ОРГАНИЗАЦИЯ СОТРУДНИЧЕСТВА ЖЕЛЕЗНЫХ ДОРОГ (ОСЖД)

I издание

Разработано экспертами ведущей железной дороги БЧ в 2014 году

Согласовано совещанием экспертов Постоянной рабочей группой по кодированию и информатике с 9 по 11 сентября 2014 г., город Трнава

Утверждено итоговым совещанием Постоянной рабочей группой по кодированию и информатике с 18 по 20 ноября 2014 года

Дата вступления в силу: 20 ноября 2014 года

Замечание:

Р 941-3

Рекомендации по применению технологии Доверенной третьей стороны для обеспечения юридической значимости электронных документов в трансграничном сообщении

Оглавление

1. Термины и определения ……. 4
2. Общие положения …… 4
3. Основные способы применения технологии ДТС ……... 5
4. Предпосылки для использования ДТС ……. 7
5. Требования к сторонам, применяющим ДТС …….. 8
6. Функции участников технологии ДТС ……. 8
7. Технические и технологические меры применения парных ЛТС ……..…… 9
8. Организационно-правовые меры применения парных ДТС …… 10
9. Порядок ведения Памятки ……...……. 10

Краткое содержание Памятки

Настоящая Памятка содержит общие рекомендации, а также перечень типовых мер, предлагаемых для железной дороги государства-участника ОСЖД при обеспечении легитимности созданных в ином правовом поле юридически значимых электронных документов, применяемых для обеспечения технологических процессов грузовых железнодорожных перевозок в трансграничном сообщении.

Памятка разработана на основе анализа практического опыта использования железными дорогами государств-участников ОСЖД технологий Доверенной третьей стороны для организации, внедрения и эксплуатации схем обеспечения юридической значимости электронных перевозочных, грузосопроводительных и иных транспортных документов в международном сообщении.

1. Термины и определения

АИС – автоматизированная информационная система.

ДТС – (Доверенная третья сторона) структура, в порядке, не противоречащем законодательству государства-участника ОСЖД, наделенная правом осуществлять деятельность по легализации ЭД и их ЭЦП/ЭП в своей юрисдикции и обеспечению гарантий доверия для стороны другой юрисдикции при трансграничном обмене ЭД.

СКЗИ – средства криптографической защиты информации.

ОСЖД – Организация сотрудничества железных дорог.

УЦ – (удостоверяющий центр), структура, уполномоченная в соответствии с законодательством государства-участника ОСЖД осуществлять функции по изданию, управлению, хранению и распространению сертификатов открытых ключей проверки подписи и списков отозванных сертификатов.

ЭД – (электронный документ) запись документированной информации в электронном виде, обеспеченная подтверждением юридической значимости путем выработки ЭЦП/ЭП в соответствии с законодательством государства-участника ОСЖД.

ЭЦП/ЭП – (электронная цифровая подпись/электронная подпись) последовательность символов, являющаяся реквизитом ЭД, предназначенная для аутентификации автора ЭД, подтверждения целостности и подлинности ЭД в соответствии с законодательством государства-участника ОСЖД.

2. Общие положения

2.1. Для применения ЭД в техпроцессах железнодорожного транспорта, принятия на их основе организационных, производственных, финансовых, юридических решений, использования ЭД в претензионных, исковых и процессуальных процедурах, железная дорога государства-участника ОСЖД должна обеспечить подтверждение в области действия своего национального законодательства юридической значимости ЭД, созданного в ином правовом поле. В частности, такая необходимость возникает при трансграничном обмене ЭД между железными дорогами ОСЖД, находящимися в правовых полях разных государств.

Для этого используется технология Доверенной третьей стороны (ДТС).

2.2. Основные технические принципы применения технологии ДТС железной дорогой государства-участника ОСЖД базируются на международных рекомендациях ITU-T X.842 «Информационные технологии. Методы защиты. Руководящие указания по применению и управлению службами Доверенной третьей стороны».

2.3. Роль ДТС заключается в обеспечении для стороны-получателя ЭД гарантии того, что ЭД обладает всей полнотой юридической значимости в правом поле стороны-отправителя ЭД. При этом обеспечение вышеуказанной гарантии для стороны-получателя ЭД производится в порядке соответствующем (не противоречащем) требованиям национального законодательства стороны-получателя ЭД.

