ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-06–ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВАЛИДАТА CSP» ВЕРСИЯ 6

Описание применения

ВАМБ.00060-06 31 01

2020

Аннотация

Данный документ содержит сведения для применения программного комплекса (ПК) ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее по тексту — СКЗИ «Валидата CSP»).

Содержание

1 ВЫПОЛНЯЕМЫЕ ФУНКЦИИ

СКЗИ «Валидата CSP» включает:

– криптографический провайдер;

– программный модуль поддержки TLS;

– программный модуль «Графический Интерфейс Пользователя Сервисов» (далее — ПМ ГИПС);

– утилиту загрузки инициализационной последовательности датчика случайных чисел функционального ключевого носителя.

Криптопровайдер СКЗИ «Валидата CSP» обеспечивает выполнение следующих низкоуровневых криптографических функций, соответствующих интерфейсу Microsoft Windows Cryptographic Service Provider (CSP), в соответствии с государственными стандартами, приведёнными в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр»:

– создание ключей электронной подписи (ЭП) и вычисление ключей проверки ЭП (для ключей ЭП длиной 256 и 512 бит);

– создание и проверка ЭП;

– выполнение зашифрования и расшифрования данных;

– выработка имитовставки данных;

– вычисление ключа парной связи Диффи-Хеллмана с использованием пар закрытых и открытых ключей;

– вычисление хэш-функции данных (для хэш-значений длиной 256 и 512 бит);

– выработка случайного числа заданной длины.

Примечание — В случае когда в сертификате ключа проверки ЭП разрешено использование ключа ЭП для шифрования («Согласование ключей»), ключ ЭП является также закрытым ключом шифрования, а ключ проверки ЭП — открытым ключом шифрования.

Программный модуль поддержки TLS криптопровайдера СКЗИ «Валидата CSP» 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 для протокола TLS 1.0;

– создание защищённого канала связи (с обеспечением контроля целостности передаваемой информации) между сервером и клиентом с использованием шифрования информации для протокола TLS 1.2;

– аутентификация сервера клиентом посредством вычисления ключа парной связи по способу Диффи-Хеллмана с использованием пар закрытых и открытых ключей;

– аутентификация клиента сервером посредством вычисления ЭП;

– вычисление расширенного мастер-секрета для протокола TLS 1.2;

– выполнение безопасного переподключения;

– обеспечения начальной аутентификации клиента в домене Microsoft Active Directory по протоколу Kerberos PKInit посредством вычисления ЭП.

ПМ ГИПС предназначен для вывода на экран некоторых диалоговых окон СКЗИ «Валидата CSP» от процессов, запущенных как сервис (служба) с правами системной учётной записи. Необходимость использования ПО ГИПС в СКЗИ «Валидата CSP» вызвана тем, что в операционной системе (ОС) Windows 10 вывод диалоговых окон сервисов (служб) напрямую невозможен.

Настройка и использование ПМ ГИПС описаны в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

Утилита загрузки инициализационной последовательности датчика случайных чисел (ДСЧ) функционального ключевого носителя (ФКН) предоставляет пользователю возможность инициализации программного ДСЧ ФКН «Валидата vdToken» и ФКН «Валидата vdToken» версия 2.0.

Подробнее работа с утилитой загрузки инициализационной последовательности ДСЧ ФКН описана в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

2 ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Защита данных с помощью криптографических преобразований — одно из возможных средств, применяемых для обеспечения безопасности информации. Применение криптографии позволяет обеспечить надёжную защиту данных при условии сохранения в тайне ключа криптографического преобразования.

Для эффективного решения проблемы защиты информации необходимо применение целого комплекса мер, который включает в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление правил для обслуживающего персонала, допущенного к работе с информацией ограниченного доступа.

Основными компонентами криптографической защиты являются:

– данные — защищаемая информация (текст, видеоизображение и т.д.) представляется в виде бинарной последовательности (далее — данные или сообщение);

– криптографическое преобразование — под криптографическим преобразованием понимают преобразование данных при помощи алгоритма шифрования, выработки электронной подписи или выработки имитовставки. Можно считать, что характер криптографического преобразования известен всем, но в то же время, не зная ключа, с помощью которого пользователем было выполнено преобразование данных, практически невозможно восстановить содержание сообщения или подделать электронную подпись/имитовставку, т.к. это требует выполнения за короткое время (пока еще информация имеет значимую ценность) неосуществимого объема вычислительной работы на самых современных ЭВМ;

– ключ (ключ связи) — конкретное значение некоторых параметров алгоритма криптографического преобразования данных, которое хранится в секрете. В СКЗИ «Валидата CSP» ключ представляет собой бинарную последовательность длины 256 или 512 бит.

