

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00077-06-ЛУ

«ВАЛИДАТА КЛИЕНТ» ВЕРСИЯ 4

Описание применения

ВАМБ.00077-06 31 01

2020

Аннотация

Настоящий документ содержит описание применения программного комплекса (ПК) ВАМБ.00077-06 «“Валидата Клиент” версия 4» (далее — ПК «Валидата Клиент»).

Документ содержит описание назначения и структуры ПК «Валидата Клиент», объектов и справочников, используемых в ПК «Валидата Клиент», а также порядок визуализации и требования к реализации криптографических протоколов.

Содержание

1 НАЗНАЧЕНИЕ	5
2 СТРУКТУРА И СОСТАВ	6
2.1 Компоненты ПК «Валидата Клиент»	6
2.2 ПК «Справочник сертификатов»	6
2.3 Утилита командной строки	7
2.4 Расширение проводника	7
2.5 ПК «Автоматизированный клиент СКЗИ»	8
2.6 ПК «Автоматизированный клиент СКЗИ. Сервис»	9
2.7 ПК «Автоматизированный клиент СКЗИ. Монитор»	9
2.8 ПК «Автоматизированный клиент СКЗИ. Сервис монитор»	10
2.9 Библиотека прикладного программного интерфейса	10
2.10 Библиотека, реализующая протокол TLS, программа TLSProху и программа STunnel	11
3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ — БАЗОВЫЕ ОБЪЕКТЫ	13
3.1 Сертификат ключа проверки ЭП	13
3.2 Список аннулированных сертификатов	13
3.3 Запрос на создание сертификата ключа проверки ЭП	14
3.4 Сообщение о компрометации	14
4 ИСПОЛЬЗУЕМЫЕ СПРАВОЧНИКИ	15
4.1 Персональный справочник пользователя	15
4.2 Локальный справочник пользователя	15
4.3 Временные справочники в оперативной памяти	15
4.4 Сетевой справочник сертификатов	15
5 КЛЮЧЕВАЯ СИСТЕМА	16
5.1 Краткое описание системы управления сертификатами	16
5.1.1 Центр сертификации	16
5.1.2 Центр регистрации	16
5.1.3 Конечный пользователь	17
5.2 Сроки действия ключей и сертификатов	17
5.3 Регистрация пользователя	17
5.4 Плановая смена ключей	18
5.4.1 Получение сертификата при идентификации пользователя при личной явке	19
5.4.2 Получение сертификата при идентификации пользователя по действующим ключу ЭП и сертификату ключа проверки ЭП	19
5.4.3 Получение сертификата при идентификации пользователя с применением информационных технологий	19
5.5 Действия при компрометации ключей	20

6 ВИЗУАЛИЗАЦИЯ ПОДПИСЫВАЕМЫХ И ЗАЩИЩАЕМЫХ ДАННЫХ	21
6.1 Визуализация объектов СУС	21
6.2 Визуализация защищаемых данных	21
6.2.1 Общие требования к используемым форматам документов . . .	22
6.2.2 Общие требования к средствам просмотра документов	22
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	22
ПЕРЕЧЕНЬ РИСУНКОВ	24

1 НАЗНАЧЕНИЕ

Программный комплекс (ПК) ВАМБ.00077-06 «Валидата Клиент» версия 4» (далее — ПК «Валидата Клиент») обеспечивает возможность создания квалифицированных электронных подписей (ЭП) и квалифицированных сертификатов ключей проверки ЭП в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и требованиями приказов ФСБ России от 27.12.2011 № 795 и № 796.

ПК «Валидата Клиент» обеспечивает выполнение следующих задач:

- создание ключа ЭП и ключа проверки ЭП для конечных пользователей — клиентов Удостоверяющего центра (УЦ), эксплуатирующих средства криптографической защиты информации;
- формирование запросов конечных пользователей в Центр регистрации (ЦР) на создание сертификатов собственных ключей проверки ЭП, а также запросов на аннулирование/прекращение действия своих сертификатов;
- формирование/проверка ЭП блоков памяти и файлов;
- зашифрование и расшифрование блоков памяти и файлов;
- предоставление прикладного программного интерфейса для работы с сертификатами, формирования/проверки ЭП блоков памяти и файлов, зашифрования и расшифрования блоков памяти и файлов;
- реализация механизма простановки и проверки штампов времени ЭП;
- реализация механизма проверки статуса сертификата;
- обеспечение конфиденциальности информации, контроля целостности и подтверждения авторства электронных документов на основе использования электронных сертификатов ключей проверки ЭП и криптографических процедур, реализованных в соответствии с ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования», ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры», ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» и ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

2 СТРУКТУРА И СОСТАВ

2.1 Компоненты ПК «Валидата Клиент»

ПК «Валидата Клиент» содержит следующие компоненты:

- ПК «Справочник сертификатов», включающий исполняемый модуль командной строки, расширение проводника и программу STunnel. ПК «Справочник сертификатов» предназначен для формирования запросов на создание и аннулирование/прекращение действия сертификатов ключей проверки ЭП, простановки и проверки ЭП электронных документов, а также выполнения операций с базой данных сертификатов (справочниками сертификатов), создаваемой на рабочем месте пользователя, и управления профилями (настройками справочников сертификатов) пользователя;

- ПК «Автоматизированный клиент СКЗИ» (далее — ПК «АК СКЗИ»). ПК «АК СКЗИ» предназначен для автоматизации работы пользователя с криптографическими операциями;