2.4. Сервисы ДТС могут включать управление ключами и сертификатами открытых ключей, поддержку идентификации и аутентификации, фиксацию времени (time stamping – метки времени), электронные нотариальные службы и службы каталогов. ДТС может предоставлять все перечисленные сервисы либо их часть.

2.5. Технология ДТС в ходе осуществления трансграничного обмена юридически значимыми ЭД между железными дорогами государств-участников ОСЖД применяется при соблюдении следующих условий:

2.5.1. Стороны трансграничного обмена применяют в техпроцессах грузовых железнодорожных перевозок электронные юридически значимые документы, подписанные ЭЦП/ЭП, соответствующие (не противоречащие) следующим международным документам:

RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS) – серия протоколов для реализации сервиса «Доверенной третьей стороны»;

RFC 5652 Cryptographic Message Syntax – синтаксис криптографических сообщений (описание формата и структуры ЭД);

RFC 5280 Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile – профиль сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей.

2.5.2. Национальное законодательство государства-участника ОСЖД содержит требования соответствия ЭД и ЭЦП/ЭП национальным нормативным актам, в том числе в форме лицензирования, сертификации средств ЭЦП/ЭП, экспортно-импортные ограничения на средства криптографической защиты и т. п., либо допускает выбор любой технологии применения ЭД и ЭЦП/ЭП.

2.5.3. Железные дороги государств-участников ОСЖД, применяющие ЭД в трансграничном сообщении имеют возможность обеспечить техническое выполнение проверки ЭЦП/ЭП для различных криптографических алгоритмов.

2.6. ДТС используется как информационный объект, обеспечивающий проведение проверок ЭЦП/ЭП обрабатываемых ЭД с пошаговой фиксацией. Результатом таких проверок является электронный документ с ЭЦП/ЭП – квитанция ДТС.

В техническом плане ДТС применяет следующие протоколы:

RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS) – серия протоколов для реализации сервиса «Доверенной третьей стороны»;

RFC 6960. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP);

RFC 3161 Time-Stamp Protocol (TSP) – протокол штампов (меток) времени,

и является составной частью трансграничного обмена ЭД.

3. Основные способы применения технологии ДТС

3.1. Существуют следующие основные способы применения ДТС для подтверждения юридической значимости ЭД, созданных в ином правовом поле:

применение технологии независимой ДТС;

применение технологии парной ДТС.

3.2. Применение технологии независимой ДТС

3.2.1. Применение классической технологии независимой ДТС предполагает использование услуг третьего субъекта, являющегося информационным посредником, обеспечивающим имеющимися аппаратно-программными и организационными средствами перепроверку ЭЦП/ЭП стороны-отправителя ЭД для стороны-получателя ЭД (рисунок 1).

3.2.2. Для информационного обмена между сторонами и ДТС используются протоколы, регламенты обмена и форматы представления данных, определяемые информационным посредником (независимой ДТС).

3.2.3. Обмен ЭД между сторонами может осуществляться как через независимую ДТС, так и непосредственно между АИС сторон.

3.2.4. Наряду с функциями информационного посредника и гаранта доверия ЭД сторон друг перед другом, независимая ДТС выступает арбитром (одним из арбитров, экспертом) по организационно-техническим вопросам в исково-претензионной деятельности между сторонами в случае использования средств ЭЦП/ЭП и ЭД.