СКЗИ «Валидата CSP» реализует следующие криптографические преобразования:

– шифрование данных, которое производится с целью скрыть содержание сообщения. Зашифрованное сообщение переводится в открытое сообщение с помощью соответствующего ключа (ключа расшифрования);

– имитозащита данных, обеспечивающая надежное установление фактов случайного или преднамеренного искажения информации в процессе её хранения или передачи по каналам связи;

– электронная подпись (ЭП), подтверждающая авторство и целостность электронных данных.

Шифрование данных и выработка имитовставки

Термин «шифрование» объединяет в себе два процесса: зашифрование и расшифрование информации.

Исходными данными в процессе зашифрования является сообщение, а результирующими — зашифрованное сообщение. В процессе расшифрования они меняются местами: исходнными данными является зашифрованное сообщение, а результирующими — расшифрованное (исходное) сообщение.

Если зашифрование и расшифрование осуществляются с использованием одного и того же ключа, то такой алгоритм криптографического преобразования называется симметричным, в противном случае — асимметричным.

В СКЗИ «Валидата CSP» используются симметричные алгоритмы криптографического преобразования данных, определенные ГОСТ Р 34.12-2015 (блочные шифры «Магма» и «Кузнечик»). Данные алгоритмы предназначены для аппаратной и аппаратно-программной реализации и удовлетворяют требованиям сертифицирующей организации.

В СКЗИ «Валидата CSP» используется механизм открытого распределения ключей, при котором для формирования симметричного ключа связи используется пара асимметричных ключей: открытый и закрытый ключи шифрования.

Важно исключить доступ к ключам шифрования посторонних лиц, так как любой, кто обладает ключом шифрования, может прочитать зашифрованное данным ключом сообщение.

ГОСТ Р 34.13-2015 предусматривает несколько режимов работы алгоритмов блочного шифрования. В СКЗИ «Валидата CSP» используется алгоритм шифрования, основанный на принципе гаммирования, который подразумевает процесс «наложения» по определённому закону (сложения по некоторому модулю) гаммы шифра на открытые данные (под гаммой понимается псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму).

ГОСТ Р 34.13-2015 также определяет процесс выработки имитовставки. Имитовставка обеспечивает защиту информации от случайных или преднамеренных искажений.

Имитовставка передается по каналу связи вместе с зашифрованным сообщением. Поступившие зашифрованные данные расшифровываются, и из полученных блоков данных вырабатывается контрольная имитовставка, которая затем сравнивается с имитовставкой, полученной по каналу связи. В случае несовпадения имитовставок все расшифрованные данные считаются ложными.

Формирование и проверка ЭП

ЭП — бинарная последовательность, зависящая от самого сообщения и от некоторого закрытого, известного только подписывающему субъекту, ключа (ключа ЭП). При этом проверка подписи возможна без получения доступа к ключу ЭП. ЭП позволяет на основе криптографических методов надёжно установить авторство и подлинность электронного документа.

ЭП позволяет заменить при безбумажном документообороте традиционную

печать и подпись. При построении ЭП вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между электронным документом, ключом ЭП и ключом проверки ЭП. Практическая невозможность подделки ЭП опирается на очень большой объём определённых математических вычислений.

Подписание электронного документа ЭП не меняет самого документа, она только даёт возможность проверить подлинность и авторство полученной информации.

В СКЗИ «Валидата CSP» реализована ЭП на базе криптографических алгоритмов, соответствующих ГОСТ Р 34.10-2012.

Механизм ЭП предполагает наличие у подписывающего сообщение субъекта ключа ЭП и ключа проверки ЭП.

Ключ ЭП используется для выработки ЭП и должен сохраняться пользователем в тайне.

Ключ проверки ЭП вычисляется как значение некоторой функции от ключа ЭП, но знание ключа проверки ЭП не даёт возможности определить ключ ЭП. Ключ проверки ЭП может быть опубликован и использоваться для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны владельца ключа ЭП в виде его отказа от подписи документа.

