ViPNet
Virtual Private Network

Порядок разбора конфликтных ситуаций, возникающих при использовании электронной цифровой подписи

Руководство администратора

ФРКЕ.00006-02 90 05

infotecs

ОАО Инфотекс
125315 Москва, Ленинградский пр-т, 80, а/я 35
Тел: (095) 737-61-96 (hotline), 737-61-92, факс 737-72-78
E-mail: hotline@infotecs.ru
WWW: http://www.infotecs.ru

СОДЕРЖАНИЕ

1. Используемые термины и сокращения

АРМ [Администратор] – автоматизированное рабочее место Администратора безопасности, реализующее, в том числе, все необходимые функции корпоративного удостоверяющего центра (УЦ), связанные с изданием, отзывом, хранением сертификатов ключей подписи, а также иные функции в соответствии с Законом об электронной цифровой подписи.

Администратор безопасности – лицо, назначенное руководителем организации, эксплуатирующей АРМ [Администратор], и предоставляющей услуги корпоративного удостоверяющего центра. Администратор безопасности обеспечивает эксплуатацию АРМ [Администратор] и является уполномоченным лицом, подписывающим своей электронной цифровой подписью сертификаты ключей подписей пользователей, зарегистрированных на данном АРМ [Администратор].

Доверенное лицо Администратора безопасности – лицо, назначенное приказом руководителя организации, и обеспечивающее удаленную регистрацию пользователей и выдачу сертификатов ключей пользователям, зарегистрированным на соответствующем АРМе [Администратор].

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Пользователь – физическое лицо, участвующее в процессе электронного документооборота.

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром пользователю информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Список отозванных сертификатов (СОС) – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, содержащий список сертификатов, действие которых прекращено или приостановлено до истечения их срока действия.

Средство криптографической защиты информации (СКЗИ) – программное или аппаратное средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности, в том числе реализующее алгоритмы электронной цифровой подписи.

Сторона пользователя – юридическое лицо, представителем которого является пользователь.

Электронный документ (ЭД) – документ, в котором информация представлена в электронно-цифровой форме, и который может быть представлен в виде файла, хранящегося на носителе.

Электронная цифровая подпись (электронная подпись, ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

2. Возникновение конфликтных ситуаций

2.1. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения ЭД, а также использованием в данных документах ЭЦП. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- не подтверждение подлинности защищенных электронных документов средствами проверки ЭЦП получателя;
- оспаривание факта идентификации владельца ЭЦП, подписавшего ЭД;
- заявление отправителя или получателя ЭД об его искажении;
- оспаривание факта отправления и/или получения защищенного ЭД;
- оспаривания времени отправления и/или получения защищенного ЭД;
- иные случаи возникновения конфликтных ситуаций.

2.2. В случае возникновения конфликтной ситуации пользователь, предполагающий возникновение конфликтной ситуации, должен направить Администратору безопасности (непосредственно или через Доверенное лицо), выдавшему ему сертификат ключа подписи:

2.2.1. Уведомление о конфликтной ситуации с изложением обстоятельств ее возникновения.

2.2.2. ЭД, подлинность которого оспаривается. ЭД вместе с ЭЦП и сертификатом ключей подписи экспортируется из приложения, в котором он был получен или создан, в соответствии с Руководством пользователя данного приложения.

2.2.3. Если в качестве приложения используется ПО ViPNet Клиент [Деловая почта], то ЭЦП и сертификат ключей подписи содержится в составе экспортируемого файла вместе с ЭД. Если используется приложение, файл с экспортированным ЭД которого не содержит в своем составе ЭЦП или сертификат ключей подписи, то данные элементы экспортируются и направляются Администратору безопасности в виде отдельных файлов.

2.2.4. При оспаривании факта доставки ЭД Администратору безопасности предоставляются подписанные принимающей стороной извещения о доставке/прочтении документа, экспортированные из приложения в виде ЭД.

2.3. Администратор безопасности обязан незамедлительно проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

2.4. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Администратора безопасности.

2.5. В случае если уведомитель не удовлетворен полученной информацией, для разрешения конфликтной ситуации проводится техническая экспертиза.

3. Порядок проведения технической экспертизы

3.1. Экспертная комиссия созывается организацией, выполняющей функции удостоверяющего центра, на основании письменного заявления (претензии) Стороны пользователя, оспаривающего ЭД. В указанном заявлении, помимо реквизитов оспариваемого документа, должно быть указано лицо (лица), уполномоченные представлять интересы Стороны в составе экспертной комиссии. Количество указанных лиц не может превышать 3 человек.

3.2. Не позднее 10 рабочих дней с момента получения претензии назначается дата место и время начала работы комиссии, о чем письменно уведомляются обе Стороны.

3.3. Состав экспертной комиссии формируется в равных пропорциях из представителей Сторон. В состав комиссии, также включается эксперт – Администратор безопасности.

3.4. Экспертиза оспариваемого электронного документа осуществляется на предоставленном Администратором безопасности персональном компьютере с установленным ПО ViPNet Клиент (абонентском пункте), обеспечивающим проверку подписи и подпись ЭД.

3.5. В случае если представители одной из Сторон по оспариваемому электронному документу не явились для участия в экспертной комиссии, экспертиза проводится без их участия, а об отсутствии представителей по оспариваемому электронному документу составляется акт, подписываемый всеми присутствующими участниками экспертной комиссии.