- ПК «Автоматизированный клиент СКЗИ. Сервис» (далее — ПК «АК СКЗИ. Сервис»). ПК «АК СКЗИ. Сервис» предназначен для автоматизации работы пользователя с криптографическими операциями;

- ПК «Автоматизированный клиент СКЗИ. Монитор» (далее — ПК «АК СКЗИ. Монитор»). ПК «АК СКЗИ. Монитор» предназначен для просмотра журналов ПК «АК СКЗИ»;

- ПК «Автоматизированный клиент СКЗИ. Сервис монитор» (далее — ПК «АК СКЗИ. Сервис монитор»). ПК «АК СКЗИ. Сервис монитор» предназначен для просмотра журналов ПК «АК СКЗИ. Сервис»;

- комплект разработчика прикладного программного обеспечения, включающий библиотеку прикладного программного интерфейса работы с сертификатами ключей для операционной системы (ОС) Windows (для C/C++ и для платформы Microsoft .Net Framework), обеспечивающую возможность встраивания ПК «Валидата Клиент» в прикладное программное обеспечение, и библиотеку, реализующую протокол TLS;

- программа TLSProxy.

ПК «Валидата Клиент» функционирует совместно с ПК ВАНБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — криптопровайдер или ПК «Валидата CSP»).

2.2 ПК «Справочник сертификатов»

ПК «Справочник сертификатов» обеспечивает:

- формирование защищенного персонального справочника пользователя, содержащего сертификат Центра сертификации (ЦС);

- формирование личных ключей ЭП и ключей проверки ЭП пользователей УЦ с использованием различных ключевых носителей в соответствии с ГОСТ Р 34.10-2012;

- формирование запроса на создание сертификата в формате PKCS#10 с использованием созданного личного ключа ЭП и ключа проверки ЭП;

- передачу запроса в защищенном виде в ЦР;
- создание и проверку ЭП файлов в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- добавление и удаление сертификатов, списков аннулированных (отозванных) сертификатов (САС);
- проверку и отображение состояния сертификатов, связанного с окончанием их сроков действия или их аннулированием/прекращением действия;
- формирование и передачу в ЦР сообщения о компрометации ключа пользователя;
- отображение содержания и вывод на печать сертификатов, запросов, САС и сообщений о компрометации;
- обновление САС с использованием сетевого справочника сертификатов;
- восстановление персонального и локального справочника пользователя из резервной копии;
- возможность подключения к терминальному серверу через входящий в состав серверных ОС Windows шлюз терминальных серверов (Terminal Services Gateway);
- возможность подключения в режиме удаленного доступа к терминальным серверам, находящихся под управлением Citrix XenDesktop/XenApp версия 7, по сетевому каналу, защищенному шифрованием и аутентификацией по протоколу TLS. Защита подключения, выполняющегося по протоколу ICA (Independent Computing Architecture), выполняется с помощью входящей в состав ПК «Валидата Клиент» программы STunnel.

Примечание — Под списком аннулированных сертификатов понимается список аннулированных сертификатов и сертификатов, действие которых прекращено, за исключением, возможно, сертификатов, действие которых прекращено по причине истечения срока действия сертификата. Случаи аннулирования и прекращения действия сертификатов устанавливаются удостоверяющим центром.

2.3 Утилита командной строки

Утилита командной строки предназначена для осуществления доступа пользователей к криптографическим функциям из режима командной строки ОС Microsoft Windows. Утилита командной строки позволяет осуществлять шифрование/расшифрование информации, формирование/проверку подлинности ЭП, а также простановку/проверку штампов времени ЭП и проверку статуса сертификата. Утилита командной строки использует ПК «Справочник Сертификатов» для управления справочниками сертификатов.

Доступ пользователей к криптографическим функциям осуществляется через вызов утилиты с заданием параметров выполнения из режима командной строки.

2.4 Расширение проводника

Программный модуль «Расширение проводника» для ОС Windows встраивается в контекстное меню Проводника. Для работы расширения проводника тре-

буется установленный и настроенный ПК «Справочник сертификатов».

Расширение проводника позволяет выполнять следующие криптографические операции с группами файлов и каталогами через пункт контекстного меню Проводника ОС Windows:

- создание и проверка (с возможностью удаления) ЭП файлов (CMS сообщений) в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- зашифрование и расшифрование файлов в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик») в режиме гаммирования с возможностью выработки имитовставки;
- зашифрование и расшифрование файлов в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью в соответствии с RFC 4357 и RFC 4490;
- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-2012 (для хэш-значений длиной 256 бит).

2.5 ПК «Автоматизированный клиент СКЗИ»

ПК «АК СКЗИ» функционирует в качестве приложения, работающего в фоновом режиме.

ПК «АК СКЗИ» позволяет выполнять следующие функции в автоматическом режиме:

- создание и проверка (с возможностью удаления) ЭП файлов (CMS сообщений) в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- зашифрование и расшифрование файлов в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик») в режиме гаммирования с возможностью выработки имитовставки;
- зашифрование и расшифрование файлов в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью в соответствии с RFC 4357 и RFC 4490;
- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-2012 (для хэш-значений длиной 256 бит);
- реализация механизма простановки и проверки штампов времени ЭП в соответствии с RFC 3161;
- упаковка и распаковка файлов и папок в/из zip- или gzip- архивов;
- перемещение и удаление файлов;
- преобразование файлов в формат и из формата Base64;
- исполнение заданной командной строки с возможностью выбора исполняемого файла и параметров выполнения;
- ведение журнала выполненных операций.