При работе с СКЗИ «Валидата CSP» каждый пользователь, обладающий правом подписи, самостоятельно формирует или получает в Удостоверяющем Центре (УЦ) личные ключ ЭП (на отчуждаемом носителе) и ключ проверки ЭП (в составе сертификата ключа проверки ЭП, издаваемого УЦ).

При выработке ЭП вначале производится хэширование документа в соответствии с ГОСТ Р 34.11-2012. Хэш-функция получает на входе исходное сообщение произвольной длины и преобразует его в хэш-значение фиксированной длины (256 или 512 бит). Значение хэш-функции сложным образом зависит от содержания документа, но не позволяет восстановить сам документ. Хэш-функция чувствительна к всевозможным изменениям в тексте, что позволяет обнаруживать любой факт случайного или намеренного искажения текста. Далее к полученному хэш-значению применяется некоторое математическое преобразование с использованием ключа ЭП, в результате которого и получается собственно подпись электронного документа.

При проверке подписи проверяющий должен располагать ключом проверки ЭП пользователя, поставившего подпись. Проверяющий должен быть полностью уверен в подлинности ключа проверки ЭП (а именно в том, что имеющийся у него ключ проверки ЭП соответствует ключу проверки ЭП конкретного пользователя).

Процедура проверки подписи состоит из вычисления хэш-значения документа и проверки некоторых соотношений, связывающих хэш-значение документа, подпись под этим документом и ключ проверки ЭП подписавшего документ пользователя. Документ считается подлинным, а подпись правильной, если эти соотношения выполняются. В противном случае подпись под документом считается недействительной.

Для разрешения споров между отправителем и получателем информации, связанных с возможностью искажения пересылаемого документа или ключа проверки ЭП, сертификат соответствующего ключа проверки ЭП может выдаваться третьей стороне (например, администратору информационной безопасности) и применяться для разбора конфликтной ситуации.

3 КЛЮЧЕВАЯ ИНФОРМАЦИЯ

3.1 Типы рабочих ключей

Под «ключом» понимается вся ключевая информация, записываемая на ключевой носитель. Эта информация представляет собой некоторую структуру данных, содержащую как собственно ключи ЭП и/или шифрования (т.е. ключи в формате криптографических стандартов), так и сопутствующую им информацию, такую как идентификаторы алгоритмов, ключи защиты ключей, имитовставки, а также информацию, необходимую для идентификации и аутентификации пользователя — владельца ключевого носителя.

Далее ключи, понимаемые как вся совокупность ключевой информации, будем продолжать называть просто ключами. Собственно ключи ЭП и шифрования будем называть «криптографическими ключами».

СКЗИ «Валидата CSP» поддерживает два типа ключей: **одинарные** и **неодинарные**.

Одинарными ключами называются ключи, существующие в виде одного единственного компонента, хранящегося на одном ключевом носителе и содержащего всю информацию, необходимую для функционирования ключа.

Неодинарными ключами называются ключи, существующие в виде нескольких компонентов, каждый из которых хранится на отдельном ключевом носителе.

3.1.1 Одинарные ключи

В СКЗИ «Валидата CSP» различают два вида одинарных ключей:

– одинарный ключ, содержащий только криптографический ключ ЭП в соответствии с ГОСТ Р 34.10-2012;

– одинарный ключ, содержащий криптографический ключ, одновременно являющийся криптографическим ключом ЭП в соответствии с ГОСТ Р 34.10-2012 и криптографическим ключом шифрования в соответствии с ГОСТ 28147–89 или ГОСТ Р 34.12-2015 (блочные шифры «Магма» и «Кузнечик») совместно с ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик» в режимах простой замены, гаммирования и выработки имитовставки). В этом случае в сертификате ключа проверки ЭП должна быть установлена область использования ключа «Согласование ключей».

3.1.1.1 Открытый и закрытый ключи шифрования

СКЗИ «Валидата CSP» предназначено для использования в системе с открытым распределением ключей. В таких системах каждый пользователь формирует два ключа шифрования: закрытый и открытый (далее — ключи шифрования или долговременные ключи шифрования). Закрытый ключ шифрования должен храниться в тайне. Открытый ключ шифрования может быть опубликован для использования всеми пользователями системы, которые обмениваются зашифрованными сообщениями. Знание открытого ключа шифрования не даёт практической возможности определить закрытый ключ.

