет некорректный формат"
318.	"Произошла ошибка в процессе формирования asn.1 структур расширений сертификата"
319.	"Параметры расширения заданы неверно"
320.	"Ошибка формирования расширения Enhanced Key Usage"
321.	"Ошибка кодирования одной из целей использования сертификата"
322.	"Ошибка формирования расширения Key Usage"
323.	"Ошибка формирования расширения Authority Key Identifier"

№	Сообщение
324.	"Ошибка формирования расширения Subject Key Identifier"
325.	"Ошибка формирования расширения Basic Constraints"
326.	"Ошибка формирования расширения CRL Revoke Reason"
327.	"Ошибка формирования расширения CRLDistributionPoints"
328.	"Ошибка формирования расширения CRL Number"
329.	"Расширение CRL Distribution Points имеет некорректный формат"
330.	"Ошибка формирования расширения AuthorityInfoAccessSyntax"
331.	"Расширение AuthorityInfoAccessSyntax имеет некорректный формат"
332.	"Ошибка формирования расширения CertificatePolicies"
333.	"Расширение CertificatePolicies имеет некорректный формат"
334.	"Ошибка выпуска атрибутного сертификата"
335.	"Произошла ошибка в процессе формирования asn.1 структур привилегий атрибутного сертификата"
336.	"Ошибка формирования атрибута RoleSyntax"
337.	"Ошибка создания запроса на отзыв сертификата"
338.	"Ошибка разбора запроса на отзыв сертификата"
339.	"Ошибка создания ответа на запрос на отзыв сертификата"
340.	"Ошибка при попытке найти подключенное устройство"
341.	"Ошибка инициализации библиотеки pkcs11"
342.	"Ошибка получения списка слотов токена"
343.	"Ошибка открытия сессии для работы с токеном"
344.	"Ошибка авторизации на токене"
345.	"Ошибка вылогирования с токена"
346.	"Ошибка инициализации хэширования на токене"
347.	"Ошибка хэширования на токене"
348.	"Ошибка хэширования на токене при поточном обновлении"
349.	"Ошибка при получении хэш-значения на токене"
350.	"Ошибка инициализации создания подписи на токене"
351.	"Ошибка в процессе создания подписи на токене"
352.	"Ошибка инициализации проверки подписи на токене"
353.	"Ошибка в процессе проверки подписи на токене"
354.	"Ошибка инициализации поиска объектов на токене"
355.	"Ошибка поиска объектов на токене"
356.	"Ошибка при получении результата поиска объектов на токене"
357.	"Ошибка при получении значения атрибута объекта на токене"
358.	"Ошибка при установке значения атрибута объекта на токене"
359.	"Ошибка создания подписи в формате pkcs7 средствами токена"
360.	"Ошибка проверки подписи в формате pkcs7 средствами токена"
361.	"Ошибка генерации случайного значения ГСЧ токена"
362.	"Ошибка создания ключевой пары на токене"
363.	"Ошибка создания сессионного ключа на токене"
364.	"Ошибка при создании ключа согласования на токене"
365.	"Ошибка экспорта сессионного ключа на ключе согласования на токене"
366.	"Ошибка импорта сессионного ключа на ключе согласования на токене"
367.	"Ошибка инициализации операции шифрования на токене"
368.	"Ошибка операции шифрования на токене"
369.	"Ошибка окончания операции шифрования на токене"
370.	"Ошибка инициализации операции расшифрования на токене"
371.	"Ошибка операции расшифрования на токене"
372.	"Ошибка окончания операции шифрования на токене"