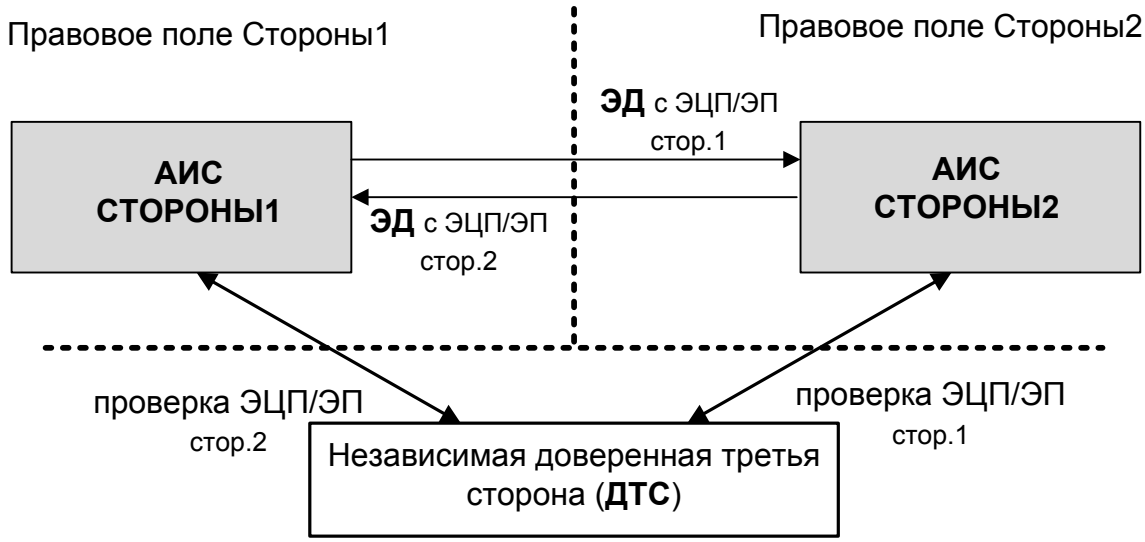

Рис.1

3.2. Применение технологии парных ДТС

3.2.1. Применение технологии парных ДТС предполагает осуществление функций проверки ЭЦП/ЭП стороны-отправителя ЭД для стороны-получателя ЭД посредством взаимодействия аппаратно-программных комплексов ДТС, являющихся субъектами национальных законодательств государств-участников ОСЖД (рисунок 2).

3.2.2. Для информационного обмена между сторонами и ДТС используются протоколы обмена информацией и унифицированные форматы представления данных RFC 3029. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS), RFC 6960. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP), либо иные, установленные организационно-техническими соглашениями между сторонами.

Применяемые правила, протоколы, регламенты обмена и форматы представления данных при использовании технологии парных ДТС не должны противоречить требованиями национального законодательства каждой их сторон.

3.2.3. При использовании технологии парных ДТС организация и осуществление исково-претензионной деятельности между сторонами по вопросам, связанным с применением средств ЭЦП/ЭП и ЭД, регулируются двусторонними соглашениями.

3.2.4. Канал обмена ЭД между сторонами определяется двусторонними организационно-техническими соглашениями.

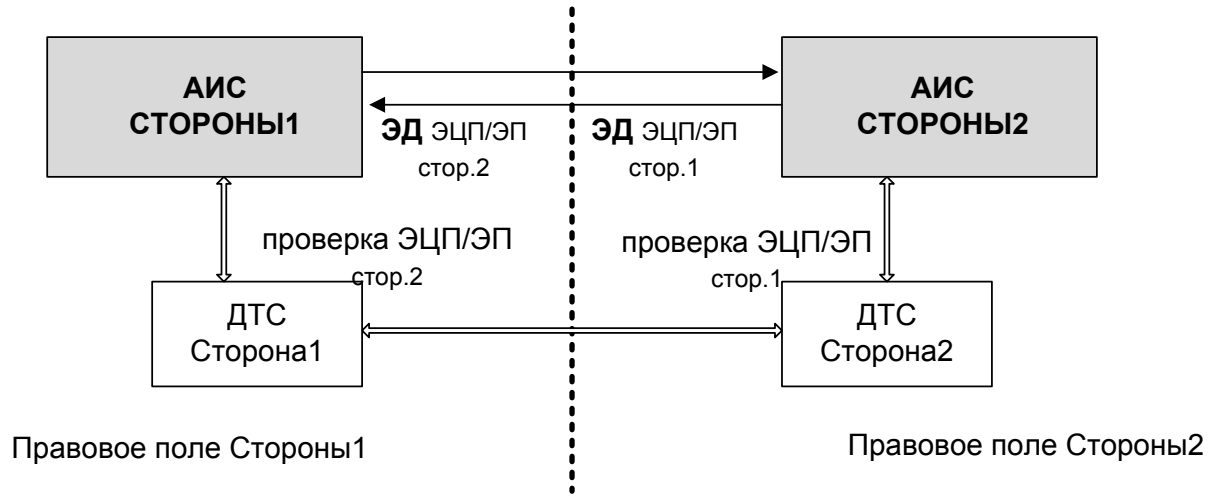

Рис. 2.