Примечание — В качестве закрытого ключа шифрования используется ключ ЭП, а в качестве открытого ключа шифрования — ключ проверки ЭП.

Пользователя, который зашифровывает сообщение, будем в дальнейшем называть отправителем; а пользователя, который расшифровывает сообщение — получателем.

Кроме долговременных ключей шифрования в процессе шифрования могут использоваться **эфемерные** ключи шифрования: **эфемерный закрытый ключ шифрования**, создаваемый отправителем сообщения с использованием генератора случайных чисел, и **эфемерный открытый ключ шифрования**, соответствующий эфемерному закрытому ключу шифрования.

Каждый эфемерный закрытый ключ шифрования используется только в одной операции шифрования. Эфемерный открытый ключ шифрования передается получателю вместе с сообщением.

Различают два вида шифрования: **неанонимное** и **анонимное**.

При **неанонимном** шифровании сообщения отправителем вычисляется общий ключ по алгоритму Диффи-Хеллмана на основе долговременного закрытого ключа шифрования отправителя и долговременного открытого ключа шифрования получателя. Для расшифрования этого сообщения получателем вычисляется тот же общий ключ на основе долговременного закрытого ключа шифрования получателя и долговременного открытого ключа шифрования отправителя.

При **анонимном** шифровании сообщения отправителем вычисляется общий ключ по алгоритму Диффи-Хеллмана на основе эфемерного закрытого ключа шифрования отправителя и долговременного открытого ключа шифрования получателя. Для расшифрования этого сообщения получателем вычисляется тот же общий ключ на основе долговременного закрытого ключа шифрования получателя и эфемерного открытого ключа шифрования отправителя.

Таким образом, для обеспечения связи с другими абонентами каждому пользователю необходимо иметь:

– собственный закрытый ключ шифрования;

– сертификаты открытых ключей шифрования пользователей сети конфиденциальной связи, заверенные Центром сертификации.

Далее ключи шифрования упоминаться не будут, и возможность использования ключа ЭП для шифрования будет определяться разрешённой областью применения соответствующего сертификата ключа проверки ЭП.

3.1.2 Неодинарные ключи

СКЗИ «Валидата CSP» поддерживает два особых типа неодинарных ключей:

– ключ в формате «3 из 6», создаваемый и загружаемый по схеме разделения секрета «3 из 6»;

– ключ в формате «2 из 3», создаваемый и загружаемый по схеме разделения секрета «2 из 3».

Ключи, используемые по схемам разделения секрета, предназначены для использования в качестве дополнительной меры, обеспечивающей устойчивость ключевой системы к компрометациям.

Ключи форматов «3 из 6» и «2 из 3» могут использоваться только как краткосрочные ключи (ключи со сроком до 15-ти месяцев).

3.1.3 Служебные ключи

Служебными ключами называются ключи, обеспечивающие функционирование служб (подсистем) криптопровайдера.

3.1.3.1 Ключи защиты

Ключами защиты называются используемые в СКЗИ «Валидата CSP» симметричные ключи, предназначенные для защиты (посредством шифрования) других ключей (рабочих ключей и других ключей защиты).

3.1.3.2 Парольный ключ

Парольный ключ — симметричный ключ, на котором зашифровываются ключи защиты при хранении их на носителе. Данный ключ представляет собой хэш-значение пароля, защищающего доступ к носителю ключевой информации абонента. Парольный ключ не записывается на ключевой носитель. В памяти ЭВМ он существует только при выполнении процедуры загрузки ключей в течение времени, необходимого для расшифрования ключей защиты рабочих ключей. После выполнения своей функции парольный ключ затирается случайной последовательностью. Проверка пароля осуществляется с использованием специального контрольного значения, записываемого в ключевой контейнер и представляющего собой дважды прохэшированный пароль (хэш-значение от хэш-значения пароля). Парольная защита устанавливается или не устанавливается по выбору пользователя при генерации ключей. При наличии парольной защиты при вводе ключа запрашивается пароль.

3.2 Сроки действия ключей и сертификатов

Сроки действия ключей и сертификатов устанавливаются в процессе выпуска сертификатов.

Максимальные сроки действия ключей и сертификатов, в зависимости от условий эксплуатации приведены ниже (Таблица 1 и Таблица 2).