Также ПК «АК СКЗИ» позволяет выполнять следующие функции в ручном режиме:

- настройка профилей, содержащих правила обработки файлов;
- настройка правил обработки файлов, в том числе добавление, редактирование, удаление, временное отключение правил и изменение порядка исполнения правил;
- экспорт правил в файл;

- импорт правил из файла;
- поиск правил по описанию;
- настройка пути записи журнала ПК «АК СКЗИ»;
- настройка списка подписантов.

2.6 ПК «Автоматизированный клиент СКЗИ. Сервис»

ПК «АК СКЗИ. Сервис» функционирует в качестве службы ОС Windows.

ПК «АК СКЗИ. Сервис» позволяет выполнять следующие функции в автоматическом режиме:

- создание и проверка (с возможностью удаления) ЭП файлов (CMS сообщений) в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- зашифрование и расшифрование файлов в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик») в режиме гаммирования с возможностью выработки имитовставки;
- зашифрование и расшифрование файлов в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью в соответствии с RFC 4357 и RFC 4490;
- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-2012 (для хэш-значений длиной 256 бит);
- реализация механизма простановки и проверки штампов времени ЭП в соответствии с RFC 3161;
- упаковка и распаковка файлов и папок в/из zip- или gzip- архивов;
- перемещение и удаление файлов;
- преобразование файлов в формат и из формата Base64;
- исполнение заданной командной строки с возможностью выбора исполняемого файла и параметров выполнения;
- ведение журнала выполненных операций.

Также ПК «АК СКЗИ. Сервис» позволяет выполнять следующие функции в ручном режиме:

- настройка профилей, содержащих правила обработки файлов;
- настройка правил обработки файлов, в том числе добавление, редактирование, удаление, временное отключение правил и изменение порядка исполнения правил;
- экспорт правил в файл;
- импорт правил из файла;
- поиск правил по описанию;
- настройка пути записи журнала «АК СКЗИ. Сервис»;
- настройка списка подписантов.

2.7 ПК «Автоматизированный клиент СКЗИ. Монитор»

ПК «АК СКЗИ. Монитор» выполняет следующие функции:

- просмотр краткого описания событий ПК «АК СКЗИ. Монитор» для каждого профиля ПК «АК СКЗИ», найденного в каталоге журнала;

- просмотр краткого описания ошибок ПК «АК СКЗИ. Монитор» для каждого профиля ПК «АК СКЗИ», найденного в каталоге журнала;
- просмотр подробного описания события/ошибки ПК «АК СКЗИ. Монитор»;
- уведомление о произошедшей ошибке;
- сброс записей журнала.

2.8 ПК «Автоматизированный клиент СКЗИ. Сервис монитор»

ПК «АК СКЗИ. Сервис монитор» выполняет следующие функции:

- просмотр краткого описания событий ПК «АК СКЗИ. Сервис монитор» для каждого профиля ПК «АК СКЗИ. Сервис», найденного в каталоге журнала;
- просмотр краткого описания ошибок ПК «АК СКЗИ. Сервис монитор» для каждого профиля ПК «АК СКЗИ. Сервис», найденного в каталоге журнала;
- просмотр подробного описания события/ошибки ПК «АК СКЗИ. Сервис монитор»;
- уведомление о произошедшей ошибке;
- сброс записей журнала.

2.9 Библиотека прикладного программного интерфейса

Библиотека прикладного программного интерфейса для работы с сертификатами ключей предназначена для предоставления программного интерфейса для работы с сертификатами и обеспечивает выполнение следующих функций:

- создание (генерация) ключей ЭП длиной 256 и 512 бит, а также соответствующих ключей проверки ЭП длиной 512 и 1024 бита согласно ГОСТ Р 34.10-2012;
- формирование первичного запроса на получение сертификата ключа проверки ЭП в формате PKCS#10;
- формирование непервичного запроса на плановую смену сертификата ключа проверки ЭП в формате PKCS#10+CMS/PKCS#7;
- формирование запроса на аннулирование сертификата ключа проверки ЭП;
- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-2012 (для хэш-значений длиной 256 и 512 бит);
- создание и проверка ЭП данных в соответствии с ГОСТ Р 34.10-2012 (для ключей ЭП длиной 256 и 512 бит);
- зашифрование и расшифрование файлов и блоков памяти в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик») в режиме гаммирования с возможностью выработки имитовставки;
- зашифрование и расшифрование файлов и блоков памяти в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью;
- создание и проверка ЭП файлов и блоков памяти в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-94 и про-

верку архивных ЭП в соответствии с ГОСТ Р 34.10-2001;

- реализация протокола безопасности транспортного уровня TLS версии 1.0;
- реализация протокола безопасности транспортного уровня TLS версии 1.2;
- реализация механизма простановки и проверки штампов времени ЭП;
- реализация механизма проверки статуса сертификата.

В состав библиотеки для C/C++ входят следующие файлы:

- `zpci1.dll` — модуль динамической библиотеки;
- `zpci1.lib` — модуль библиотеки для линковки с динамической библиотекой;
- `vcert1.h` — файл с описанием прототипов функций библиотеки;
- `vcerterr.h` — файл с определениями кодов возврата функций библиотеки.

В состав библиотеки для платформы Microsoft .Net Framework входит модуль динамической библиотеки `vspia2.dll`.

2.10 Библиотека, реализующая протокол TLS, программа TLSProхy и программа STunnel

Программа STunnel, используя библиотеку, реализующую протокол TLS, позволяет создавать TLS-туннель, обеспечивающий криптографическую защиту произвольного TCP-соединения посредством оборачивания (инкапсуляции) этих данных протоколом TLS.

