№ 7 (35), июль 2011

«Меры и средства защиты персональных данных»

Доверенная третья сторона при трансграничной передаче персональных данных

Любая деловая активность - будь то электронная торговля, таможенное и иное оформление грузов, телемедицина, дистанционное образование - предполагает обмен документами, информацией между участниками бизнес-процесса.

Сегодня основная тенденция, сопровождающая процессы перевода документов и услуг в электронный вид, сводится к решению главной задачи – созданию доверенной инфраструктуры, содержащей доверенные сервисы, которые бы могли использоваться в автоматизированных системах, реализующих те или иные бизнес-процессы. Техническая концепция «Доверенной третьей стороны» (далее - ДТС), воплощающая эти идеи, изложена в международных рекомендациях X.842, определяющих требования к перечню доверенных сервисов как к комплексу организационно-технических мероприятий.

Немного истории

Одним из первых решений проблемы доверенного электронного трансграничного взаимодействия была работа по созданию макета Узла международного взаимодействия в сфере электронной цифровой подписи. Этот узел, по сути, представляет собой некую зону, где подписи из разных стран признавались бы действительными всеми странами-участниками. В то время, в 2006 году, технические решения этой проблемы уже были как у зарубежных, так и у отечественных разработчиков. Не хватало только политического вектора. Практически эта идея была реализована в работах по государственному контракту, который продвигали Росинформтехнологии. Созданный макет взаимодействия прошел общественную приемку-демонстрацию в начале 2007 года и даже был проверен на деле.

Проект не получил активной практической поддержки за рубежом. Но опыт проводимых работ стал толчком по выработке идеи «многополярности» электронного мира. В этом мире каждый «игрок» живет в отношении электронной подписи по своим правилам, со своими алгоритмами, в своем правовом пространстве, но при этом существует и механизм проверки, который позволяет доверять документам с электронными подписями одной страны в другой.

В нашей стране это направление одними из первых начали развивать специалисты ООО «Топ Кросс». Эта компания активно занималась созданием макета взаимодействия. В ходе разработки ею были установлены деловые отношения с польской фирмой Unizeto Technologies SA, которая в качестве доверенного квалификационного центра успешно занимается проблемой обеспечения трансграничности электронной подписи в Евросоюзе. Директива Еврокомиссии очерчивает для европейских стран законодательные рамки, в которых должно строиться нормативно-правовое поле работы с электронными подписями. При этом каждой стране - свое специфическое локальное законодательство в отношении электронной подписи. Поэтому для решения проблемы использования электронной подписи при трансграничном обмене информацией главное - понять, до какой степени данная подпись соответствует всем национальным правилам, скажем, Греции, чтобы быть действительной, например, в Польше. Отдельный вопрос – как проверить эту подпись? Это тоже немаловажный аспект, требующий пристального рассмотрения.

Доверенная третья сторона – это, по сути, имеющая специальную аккредитацию (комплект разрешительных локальных документов) организация, которая обладает определённым техническим и технологическим потенциалом, отслеживает изменение НПА и соответствующих технических требований, оказывает услуги по проведению различных проверочных (валидационных) и не только процедур. В части трансграничного обмена ДТС должна взаимодействовать с аналогичными ДТС из других юрисдикций с той задачей, чтобы в случае необходимости перетранслировать запрос проверки, например, электронной подписи, в тот ДТС, в зоне которого функционирует автор проверяемой подписи.

Доверенная третья сторона и персональные данные

Иными словами, доверенная третья сторона - это средство обеспечения доверия в системе электронного трансграничного документооборота. И здесь не играет роли, какая это информация - финансовые ли документы или персональные данные. Но если речь идет о персональных данных и особенно, если мы говорим о передаче персональных данных через государственную границу, то необходимо иметь в виду, что мы должны не только обеспечить конфиденциальность, но и достоверность передаваемой информации.

Об этом говорится в тексте действующей редакции Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных» (далее – 152-ФЗ). Обратимся к статье 5 настоящего закона, в которой говорится о принципах обработки персональных данных. Среди прочих принципов здесь отмечается, что обработка персональных данных должна обеспечиваться по принципу «…достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных» (часть 4, статья 5 ФЗ-152).

Здесь нас, в первую очередь, волнует принцип достоверности персональных данных.

Рассмотрим такую ситуацию. Например, в рамках своей деятельности оператор персональных данных из Российской Федерации, скажем, или из иной страны Таможенного союза, передает персональные данные оператору в другую страну СНГ, допустим, в Казахстан. Как оператору в Казахстане понять, что пришли персональные данные именно от оператора из Российской Федерации? Как понять, что они пришли целыми, неизменёнными? Для этого обычно используют электронную подпись. Но как быть (а так оно и есть на самом деле), если в Казахстане свои стандарты на электронную подпись, отличающиеся от российских? Как проверить на казахстанской стороне электронную цифровую подпись по ГОСТ Р 34.10-2001? Для обеспечения продуктивного взаимодействия между этими странами и необходимо, чтобы в каждой из них было по Доверенной третьей стороне. Кстати, именно по этому пути пошли и в концепции построения информационных систем в Таможенном Союзе.

Выполнение требования законодательства о персональных данных в части обеспечения достоверности передаваемых персональных данных возможно сегодня только с применением локально легитимных криптографических средств, в том числе и электронной подписи. Этот инструмент придает электронному документу такую же юридическую силу, как и бумажному. Применение же электронной подписи в трансграничном режиме чрезвычайно затруднительно осуществить без использования Доверенной третьей стороны с её набором доверенных сервисов, основанных на международных стандартах.

Сергей Муругов,
генеральный директор ООО «Топ Кросс»

Читайте также в рубрике:

Анти-ТОР зловредов: включаем голову и концентрируем внимание на мелочах
Взгляд кадровика: проблема инсайдера как проблема нелояльного сотрудника
Доверенная третья сторона при трансграничной передаче персональных данных

персональные данные персональные данные персональные данные персональные данные персональные данные персональные данные персональные данные персональные данные персональные данные персональные данные

Электронное периодическое издание «Персональные данные».
Свидетельство о регистрации средства массовой информации Эл № ФС77-33721 от 26 сентября 2008 г., выданное Федеральной службой по надзору в сфере связи и массовых коммуникаций

© 2008-2011 ИнфоТехноПроект

Адрес редакции:
119607, Москва, Мичуринский проспект, д.45
Телефон редакции: +7 (499) 249–93–94
+7 (495) 931–62–55

Карта сайта © Использование материалов сайта осуществляется только с письменного согласия редакции

техподдержка: support@privacy-journal.ru, отдел маркетинга: pr@privacy-journal.ru