Таблица 1 – Максимальные сроки действия ключей и сертификатов пользователей Центра Сертификации

Ключ/сертификат	**Срок действия**	**Условия применения**
Ключ ЭП, находящийся в режиме неизвлекаемого ключа на функциональном ключевом носителе (ФКН) «Валидата vdToken» или «Валидата vdToken» версия 2.0	Не более 3 лет (36 месяцев)	Только при использовании СКЗИ «Валидата CSP» в варианте исполнения 1 или 2
Ключ ЭП (для всех ключей ЭП, отличных от указанных выше в настоящей таблице, в том числе для ключей, записываемых на ФКН в режиме извлекаемого ключа)	Не более 15 месяцев	Без ограничений
Ключ проверки ЭП, сертификат ключа проверки ЭП	Не более 15 лет (180 месяцев) после окончания срока действия соответствующего ключа ЭП, максимальный срок действия — 18 лет (216 месяцев)	Без ограничений

Таблица 2 – Максимальные сроки действия ключей и сертификатов Администраторов Центра Сертификации

Ключ/сертификат	**Срок действия**	**Условия применения**
Ключ ЭП, находящийся в режиме неизвлекаемого ключа на ФКН «Валидата vdToken» или «Валидата vdToken» версия 2.0	Не более 5 лет (60 месяцев), из которых подписание сертификатов и списков аннулированных сертификатов возможно не более первых 3 лет (36 месяцев), далее — только подписание списков аннулированных сертификатов	Предназначены для использования только в Центрах Сертификации Удостоверяющих центров.
Ключ проверки ЭП, сертификат ключа проверки ЭП	Не более 15 лет (180 месяцев) после окончания срока, в который разрешено подписание сертификатов соответствующим ключом ЭП, максимальный срок действия — 18 лет (216 месяцев)	Без ограничений

4 СЧИТЫВАТЕЛИ КЛЮЧЕЙ

Для выполнения большинства криптографических операций требуются ключи. Ключ ЭП обычно хранится на отчуждаемых носителях (USB flash, «таблетках» - Touch Memory и т.д.). Для чтения и записи ключей на ключевые носители предназначены программные модули - считыватели ключей. СКЗИ «Валидата CSP» может работать с несколькими считывателями ключей, их использование регулируется **программой конфигурации** СКЗИ «Валидата CSP».

Настройка использования считывателей ключей с помощью программы конфигурации описана в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

5 ДАТЧИКИ СЛУЧАЙНЫХ ЧИСЕЛ

В процессе функционирования СКЗИ «Валидата CSP» используется программный датчик случайных чисел (ДСЧ).

Для инициализации программного ДСЧ используется физический ДСЧ.

Типы физических ДСЧ, которые поддерживаются в СКЗИ «Валидата CSP», приведен в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Использование физического ДСЧ регулируется программой конфигурации СКЗИ «Валидата CSP».

Настройка использования ДСЧ с помощью программы конфигурации описана в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

6 ПРОГРАММНЫЙ МОДУЛЬ ПОДДЕРЖКИ TLS

6.1 Среда функционирования программного модуля

Программный модуль поддержки TLS криптопровайдера СКЗИ «Валидата CSP» предназначен для использования на версиях ОС, перечень которых приведён в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Для корректной работы модуля поддержки TLS необходимо наличие установленного обновления ОС Microsoft Windows KB 980436 (http://support.microsoft.com/kb/980436), или более нового обновления, его заменяющего.

В качестве клиентского программного обеспечения (ПО), использующего протокол TLS, поддерживаются следующие программные продукты:

– Microsoft Internet Explorer (IE) версий 9.0, 10.0 и 11.0;

– Remote Desktop Client (RDC) версий 7.0, 8.0, 8.1 и 10.0.

В качестве серверного ПО, использующего протокол TLS, поддерживаются следующие программные продукты:

– Internet Information Server (IIS) версий 7.5 (из состава Microsoft Windows Server 2008 R2), 8.0 (из состава Microsoft Windows Server 2012), 8.5 (из состава Microsoft Windows Server 2012 R2) и 10 (из состава Microsoft Windows Server 2016/2019);

– Terminal Services (TS) из состава ОС Microsoft Windows Server;

– Terminal Services Gateway (TS Gateway) из состава ОС Microsoft Windows Server.

В качестве серверного ПО, использующего протокол Kerberos PKInit, поддерживаются контроллеры доменов Microsoft Active Directory под управлением ОС Microsoft Windows Server.