Программа TLSProхy, которая является аналогом программы STunnel, также предназначена для защиты данных, передаваемых по TCP соединениям, посредством оборачивания (инкапсуляции) этих данных протоколом TLS. В отличие от программы STunnel, программа TLSProхy всегда выполняет двухстороннюю аутентификацию (проверяет цепочку сертификата противоположной стороны), а также имеет возможность фильтровать (блокировать) TLS соединения на основании данных сертификатов противоположной стороны.

ПК «Валидата Клиент» обеспечивает выполнение следующих функций поддержки протокола TLS:

- создание защищённого канала связи (с обеспечением контроля целостности передаваемой информации) между сервером и клиентом с использованием шифрования информации в соответствии с ГОСТ 28147-89 для протокола TLS 1.0 (согласно RFC 2246);
- создание защищённого канала связи (с обеспечением контроля целостности передаваемой информации) между сервером и клиентом с использованием шифрования информации в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочный шифр «Кузнечик») для протокола TLS 1.2 (согласно RFC 5246);
- аутентификация сервера клиентом посредством вычисления ключа парной связи по способу Диффи-Хеллмана с использованием пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10-2012;
- аутентификация клиента сервером посредством вычисления ЭП в соответствии с ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012;
- вычисление расширенного мастер-секрета в соответствии с RFC 7627 для протокола TLS 1.2;

– выполнение безопасного переподключения в соответствии с RFC 5746.

Программы STunnel и TLSProxy могут использоваться в тех случаях, когда отсутствует возможность использования внутренних механизмов ОС для обеспечения защиты передаваемых данных с помощью сертифицированной реализации протокола TLS.

Например, использование криптопровайдера обеспечивает защиту данных, передаваемых по протоколу HTTPS между Web-браузером Internet Explorer и Web-сервером Internet Information Server. В данном конкретном случае криптопровайдер позволяет использовать внутренние механизмы ОС для обеспечения защиты — а именно, инкапсуляцию данных протокола HTTP в сертифицированную реализацию протокола TLS. Эта возможность реализована за счет того, что, во-первых, криптопровайдер встраивается в пакет безопасности SChannel (отвечающий за функционирование протокола TLS в ОС Windows), и, во-вторых, Internet Explorer/Internet Information Server обращаются к пакету безопасности SChannel для обеспечения защищенной передачи данных.

В случае применения стороннего Web-браузера — например, Mozilla FireFox — использование внутреннего механизма ОС является невозможным, поскольку Mozilla FireFox не обращается к пакету безопасности SChannel для обеспечения защищенной передачи данных. Дополнительно, Mozilla ForeFox не включает в себя встроенную сертифицированную реализацию протокола TLS. Именно в этом случае программа STunnel/TLSProxy оказывается полезной — ее следует настроить и запустить на ЭВМ клиента в режиме прокси-клиента, к которому будет подключаться (без применения защиты) Mozilla FireFox. Прокси-клиент, в свою очередь, будет устанавливать защищенное соединение (TCP соединение, обернутое протоколом TLS) с Web-сервером. Таким образом, обмен данными между ЭВМ клиента и сервера оказывается защищенным посредством использования сертифицированной реализации протокола TLS.

Аналогичная ситуация возникает при применении стороннего Web-сервера — например Apache. В этом случае программу STunnel/TLSProxy следует настроить и запустить в режиме прокси-сервера, к которому подключается Web-браузер, организуя защищенное соединение. Прокси-сервер, в свою очередь, устанавливает открытое соединение с Web-сервером. Следует обратить внимание на то, что прокси-сервер может функционировать как на той же ЭВМ, что и Web-сервер, так и на специально выделенной ЭВМ — при этом, во втором варианте сетевой трафик между прокси-сервером и Web-сервером будет передаваться по вычислительной сети в открытом виде. Дополнительно, для обеспечения повышенной отказоустойчивости серверной подсистемы, можно запустить несколько экземпляров прокси-сервера на балансирующем или отказоустойчивом кластере, состоящем из множества ЭВМ.

Примечание — Сертификаты сервера и клиента, используемые в программе STunnel, необходимо формировать в соответствии с требованиями, изложенными в документе ВАНБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора». Сертификаты сервера и клиента, используемые в программе TLSProxy, необходимо формировать в соответствии с требованиями, изложенными в документе ВАНБ.00077-06 91 06 «“Валидата Клиент” версия 4. Программа TLSProxy. Руководство по установке и настройке».

3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ — БАЗОВЫЕ ОБЪЕКТЫ

К базовым объектам ПК «Валидата Клиент» (объектам, используемым в процессе управления сертификатами, т.е. фактически входным и выходным данным) относятся:

- сертификат ключа проверки ЭП;
- список аннулированных сертификатов;
- запрос на создание сертификата ключа проверки ЭП;
- сообщение о компрометации;
- упакованные данные.

3.1 Сертификат ключа проверки ЭП

Сертификат ключа проверки ЭП представляет собой структурированную двоичную запись в формате ASN.1, состоящую из:

- имени субъекта или объекта системы, однозначно идентифицирующего его в системе;
- ключа проверки ЭП субъекта или объекта системы;
- дополнительных атрибутов, определяемых требованиями использования сертификата в системе;
- ЭП издателя (Центра сертификации), заверяющей совокупность перечисленных выше данных.