№	Сообщение
373.	"Ошибка операции создания объекта на токене"
374.	"Ошибка операции удаления объекта на токене"
375.	"Ошибка при создании запроса на сертификат на токене"
376.	"Ошибка при получении списка криптографических механизмов токена"
377.	"Ошибка при получении информации о криптографическом механизме токена"
378.	"Ошибка при сравнении хэш-значений документов"
379.	"Ошибка при проверке сигнатуры подписи"
380.	"Библиотека pkcs11 уже была проинициализирована"
381.	"Ошибка декодирования структуры асн"
382.	"Ошибка кодирования структуры асн"
383.	"Ошибка при конвертации строки"
384.	"Ошибка при конвертации объектного идентификатора"
385.	"На устройстве отсутствуют необходимые ключи"
386.	"Функции передано название неизвестного хранилища сертификатов"
387.	"Функции переданы неизвестные параметры"
388.	"Не найден закрытый ключ на токене"
389.	"Не найден открытый ключ на токене"
390.	"Ошибка при получении информации о подключенном слоте"
391.	"Ошибка при получении информации о подключенном токене"
392.	"Ошибка при загрузке библиотеки pkcs11"
393.	"Функции не передан ПИН-код для токена"
394.	"Недостаточно памяти для выполнения функции"
395.	"Неправильный идентификатор слота"
396.	"Критическая ошибка, связанная с аппаратным обеспечением"
397.	"При выполнении функции возник сбой"
398.	"Недопустимый аргумент"
399.	"Предпринята попытка присвоения значения атрибуту, который нельзя изменять"
400.	"Приложение не поддерживает защиту потоков от одновременного использования различными функциями"
401.	"Запрашиваемый атрибут недоступен для чтения"
402.	"Некорректный тип атрибута"
403.	"Атрибут нулевой длины"
404.	"Ошибка при обращении к устройству или слоту"
405.	"Для выполнения функции недостаточно памяти в устройстве"
406.	"При выполнении функции устройство было отключено"
407.	"Выбранный механизм не поддерживает расшифрование данных выбранной длины"
408.	"Выбранная функция не поддерживается модулем сопряжения или не найден дополнительный подключаемый модуль"
409.	"Функции передан некорректный дескриптор ключа"
410.	"Недопустимый размер ключа"
411.	"Данный тип ключа не может использоваться с заданным механизмом"
412.	"Ключ, используемый для выполнения криптографических операций, имеет атрибуты, не позволяющие использовать его для данных операций"
413.	"Ключ не может быть экспортирован"
414.	"При выполнении криптографической функции был указан неправильный механизм"
415.	"При выполнении криптографической функции были заданы некорректные параметры механизма"
416.	"Функции передан некорректный дескриптор объекта"
417.	"Одна или несколько выполняющихся операций препятствуют выполнению новой операции"
418.	"Выполнение операции без предварительного указания параметров невозможно"

№	Сообщение
419.	"Функции передан неверный ПИН-код"
420.	"Значение ПИН-кода содержит недопустимые символы"
421.	"Недопустимая длина ПИН-кода"
422.	"ПИН-код заблокирован"
423.	"При выполнении функции сеанс был закрыт"
424.	"Достигнуто предельное количество открытых сеансов для данного устройства"
425.	"Функции передан некорректный дескриптор сеанса"
426.	"Невозможно открыть параллельный сеанс"
427.	"Открыт сеанс работы с тем же устройством. Поэтому устройство не может быть инициализировано с помощью функции C_InitToken"
428.	"Открыт сеанс только для чтения. Смена режима невозможна"
429.	"Открыт сеанс чтения/записи. Открыть сеанс только для чтения невозможно"
430.	"Неправильное значение ЭП или имитовставки"
431.	"Значение ЭП неверно, по крайней мере, по длине"
432.	"Для создания объекта недостаточно атрибутов"
433.	"Заданные в шаблоне значения атрибутов противоречат друг другу"
434.	"В момент выполнения функции устройство было отключено"
435.	"Невозможно определить тип устройства, подключенного к слоту"
436.	"Устройство недоступно для записи"
437.	"Устройство уже работает в режиме, включение которого требует ввода данного ПИН-кода"
438.	"Неверный режим работы устройства"
439.	"Начальное значение ПИН-кода не установлено"
440.	"Задан некорректный режим работы с модулем сопряжения"
441.	"Переключение из режима администратора в режим пользователя или из режима пользователя в режим администратора невозможно"
442.	"Включение одновременно режимов пользователя и администратора невозможно"
443.	"Размер заданного буфера является недостаточным для сохранения результатов функции"
444.	"Запрашиваемый объект недоступен для чтения"
445.	"Выполнение функции без инициализации модуля сопряжения невозможно"
446.	"Повторная попытка инициализировать модуль сопряжения без предварительного выполнения функции C_Finalize"
447.	"Запрос ЭП отклонён пользователем"
448.	"Неизвестная ошибка"