6.2 Описание механизма построения цепочек сертификатов в ОС Windows с модулем поддержки TLS

6.2.1 Общие положения

Программный модуль поддержки TLS криптопровайдера СКЗИ «Валидата CSP» встраивается в ОС Windows и обеспечивает возможность работы с сертификатами, созданными в соответствии с ГОСТ Р 34.10-2012, в частности, для построения и проверки их цепочек, с помощью интерфейса Microsoft Windows CSP. Данные возможности, таким образом, становятся доступными прикладному ПО, разработанному, в том числе, и сторонними производителями прикладного ПО.

Цепочка сертификатов, известная также как путь сертификации, предназначена для аутентификации, посредством ЭП, конечного сертификата с помощью сертификата корневого ЦС (Certificate Authority, CA), находящегося в начале цепочки, и, возможно, сертификатов промежуточных ЦС, находящихся в цепочке между сертификатом корневого ЦС и конечным сертификатом. Сертификат корневого ЦС является самоподписанным, т.е. данный сертификат аутентифицирует себя сам. Также сертификат корневого ЦС аутентифицирует следующий

за ним в цепочке сертификат промежуточного ЦС. Далее, по цепочке, мы приходим к последнему сертификату промежуточного ЦС, который уже аутентифицирует собственно конечный сертификат.

6.2.2 Проверка текущего статуса

Для проверки текущего статуса или действительности конечного сертификата цепочки сертификатов как таковой недостаточно - например, если с момента выпуска конечного сертификата последний был аннулирован/прекратил действие. Для подтверждения действительности сертификатов используют либо CAC (Certificate Revocation List, CRL), либо Протокол сетевого статуса сертификата (ПССС, Online Certificate Status Protocol, OCSP).

CAC представляет собой список серийных номеров аннулированных и прекративших действие сертификатов данного ЦС (за исключением, возможно, сертификатов, срок действия которых истек), заверенный ЭП на ключе ЭП администратора ЦС. Дополнительно, CAC содержит время аннулирования/прекращения действия каждого сертификата и, возможно, причину аннулирования/прекращения действия. ПССС позволяет получить от ответчика ПССС, для каждого выпущенного данным ЦС конечного сертификата, заверенное ЭП подтверждение текущего статуса этого сертификата. Для аннулированных/прекративших действие сертификатов заверенное ЭП подтверждение содержит время и, возможно, причину аннулирования/прекращения действия. В ответчике ПССС для простановки ЭП используется специальный конечный сертификат, выпущенный данным ЦС и содержащий необходимое расширенное использование ключа.

При использовании CAC для проверки действительности конечного сертификата для каждого ЦС (и корневого, и промежуточных) производится попытка найти в CAC данного ЦС серийный номер следующего сертификата цепочки. Если, при наличии искомого серийного номера в CAC, время аннулирования/-прекращения действия уже наступило, то следующий сертификат цепочки и, следовательно, конечный сертификат, считаются аннулированными/прекратившими действие.

При использовании ПССС для проверки действительности конечного сертификата для каждого ЦС (и корневого, и промежуточных) производится посылка ПССС-запроса, содержащего серийный номер следующего сертификата цепочки, соответствующему данному ЦС ПССС-ответчику. Последний формирует заверенное ЭП подтверждение, содержащее текущий статус проверяемого сертификата. Если проверяемый сертификат аннулирован/прекратил действие и время аннулирования/прекращения действия уже наступило, то следующий сертификат цепочки и, следовательно, конечный сертификат, считаются аннулированными/прекратившими действие.

6.2.3 Хранилища сертификатов и CAC

В ОС Windows хранилища сертификатов используют Реестр ОС для хранения сертификатов и CAC и делятся на хранилища компьютера и пользовательские. Как следует из названия, хранилища компьютера являются общими для всех пользователей и используются, в том числе, системными процессами ОС. Пользовательские хранилища привязаны к каждому конкретному пользователю, и у каждого пользователя они индивидуальные. При этом, в пользовательские хранилища автоматически включаются также сертификаты и CAC из хра-

нилищ компьютера (за исключением хранилища *Личное*).