3.3. Аспекты, перечисленные выше, а также анализ опыта практического применения технологии ДТС, полученного железными дорогами, участвующими в работах в рамках соответствующих тем Постоянной рабочей группы по кодированию и информатике Комитета ОСЖД, указывают, что в настоящее время наиболее приемлемым является способ использования парных ДТС.

Основные положения настоящей Памятки разработаны с учетом предположения, что железные дороги государств-участников ОСЖД применяют технологию парных ДТС.

4. Предпосылки для использования ДТС

4.1. Организация и осуществление грузовых железнодорожных перевозок в международном сообщении.

4.2. Наличие и практическое применение технологий внутренних грузовых железнодорожных перевозок на основе юридически значимых ЭД, подписанных ЭЦП/ЭП.

4.3. Наличие требований национального законодательства по обеспечению юридической значимости ЭД путем его подписания ЭЦП/ЭП, соответствующих (не противоречащих) следующим международным документам:

RFC 5652 Cryptographic Message Syntax – синтаксис криптографических сообщений (описание формата и структуры ЭД);

RFC 5280 Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile – профиль сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей.

4.4. Наличие двусторонних соглашений между железными дорогами государств-участников ОСЖД об использовании в трансграничном грузовом сообщении юридически значимых ЭД, подписанных ЭЦП/ЭП.

4.5. Необходимость подтверждения юридической значимости ЭД в своей юрисдикции путем проверки ЭЦП/ЭП, выработанной в ином правовом поле, обес-

печение гарантий доверия для стороны другой юрисдикции при трансграничном обмене ЭД, в том числе для использования ЭД, созданных в правовом поле другой стороны, в претензионных, исковых и процессуальных процедурах своей юрисдикции.

4.6. Запрещение (ограничение) национального законодательства на использование в своей юрисдикции средств ЭЦП/ЭП, не прошедших установленные процедуры сертификации, лицензирования, ограничение экспортно-импортных операций в отношении средств ЭЦП/ЭП.

5. Требования к сторонам, применяющим ДТС

5.1. Наличие в государстве-участнике ОСЖД правовой и нормативной технической базы использования ЭД и ЭЦП/ЭП, а также опыта внедрения средств ЭЦП/ЭП и использования юридически значимых ЭД железной дорогой государства-участника ОСЖД.

5.2. Использование железной дорогой государства-участника ОСЖД АИС, предназначенной (-ных) для создания, обмена и исполнения ЭД в рамках технологических процессов грузовых железнодорожных перевозок, обеспечения юридической значимости и подлинности-ЭД в своем правовом поле.

5.3. Использование в соответствии с национальным законодательством железной дорогой государства-участника ОСЖД функционала УЦ в рамках инфраструктуры открытых ключей.

5.4. Обеспечение железной дорогой государства-участника ОСЖД выполнения требований национального законодательства в части разрешения (регулирования, допущения использования) применения в своей юрисдикции международных документов, составляющих техническую основу технологии ДТС:

RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS) – серия протоколов для реализации сервиса «Доверенной третьей стороны»;

RFC 6960 Online Certificate Status Protocol (OCSP) – протокол проверки статусов сертификатов открытых ключей;

RFC 3161 Time-Stamp Protocol (TSP) – протокол штампов (меток) времени.

5.5. Обеспечение железной дорогой государства-участника ОСЖД взаимодействия находящейся в своем правовом поле ДТС со своей АИС с одной стороны, и с соответствующей ДТС (парной ДТС) сопредельной железной дороги с другой стороны.

6. Функции участников технологии ДТС

6.1. Функции АИС сторон

АИС железной дороги государства-участника ОСЖД осуществляет:

6.1.1. Выработку-проверку ЭЦП/ЭП, формирование ЭД в соответствии с требованиями национального законодательства;

6.1.2. В установленном порядке применение юридически значимого ЭД в техпроцессах грузовых железнодорожных перевозок;

6.1.3. Передачу ЭД на сопредельную железную дорогу - прием ЭД от сопредельной железной дороги;

6.1.4. Формирование и отправку в ДТС, действующей в своем правовом поле, заявок на проверку ЭЦП/ЭП ЭД, подписанных на стороне сопредельной железной дороги;

6.1.5. Прием от ДТС, действующей в своем правовом поле, квитанций с результатами проверки ЭЦП/ЭП ЭД, поступившего от сопредельной железной дороги, и проверка ЭЦП/ЭП ДТС, действующий в своем правовом поле.