Формат сертификата определен в рекомендациях ITU-T 1997 года [X.509] и рекомендациях IETF 2008 года [RFC 5280]. В настоящее время основным принятым форматом является формат версии 3, позволяющий определить дополнения (extensions), с помощью которых реализуется определенная политика безопасности в системе.

3.2 Список аннулированных сертификатов

CAC представляет собой структурированную двоичную запись в формате ASN.1, состоящую из:

- имени издателя (Центра сертификации), выпустившего CAC;
- даты выпуска CAC и опциональной даты обновления CAC;
- дополнительных атрибутов, которые могут быть включены в CAC;
- списка элементов, каждый из которых включает ссылку на аннулируемый/прекращающий действие сертификат, и дополнительной информации о нем и причинах его аннулирования/прекращения действия;
- ЭП издателя, заверяющей совокупность этих данных.

Формат CAC определен в рекомендациях ITU-T 1997 года [X.509] и рекомендациях IETF 2008 года [RFC 5280]. В настоящее время основным принятым форматом является формат CAC версии 2.

3.3 Запрос на создание сертификата ключа проверки ЭП

Запрос на создание сертификата ключа проверки ЭП представляет собой структурированную двоичную запись в формате ASN.1, состоящую из:

- имени субъекта или объекта системы, однозначно идентифицирующего его в системе;
- ключа проверки ЭП субъекта или объекта системы;
- дополнительных атрибутов, которые могут быть включены в сертификат;
- ЭП субъекта или объекта системы на ключе ЭП, соответствующем ключу проверки ЭП в запросе, заверяющей совокупность этих данных.

В соответствии с международной практикой запрос на создание сертификата оформляется по стандарту PKCS#10 [PKCS-10, RFC 2986].

3.4 Сообщение о компрометации

Сообщение о компрометации представляется в виде структурированной двоичной записи в формате ASN.1, состоящей из:

- аннулируемого/прекращающего действие сертификата;
- даты и кода мотивации аннулирования/прекращения действия сертификата;
- заверяющей совокупность этих данных ЭП субъекта или объекта системы на ключе ЭП, соответствующем аннулируемому/прекращающему действие сертификату.

4 ИСПОЛЬЗУЕМЫЕ СПРАВОЧНИКИ

ПК «Валидата Клиент» обеспечивает работу со следующими видами справочников:

- персональный справочник пользователя;
- локальный справочник пользователя;
- временный справочник в оперативной памяти;
- сетевой справочник сертификатов.

4.1 Персональный справочник пользователя

Персональный справочник пользователя (ПСП) — защищенное хранилище, содержащее сертификаты доверенных (корневых) ЦС. ПСП защищен ЭП, вычисленной при его формировании на ключе ЭП пользователя. Проверка ЭП ПСП выполняется на сертификате ключа проверки ЭП пользователя. Для хранения ПСП может использоваться файл - подписанное CMS-сообщение, а также системное хранилище сертификатов ОС Microsoft Windows.

4.2 Локальный справочник пользователя

Локальный справочник пользователя (ЛСП) — незащищенное хранилище, содержащее сертификаты ЦС второго и более низких уровней, САС ЦС любых уровней, сертификаты ЦР, рабочий сертификат, запросы PKCS#10, запросы на аннулирование/прекращение действия, а также сторонние сертификаты. Для хранения ЛСП могут использоваться базы данных GDBM и ODBC, а также системное хранилище сертификатов ОС Microsoft Windows.

4.3 Временные справочники в оперативной памяти

Временные справочники по своему функциональному назначению аналогичны локальному справочнику пользователя, за исключением того, что они создаются в оперативной памяти и могут быть использованы как кэш объектов для увеличения производительности системы.

4.4 Сетевой справочник сертификатов

Сетевой справочник сертификатов (ССС) — незащищенное хранилище (опциональное), содержащее сертификаты ЦС второго и более низких уровней, САС ЦС любых уровней, сертификаты ЦР, а также сторонние сертификаты. Доступ к СССР осуществляется по стандартному протоколу **Lightweight Directory Access Protocol (LDAP)**.

5 КЛЮЧЕВАЯ СИСТЕМА

5.1 Краткое описание системы управления сертификатами

Систему управления сертификатами (СУС) образуют УЦ и конечные пользователи. В свою очередь, УЦ включает следующие компоненты:

- Центр сертификации (ЦС);
- Центр регистрации (ЦР);
- Сетевой справочник сертификатов (подраздел 4.4).

5.1.1 Центр сертификации

К основным функциям ЦС в части, касающейся конечных пользователей, относятся:

- выпуск сертификатов ключей проверки ЭП пользователей по запросам от ЦР своего уровня и САС;
- ведение базы всех, изготовленных данным ЦС, сертификатов и САС (в течение установленного срока хранения) и их резервное копирование.

5.1.2 Центр регистрации

ЦР является единственной точкой входа (регистрации) участников системы. Только зарегистрированный в ЦР пользователь может получить сертификат ключа проверки ЭП, соответствующий своему ключу ЭП.

Основные функции ЦР:

- регистрация новых пользователей системы и формирование для них ключей ЭП и ключей проверки ЭП;
- получение, регистрация и обработка запросов на создание сертификатов ключей проверки ЭП от пользователей системы;
- создание и отправка в ЦС запросов на выпуск сертификатов ключей проверки ЭП пользователей системы;
- формирование шаблонов сертификатов ключей проверки ЭП на основе полученных запросов с добавлением в них атрибутов пользователя в виде дополнений X.509;
- получение и обработка сообщений от пользователей о компрометации их ключей;
- администрирование ССС;
- организация оперативного оповещения пользователей обо всех изменениях, происходящих в сети (о компрометации ключей, восстановлении связи после компрометации ключей, включении новых пользователей, плановой смене ключей и т.п.), и поддержка его функционирования;
- разбор конфликтных ситуаций и доказательство авторства электронного документа, снабженного ЭП.