Также хранилища различаются по типу хранимых ими объектов:

– *Личное (Personal, MY)* - предназначено для хранения личных сертификатов, для которых есть соответствующие им ключи ЭП;

– *Другие пользователи (Other People, AddressBook)* - предназначено для хранения сертификатов сторонних пользователей;

– *Доверенные корневые центры сертификации (Trusted Root Certification Authorities, ROOT)* - предназначено для хранения сертификатов и САС корневых ЦС;

– *Промежуточные центры сертификации (Intermediate Certification Authorities, CA)* - предназначено для хранения сертификатов и САС промежуточных ЦС.

Таким образом, хранилища пользователя *Другие пользователи*, *Доверенные корневые центры сертификации* и *Промежуточные центры сертификации* включают в себя сертификаты и САС из соответствующих хранилищ компьютера.

Для управления объектами, расположенными в хранилищах сертификатов ОС Windows, рекомендуется использовать *Консоль управления Microsoft (Microsoft Management Console, MMC)*. После запуска *MMC* следует добавить оснастку *Сертификаты (Certificates)* учетной записи пользователя или учетной записи компьютера - от этого выбора зависит, какие хранилища сертификатов будут отображаться. Следует отметить, что для добавления оснастки *Сертификаты* учетной записи компьютера необходимы права локального администратора.

6.2.4 Описание алгоритма построения цепочек

Для построения и проверки цепочек сертификатов прикладное ПО использует функции Microsoft Windows CSP. При вызове этих функций прикладное ПО выбирает ”двигатель” (Engine), используемый для построения цепочек - компьютера или пользовательский (используется по умолчанию). При выборе ”двигателя” компьютера используются хранилища сертификатов компьютера, при выборе пользовательского ”двигателя” используются хранилища сертификатов пользователя.

Построение цепочки сертификатов начинается с проверяемого (конечного) сертификата. Для возможности построения цепочки в проверяемом сертификате должно присутствовать расширение (Extension) *Идентификатор ключа Центра сертификации (Authority Key Identifier)*. В данном расширении находится, в числе прочего, *Идентификатор ключа (Key Identifier)* - хэш открытого ключа - сертификата ЦС, на котором был выпущен проверяемый сертификат. По этому идентификатору и производится поиск сертификата ЦС в локальных хранилищах *Доверенные корневые центры сертификации* и *Промежуточные центры сертификации* - в искомом сертификате ЦС этот идентификатор равен значению, находящемуся в расширении *Идентификатор ключа субъекта (Subject Key Identifier)*.

При отсутствии искомого сертификата ЦС в локальных хранилищах производится попытка нахождения в проверяемом сертификате расширения *Доступ к информации о Центре сертификации (Authority Information Access, AIA)*. В дан-

ном расширении, в числе прочего, находится список уникальных идентификаторов ресурса (Unique Resource Identifier, URI), указывающих на искомый сертификат ЦС, доступный по сети. Каждый URI из списка используется при попытке загрузки сертификата ЦС последовательно до успешной загрузки искомого объекта.

После успешного нахождения искомого сертификата ЦС (локально или по сети) производится поиск САС, соответствующего найденному сертификату ЦС. Поиск САС также изначально производится в локальных хранилищах *Доверенные корневые центры сертификации* и *Промежуточные центры сертификации*. В искомом САС значение *Идентификатор ключа* из состава расширения *Идентификатор ключа Центра сертификации* должно быть равно значению, находящемуся в расширении *Идентификатор ключа субъекта* сертификата ЦС.

При отсутствии искомого САС в локальных хранилищах производится попытка нахождения в проверяемом сертификате расширения *Точки распространения САС (CRL Distribution Points, CDP)*. В данном расширении находится список URI, указывающих на искомый САС, доступный по сети. Каждый URI из списка используется при попытке загрузки САС последовательно до успешной загрузки искомого объекта.

Следует упомянуть об особенностях, связанных с использованием для построения цепочек САС, содержащих расширение *Точка распространения выдачи (Issuing Distribution Point, IDP)*:

– в ОС Windows расширение *IDP* не используется для загрузки и/или обновления САС по сети;

– сертификаты, выпущенные на сертификате ЦС, соответствующем САС с расширением *IDP*, должны содержать расширение *CDP*;

– списки URI, содержащиеся в расширении *IDP* САС и в расширении *CDP* сертификатов, выпущенных данным ЦС, должны совпадать.