6.2. Функции ДТС

6.2.1. ДТС, действующая в своем правовом поле, осуществляет:

6.2.1.1. Прием заявок, поступивших от АИС, действующей в своем правовом поле, проверку их ЭЦП/ЭП;

6.2.1.2. Формирование и передачу в АИС, действующей в своем правовом поле, подписанных квитанций с результатами проверки ЭЦП/ЭП ЭД;

6.2.1.3. Формирование и отправку в парную ДТС сопредельной железной дороги (действующую в ином правовом поле) запросов на проверку ЭЦП/ЭП ЭД, подписанных в АИС сопредельной железной дороги (действующей в ином правовом поле);

6.2.1.4. Прием от парной ДТС сопредельной железной дороги (действующей в ином правовом поле) ответов с результатами проверки ЭЦП/ЭП ЭД и проверку их ЭЦП/ЭП.

6.2.2. Парные ДТС сторон обеспечивают доверенный (защищенный) канал взаимодействия для передачи запросов и ответов.

При этом используется строгая аутентификация сторон, на основе применения согласованных средств криптографической защиты доверенного канала взаимодействия парных ДТС.

7. Технические и технологические меры применения парных ДТС

Железные дороги государств-участников ОСЖД, применяющие технологию ДТС для обеспечения юридической значимости ЭД, созданных в ином правовом поле:

7.1. Организуют взаимодействие всех субъектов информационного обмена со своими АИС, обеспечивающими применение юридически значимых ЭД и участвующими в международном трансграничном технологическом взаимодействии;

7.2. Обеспечивают использование элементов криптографических протоколов проверки статусов сертификатов (OCSP) и штампов времени (TSP) для подтверждения факта и времени выработки ЭЦП/ЭП ЭД, а также действительности сертификата открытого ключа на момент подписи;

7.3. Устанавливают согласованный срок хранения квитанций ДТС сторон;

7.4. Определяют процедуру обмена сертификатами открытых ключей проверки подписи ДТС, используемых для подписи запросов-ответов ДТС;

7.5. Определяют процедуру обмена сертификатами открытых ключей проверки подписи ДТС, используемых для организации защищенных каналов взаимодействия между парными ДТС;

7.6. Используют согласованные алгоритм и протокол обмена сообщениями между ДТС при проверке ЭЦП/ЭП, определяющие структуру, форматы сообщений;

7.7. Согласовывают требования к средствам вычислительной техники, программным средствам, средствам телекоммуникаций и иные технические требования, необходимые для организации взаимодействия между парными ДТС.

8. Организационно-правовые меры применения парных ДТС

При организации применения ДТС для обеспечения юридической значимости ЭД в трансграничном сообщении железные дороги государств-участников ОСЖД:

8.1. Разрабатывают и в установленном порядке применяют двусторонние соглашения, описывающие организационно-правовые, технические и технологические аспекты обмена юридически значимыми ЭД в трансграничном сообщении, меры обеспечения юридической значимости ЭД, созданных в ином правовом поле, в том числе протоколы взаимодействия сервисов парных ДТС, регламенты взаимодействия сторон при эксплуатации парных ДТС, реализацию претензионных процедур с учетом требований национальных законодательств сторон.

8.2. В установленном порядке определяют, что стороны признают юридическую силу ЭД, исходящих от железной дороги-отправителя ЭД и выполненных по правилам и требованиям ее национального законодательства, если ЭД имеет электронную квитанцию ДТС своего правового поля, соответствующую требованиям двусторонних соглашений.

8.3. Признают, что используемые участниками взаимодействия средства защиты информации обеспечивают достаточную защиту и целостность ЭД и ЭД создаются в порядке, установленном правилами и требованиями законодательства государства каждой стороны, участвующей в трансграничном обмене юридически значимыми ЭД.

8.4. Разрабатывают, согласовывают и применяют организационные требования взаимодействия парных ДТС между собой.

9. Порядок ведения Памятки

Внесение изменений в Памятку производится в соответствии с актуализацией памяток ОСЖД по теме «Безопасность информационных ресурсов и информационно-телекоммуникационной инфраструктуры». Памятка актуализируется решением Постоянной рабочей группы ОСЖД по кодированию и информатике.

Организация, ответственная за ведение Памятки - ОСЖД.