5.1.3 Конечный пользователь

Конечный пользователь — это объект автоматизированных систем, являющийся владельцем сертификата. В качестве ПО конечного пользователя используется ПК «Валидата Клиент».

5.2 Сроки действия ключей и сертификатов

Сроки действия ключей и сертификатов в зависимости от условий эксплуатации приведены в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

5.3 Регистрация пользователя

Общая схема регистрации пользователя приведена ниже (Рисунок 1).

Ключ ЭП и запрос на создание сертификата может быть создан как самим пользователем, так и Администратором или Оператором ЦР в процессе регистрации пользователя.

В первом случае пользователь на своём рабочем месте создаёт ключ ЭП, а также запрос на создание сертификата в формате PKCS#10. Далее пользователь системы (или доверенное лицо) прибывает в ЦР с документами, необходимыми для регистрации пользователя в системе в соответствии с регламентом эксплуатирующей организации, а также с запросом на создание сертификата на отчуждаемом носителе.

Во втором случае пользователь (или его доверенное лицо) прибывает в ЦР только с документами, необходимыми для регистрации.

Администратор или Оператор ЦР проверяет предоставленные пользователем документы и, в случае успешной проверки, производит регистрацию пользователя. Если пользователь создал свой ключ ЭП и запрос на выпуск сертификата на рабочем месте, Администратор или Оператор ЦР производит проверку предоставленного запроса на выпуск сертификата, в противном случае Администратор или Оператор ЦР самостоятельно создаёт ключ ЭП для пользователя, а также формирует запрос на создание сертификата.

После проверки (формирования) запроса Администратор или Оператор ЦР отправляет его в ЦС. После выпуска сертификата ЦС пересылает его в ЦР, откуда сертификат может быть отправлен пользователю по электронной почте или выдан ему при личной явке в ЦР.