Вместо САС для определения действительности проверяемого сертификата может использоваться ПССС. Для этого в расширении *Доступ к информации о Центре сертификации* проверяемого сертификата должен присутствовать URI ПССС ответчика данного ЦС. При использовании ПССС формируется ПССС-запрос и посылается ПССС-ответчику. Полученное от ПССС-ответчика подтверждение содержит текущий статус проверяемого сертификата.

После нахождения сертификата ЦС и САС (или после получения подтверждения от ПССС-ответчика) выполняется криптографическая проверка полученных объектов, а также проверка действительности проверяемого сертификата. При успешном выполнении проверок, если найденный сертификат ЦС не является самоподписанным или не был найден в локальном хранилище *Доверенные корневые центры сертификации*, он занимает место проверяемого сертификата, и весь вышеописанный алгоритм повторяется рекурсивно.

Результат построения и проверки цепочки сертификата определяется следующим образом:

– *Аутентичность конечного сертификата не установлена* - если, по какой-либо причине, очередной искомый сертификат ЦС не был найден, или если цепочка не начинается с самоподписанного сертификата корневого ЦС, найденного в локальном хранилище *Доверенные корневые центры сертификации*;

– *Действительность конечного сертификата не установлена* - если, по какой-либо причине, очередной искомый САС данного ЦС не был найден, или не было получено доверенное подтверждение от ПССС-ответчика данного ЦС;

– *Конечный сертификат аннулирован* - если очередной проверяемый сертификат был найден в САС вышестоящего ЦС или OCSP ответчик вышестоящего ЦС возвратил подтверждение, содержащее статус ’аннулирован’, и время аннулирования уже наступило;

– *Конечный сертификат действителен* - в остальных случаях.

В состав ОС Windows входит утилита CertUtil, с помощью которой можно выполнять различные операции, связанные с сертификатами, САС, цепочками, и т.п.

В частности, для построения и проверки цепочки сертификата с именем субъекта *CN=Test,CN=Users,DC=Company,DC=ru*, находящегося в хранилище пользователя *Личное*, можно использовать следующую команду:
certutil.exe -user -verifystore MY Test

Результатом выполнения данной команды будет либо подтверждение действительности проверяемого сертификата, либо описание ошибки, возникшей в результате построения или проверки его цепочки.

6.2.5 Кэширование объектов

При построении цепочек сертификатов возможно выполнение загрузки сертификатов промежуточных ЦС или САС по сети на основании информации, содержащейся в расширениях *AIA* и/или *CDP*. Для исключения необходимости повторной загрузки уже загруженных объектов последние запоминаются в специальном файловом кэше. При выполнении загрузки объекта по сети вначале производится попытка найти его в этом кэше для повышения общей производительности криптографической подсистемы.

Используемый кэш зависит от «двигателя», выбранного прикладным ПО для построения цепочек - «двигатель» компьютера и каждый пользовательский «двигатель» используют собственный выделенный кэш. Объекты хранятся в кэше, в общем случае, до истечения срока их действия - например, САС, находящийся в кэше, будет действителен до момента времени, указанного в поле *Следующее обновление (Next Update)*.

Для детального просмотра содержимого кэша можно воспользоваться следующей командой:
*certutil.exe -v -urlcache **

Для полной очистки содержимого кэша можно воспользоваться следующей командой:
*certutil.exe -v -urlcache * delete*

Однако, рекомендуется не пользоваться командой очистки кэша, а помечать все записи кэша как недействительные с помощью следующей команды (для выполнения требуются права локального администратора):
certutil.exe -setreg chain\ChainCacheResyncFiletime @now

Более детально описание механизма кэширования объектов приведено в статье по ссылке http://technet.microsoft.com/en-us/library/ee619754%28v=ws.10%29.aspx.

Использование модуля поддержки TLS с клиентским и серверным ПО описано в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ДСЧ	Датчик случайных чисел
КЗИ	Криптографическая защита информации
ОС	Операционная система (Operating System)
ПК	Программный комплекс
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
ПССС	Протокол сетевого статуса сертификата
САС	Список аннулированных сертификатов (Certificate Revocation List)
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
ФКН	Функциональный ключевой носитель
ЦС	Центр сертификации (Certification Authority)
ЭВМ	Электронная вычислительная машина
ЭП	Электронная подпись (Digital Signature)

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного докум и дата	Подп	Дата
Изм	изменённых	заменённых	новых	аннулированных					