3.6. Экспертиза осуществляется в три этапа:

3.6.1. Проверка оборудования и программного обеспечения и тестирование их работоспособности;

3.6.2. Контроль целостности оспариваемого электронного документа путем проверки ЭЦП при помощи сертификата открытого ключа ЭЦП, представленного Стороной;

3.6.3. Проверка принадлежности, актуальности и целостности сертификата, использованного комиссией для проверки ЭЦП.

3.7. Проверка работоспособности оборудования и программного обеспечения проводится путем проведения тестов пробной подписи и проверки подписи в присутствии членов экспертной комиссии.

3.8. Контроль целостности оспариваемого документа производится посредством стандартной процедуры импорта файлов ЭД с ЭЦП и сертификатом в ПО ViPNet Клиент и затем, проверки ЭЦП импортированного документа, в соответствие с руководством пользователя [2].

3.9. Проверка принадлежности, актуальности и целостности сертификата ключей подписи производится путем вызова в программе диалога просмотра сертификата, представленного вместе с ЭД. Просматриваемый сертификат распечатываются на бумажном носителе, и передается членам экспертной комиссии.

3.9.1. В случае если сертификат, используемый при проверке подписи, издавался на основании письменного запроса пользователя, то для доказательства принадлежности актуальности и целостности сертификата, использованного для проверки ЭЦП, Администратором безопасности и соответствующей Стороной комиссии предъявляется сертификаты на бумажном носителе, оформленные при получении сертификата. Члены комиссии производят визуальную сверку данных сертификатов с распечатанным сертификатом, использованным при подписи оспариваемого документа.

3.9.2. В случае если сертификат был издан на основании электронного запроса, подписанного ЭЦП с использованием ранее изданного официально оформленного сертификата, комиссии предъявляется логически связанная цепочка запросов на сертификаты и сертификаты, распечатанные на бумажных носителях, которые в совокупности подтверждают принадлежность сертификата лицу, сформировавшему ЭЦП. Распечатка этих запросов и сертификатов на бумажные носители производится Администратором безопасности в АРМ [Администратора]. Цепочка запросов признается действительной, а сертификат принадлежащим указанному владельцу, если выполнены следующие условия:

3.9.2.1. Цепочка логически связана, т.е. каждый следующий запрос подписан с использованием сертификата, изданного на основании предыдущего запроса.

3.9.2.2. Подпись под каждым запросом в цепочке действительна на момент издания сертификата по данному запросу.

3.9.2.3. Сертификат, которым подписан каждый запрос, действителен на момент подписания запроса.

3.9.2.4. Последним элементом в цепи является электронный сертификат (распечатывается), соответствующий (при визуальном сравнении) сертификату, используемому комиссией для проверки ЭЦП по оспариваемому электронному документу;

3.9.2.5. Сертификат, которым заверен первый запрос в цепочке (распечатывается), соответствует (при визуальном сравнении) официально оформленному сертификату, предъявленному комиссии.

3.10. Подтверждением подлинности оспариваемого электронного документа, является единовременное выполнение следующих условий:

3.10.1. Проверка ЭЦП оспариваемого электронного документа с сертификатом ключей подписи, предъявленными Стороной (п. 3.8), дала положительный результат.

3.10.2. Подтверждена принадлежность, актуальность и целостность сертификата ключей подписи пользователя Стороны (п. 3.9), с помощью которого проводится проверка ЭЦП оспариваемого электронного документа.

3.10.3. Если у заявителя отсутствуют сомнения в принадлежности сертификата, то проверка по п. 3.9 может не производиться.

3.11. При необходимости подтверждения факта доставки и сроков доставки ЭД производится экспертиза извещения о доставке, представленного отправителем ЭД, и подписанного ЭЦП получателя ЭД. Извещение содержит контрольные суммы принятого ЭД из состава ЭЦП этого ЭД, однозначно идентифицирующие ЭД, на который оно сформировано. Проверка подлинности извещения производится аналогично процедурам проверки ЭД, приведенным выше.

4. Оформление результатов технической экспертизы

4.1. Результаты экспертизы оформляются в виде письменного заключения – Акта экспертной комиссии, подписываемого всеми членами комиссии. Акт составляется немедленно после завершения экспертизы. В Акте фиксируются результаты всех этапов, проведенной экспертизы, а также все существенные реквизиты оспариваемого электронного документа. Акт составляется в трех экземплярах - по одному для каждой из Сторон и УЦ. Акт комиссии является окончательным и пересмотру не подлежит.

4.2. К акту прилагаются распечатки материалов, предоставленных на экспертизу (сертификаты, запросы на сертификат, извещения о доставке) и результаты проверки подписи представленных ЭД.

4.3. Подтверждение подлинности электронного документа, зафиксированного в Акте, будет означать, что этот документ имеет юридическую силу. Не подтверждение подлинности электронного документа, зафиксированное в Акте, будет означать, что это представленный электронный документ не имеет юридической силы.

4.4. Акты, составленные экспертной комиссией, являются надлежащим доказательством при дальнейшем разбирательстве споров в суде (арбитражном суде).

5. Документация

1. ViPNet [Удостоверяющий и Ключевой Центр] Руководство Администратора.
2. ViPNet Клиент [Деловая Почта] Руководство пользователя.