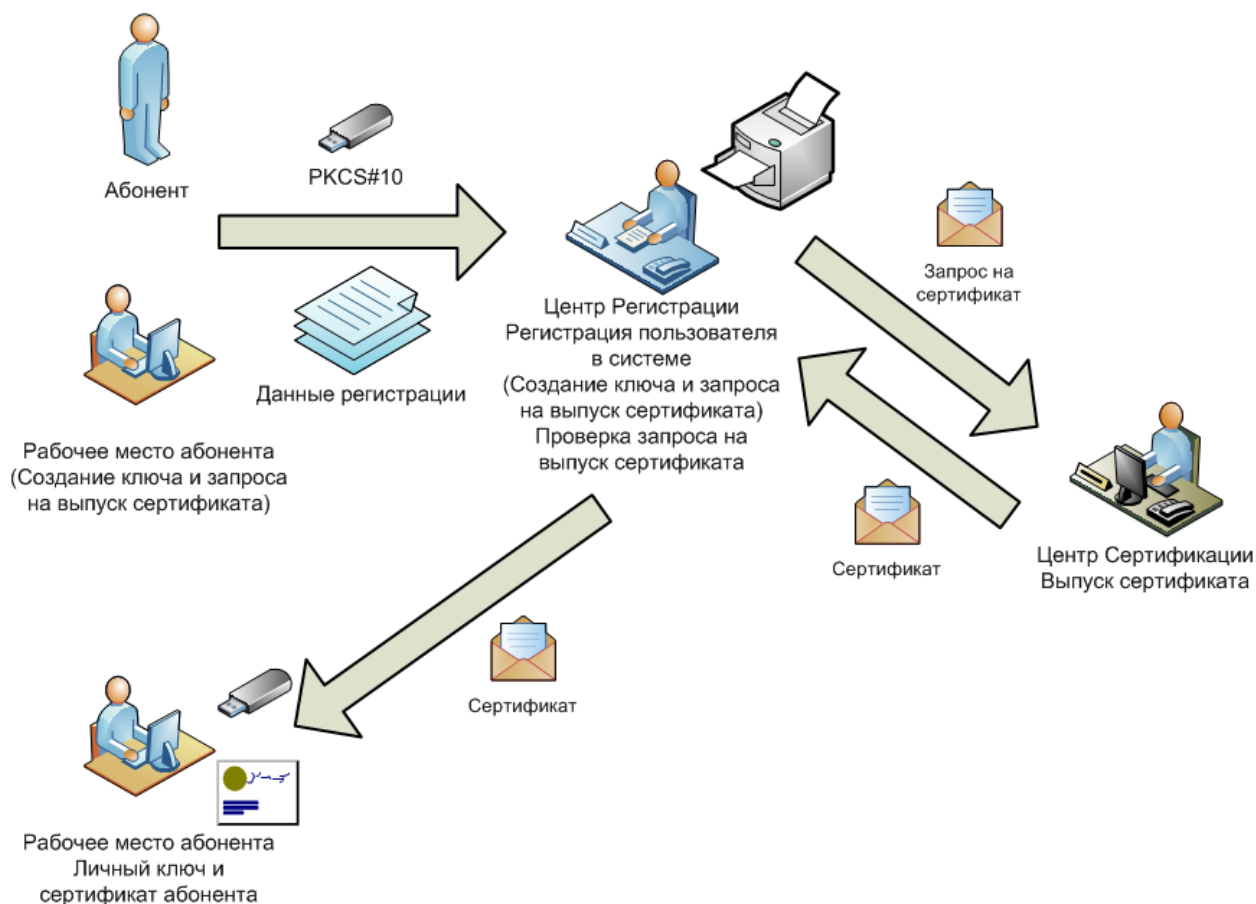


Рисунок 1 – Регистрация пользователя

5.4 Плановая смена ключей

Пользователь, имеющий действующий ключ ЭП и соответствующий ему сертификат ключа проверки ЭП, до окончания срока действия данного ключа ЭП должен провести процедуру плановой смены, т.е. сформировать новый ключ ЭП и соответствующий ему запрос на получение сертификата, и на основании последнего получить сертификат ключа проверки ЭП в УЦ.

Конкретные способы получения нового сертификата ключа проверки ЭП, в том числе порядок использования запросов на бумажных носителях и требования к их заверению, определяются УЦ, в котором зарегистрирован пользователь, и указываются в регламенте или другом нормативном документе УЦ.

При получении нового сертификата ключа проверки ЭП пользователь добавляет его в локальный справочник сертификатов (при его использовании).

Незадолго до окончания действия текущего рабочего ключа ЭП пользователь делает рабочими новый ключ ЭП и соответствующий ему новый сертификат ключа проверки ЭП.

После окончания срока действия старого рабочего ключа ЭП необходимо незамедлительно уничтожить старый ключ ЭП средствами ПК «Валидата Клиент».

Ниже в настоящем подразделе описаны возможные способы получения пользователем нового ключа ЭП и соответствующего ему сертификата ключа проверки ЭП исходя из функционала, предоставляемого ПК «Валидата Клиент» и возможных способов идентификации пользователя.

5.4.1 Получение сертификата при идентификации пользователя при личной явке

В данном разделе описаны способы создания сертификата ключа проверки ЭП пользователя, при которых его идентификация выполняется при личной явке в ЦР. При этом ключ ЭП и запрос на получение сертификата ключа проверки ЭП могут быть сформированы одним из следующих способов:

- Администратором или Оператором ЦР в присутствии пользователя при личной явке в ЦР;
- пользователем самостоятельно, при этом запрос на создание сертификата формируется в формате PKCS#10;
- при наличии действующих ключа ЭП и соответствующего ему сертификата ключа проверки ЭП пользователем, с подписанием запроса в формате PKCS#10 с использованием действующего ключа ЭП (в формате PKCS#10+CMS/PKCS#7).

В случае если пользователь сам формирует запрос на получение нового сертификата ключа проверки ЭП (в формате PKCS#10 или PKCS#10+CMS/PKCS#7), он должен принести его в ЦР в электронном виде на отчуждаемом носителе.

Выпущенный сертификат пользователь получает по каналам связи (например, по электронной почте) или «из рук в руки» при личной явке в ЦР.

5.4.2 Получение сертификата при идентификации пользователя по действующим ключу ЭП и сертификату ключа проверки ЭП

Для получения сертификата данным способом пользователь должен:

- сформировать новый ключ ЭП и запрос на создание нового сертификата ключа проверки ЭП в формате PKCS#10;
- подписать запрос с использованием действующего ключа ЭП (в формате PKCS#10+CMS/PKCS#7);
- передать его в УЦ по каналам связи, например, по электронной почте.

В данном случае идентификация пользователя в УЦ будет проходить исключительно по ЭП, выполненной с использованием действующего ключа ЭП пользователя.

Выпущенный сертификат пользователь получает по каналам связи (например, по электронной почте) или «из рук в руки» при личной явке в ЦР.

Проведение пользователем двух (и более) подряд плановых смен данным способом не допускается.

5.4.3 Получение сертификата при идентификации пользователя с применением информационных технологий

В случае если УЦ, в котором зарегистрирован пользователь, является аккредитованным, он должен предоставить пользователю возможность идентификации с применением информационных технологий способами, перечисленными в пункте 1 статьи 13 Федерального закона № 63-ФЗ «Об электронной подписи». При этом для защиты передаваемых биометрических персональных данных пользователь обязан использовать шифровальные (криптографические) сред-

ства, предоставляемые УЦ, иначе ему будет отказано в проведении идентификации.

При использовании данного способа идентификации:

- пользователь может самостоятельно сформировать новый ключ ЭП и соответствующий ему запрос на создание нового сертификата ключа проверки ЭП в формате PKCS#10;

- при наличии действующих ключа ЭП и соответствующего ему сертификата ключа проверки ЭП, пользователь может сформировать новый ключ ЭП и запрос на создание нового сертификата ключа проверки ЭП в формате PKCS#10, и подписать запрос с использованием действующего ключа ЭП (в формате PKCS#10+CMS/PKCS#7).

Сформированный одним из указанных выше способов запрос передается в УЦ установленным порядком.

Выпущенный сертификат пользователь получает по каналам связи (например, по электронной почте) или «из рук в руки» при личной явке в ЦР.

5.5 Действия при компрометации ключей

При компрометации ключа у пользователя он должен немедленно прекратить связь по сети с другими пользователями.

Пользователь (или администратор информационной безопасности организации) должен немедленно известить УЦ о компрометации ключей пользователя.

При наличии сетевого взаимодействия пользователь может оповестить УЦ путем формирования сообщения о компрометации с помощью ПК «Валидата Клиент».

