



**Порядок
разбора конфликтных ситуаций,
возникающих при использовании
электронной подписи**

Руководство администратора

ФРКЕ.00006-05 90 05

© 1991 – 2012 ОАО «ИнфоТекС», Москва, Россия.

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТекС».

ViPNet является зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «ИнфоТекС».

Все торговые марки и названия программ являются собственностью их владельцев.

ОАО «ИнфоТекС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 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	4
2.	ВОЗНИКНОВЕНИЕ КОНФЛИКТНЫХ СИТУАЦИЙ.....	4
3.	ПОРЯДОК ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ	5
4.	ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ	7
5.	ДОКУМЕНТАЦИЯ	7

1. Используемые термины и сокращения

АРМ Администратор — автоматизированное рабочее место администратора безопасности, реализующее, в том числе, все необходимые функции корпоративного Удостоверяющего центра, связанные с изданием, отзывом, хранением сертификатов открытого ключа подписи, а также иные функции в соответствии с законом «Об электронной 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 подписью сертификаты пользователей, зарегистрированных на данном АРМ Администратор.

Доверенное лицо администратора безопасности — лицо, назначенное приказом руководителя организации, и обеспечивающее удаленную регистрацию пользователей и выдачу сертификатов подписи пользователям, зарегистрированным на соответствующем АРМе Администратор.

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

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

Пользователь — физическое лицо, участвующее в процессе электронного документооборота.

Сертификат открытого ключа подписи — документ на бумажном носителе или электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, который включает в себя открытый ключ и который выдается Удостоверяющим центром пользователю информационной системы для подтверждения подлинности электронной подписи и идентификации владельца сертификата.

Список отозванных сертификатов (СОС) — документ на бумажном носителе или электронный документ с электронной 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 подписи.

Сторона пользователя — юридическое лицо, представителем которого является пользователь.

Электронный документ (ЭД) — документ, в котором информация представлена в электронной форме, и который может быть представлен в виде файла, хранящегося на носителе.

Электронная подпись — реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий идентифицировать владельца сертификата открытого 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 электронной подписи. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- * не подтверждение подлинности защищенных электронных документов средствами проверки электронной подписи получателя;
- * оспаривание факта идентификации владельца электронной подписи, 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 открытого ключа подписи:
- 2.2.1. Уведомление о конфликтной ситуации с изложением обстоятельств ее возникновения.
 - 2.2.2. ЭД, подлинность которого оспаривается. ЭД вместе с электронной подписью и сертификатом открытого ключа подписи экспортируется из приложения, в котором он был получен или создан, в соответствии с документацией на данное приложение.
 - 2.2.3. Если в качестве приложения используется программа ViPNet Деловая почта, то электронная подпись и сертификат открытого ключа подписи содержится в составе экспортируемого файла вместе с ЭД. Если используется приложение, файл с экспортированным ЭД которого не содержит в своем составе электронной подписи или сертификат 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 создается 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 программным обеспечением ViPNet Client (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 электронной подписи при помощи сертификата открытого ключа

- подписи, представленного стороной.
- 3.6.3. Проверка принадлежности, актуальности и целостности сертификата, использованного комиссией для проверки электронной подписи.
- 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 электронной подписью и сертификатом в программном обеспечении ViPNet Client и затем, проверки электронной подписи импортированного документа, в соответствии с руководством пользователя [2].
- 3.9. Проверка принадлежности, актуальности и целостности сертификата открытого ключа 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 электронной подписи, администратором безопасности и соответствующей стороной комиссии предъявляются сертификаты на бумажном носителе, которые были оформлены при их получении. 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 ранее изданным официально оформленным сертификатом, комиссии предъявляется логически связанная цепочка запросов на сертификаты и сертификаты, распечатанные на бумажных носителях, которые в совокупности подтверждают принадлежность сертификата лицу, сформировавшему электронную подпись. Распечатка этих запросов и сертификатов на бумажные носители производится администратором безопасности на АРМ Администратора. Цепочка запросов признается действительной, а сертификат принадлежащим указанному владельцу при выполнении следующих условий:
- 3.9.2.1. Цепочка логически связана, то есть 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 сертификат (распечатывается), соответствующий (при визуальном сравнении) сертификату, используемому комиссией для проверки электронной подписи 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 электронной подписи оспариваемого электронного документа с сертификатом открытого ключа подписи, предъявленными стороной (п. 3.8), дала положительный результат.
- 3.10.2. Подтверждена принадлежность, актуальность и целостность сертификата открытого ключа подписи пользователя стороны (п. 3.9), с помощью которого проводится проверка электронной подписи 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 электронной подписью получателя ЭД. Извещение содержит контрольные суммы принятого ЭД из состава электронной подписи 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 Удостоверяющего центра. Акт комиссии является окончательным и пересмотру не подлежит.
- 4.2. К акту прилагаются распечатки материалов, предоставленных на экспертизу (сертификаты, запросы на сертификаты, 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 Administrator Удостоверяющий и ключевой центр. Руководство администратора».
2. «ViPNet Деловая почта. Руководство пользователя».