Далее пользователь формирует новый ключ ЭП, а также запрос на создание сертификата ключа проверки ЭП. Так как пользователь не может использовать скомпрометированный ключ для формирования ЭП и передачи запроса в защищённом виде по сети, сформированный запрос вместе с бланками доставляется лично пользователем (или администратором информационной безопасности) в ЦР или же доставка запроса выполняется по дополнительным защищенным каналам связи.

6 ВИЗУАЛИЗАЦИЯ ПОДПИСЫВАЕМЫХ И ЗАЩИЩАЕМЫХ ДАННЫХ

В данном разделе изложен порядок визуализации в ПК «Валидата Клиент» данных, подлежащих подписанию посредством ЭП, и данных, ЭП которых проверяется. Под визуализацией данных понимается отображение данных на экране в формате, обеспечивающем просмотр этих данных лицом, осуществляющим подписание данных или проверку их ЭП.

Предписываемый ниже порядок визуализации направлен на выполнение требований, установленных п. 8 и п. 9 «Требований к средствам электронной подписи», утвержденных приказом ФСБ России от 27.12.2011 № 796 (далее — требования к визуализации).

Требования к визуализации не применяются в случае использования ПК «Валидата Клиент» для автоматического создания и (или) автоматической проверки ЭП.

6.1 Визуализация объектов СУС

Требования по визуализации относятся к следующим объектам СУС:

- справочники сертификатов ключей проверки ЭП;
- сертификаты ключей проверки ЭП;
- запросы на создание сертификата ключей проверки ЭП;
- списки аннулированных сертификатов;
- запросы на аннулирование/прекращение действия сертификата;
- сообщения о компрометации ключей ЭП.

Под визуализацией объектов СУС понимается отображение состава этих объектов, т.е. значений полей структуры объектов, предусмотренных соответствующими стандартами. Визуализация данных объектов осуществляется с помощью соответствующих опций и вкладок графического пользовательского интерфейса ПК «Валидата Клиент». Подробно порядок визуализации объектов СУС изложен в документе ВАМБ.00076-03 31 01 «АПК «Валидата УЦ» версия 3.1». Описание применения».

6.2 Визуализация защищаемых данных

В настоящем разделе приведены сведения о форматах документов и средствах просмотра документов, обеспечивающих выполнение требований к визуализации в случае использования утилиты командной строки, Мастера установки ЭП или Мастера проверки ЭП из состава ПК «Валидата Клиент» для подписания и проверки ЭП файлов, а также если пользователь в ручном режиме отправляет файлы на обработку ПК «АК СКЗИ» или ПК «АК СКЗИ. Сервис».

Пользователь должен просмотреть документ перед его подписанием или после проверки его ЭП в случае использования утилиты командной строки, Мастера установки ЭП или Мастера проверки ЭП. Если пользователь в ручном режиме отправляет файлы на обработку ПК «АК СКЗИ» или ПК «АК СКЗИ. Сервис», он должен просмотреть документы перед их отправкой на подписание в ПК

«АК СКЗИ» или ПК «АК СКЗИ. Сервис» или после завершения проверки их ЭП в ПК «АК СКЗИ» или ПК «АК СКЗИ. Сервис».

Порядок использования утилиты командной строки приведен в документе ВАМБ.00077-06 92 02 «“Валидата Клиент” версия 4. Исполняемый модуль командной строки. Руководство пользователя».

Порядок использования Мастера установки ЭП и Мастера проверки ЭП приведен в документе ВАМБ.00077-06 92 01 «“Валидата Клиент” версия 4. Справочник сертификатов. Руководство пользователя».

Порядок использования ПК «АК СКЗИ» приведен в документе ВАМБ.00077-06 92 03 «“Валидата Клиент” версия 4. Автоматизированный клиент СКЗИ. Руководство пользователя». Порядок использования ПК «АК СКЗИ. Сервис» приведен в документе ВАМБ.00077-06 92 04 «“Валидата Клиент” версия 4. Автоматизированный клиент СКЗИ. Сервис. Руководство пользователя».

6.2.1 Общие требования к используемым форматам документов

При подписании и проверке ЭП электронный документ должен быть представлен в форматах ODF, XML или PDF.

6.2.2 Общие требования к средствам просмотра документов

Просмотр документов при их подписании и проверке их ЭП необходимо выполнять с помощью следующих удовлетворяющих требованиям ФСБ России программных средств:

- для файлов формата XML — Microsoft Internet Explorer версии 11.0, Microsoft Edge версии 40.15063 и выше, Mozilla Firefox (68.0 или более новый), Google Chrome (79.0 или более новый), Chromium GOST (96 или более новый), Яндекс Браузер (22.9 или более новый);

- для файлов форматов ODF — Microsoft Office (Word) 2013 или выше;

- для файлов формата PDF — Adobe Acrobat (Reader) версии 15.0 или выше.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ДСЧ	Датчик случайных чисел
ЛСП	Локальный справочник пользователя
ОС	Операционная система
ПК	Программный комплекс
ПСП	Персональный справочник пользователя
САС	Список аннулированных сертификатов
СКЗИ	Средство криптографической защиты информации
ССС	Сетевой справочник сертификатов
СУС	Система управления сертификатами
УЦ	Удостоверяющий центр
ЦР	Центр регистрации
ЦС	Центр сертификации
ЭП	Электронная подпись

ПЕРЕЧЕНЬ РИСУНКОВ

1	Регистрация пользователя	18
---	------------------------------------	----

[illegible][illegible]