О ДОВЕРИИ К СЕРВИСАМ БЕЗОПАСНОСТИ, обеспечивающим юридическую силу ЭД

Часть 1

А.Сабанов, к.т.н., доцент МГТУ им. Н.Э.Баумана

Для построения пространства доверия к электронным документам (ЭД), заверенным квалифицированной электронной подписью (ЭП) и претендующим на право обладания юридической силой (ЮС), необходима разработка требований к обеспечивающим их сервисам безопасности.

Постановка задачи

В качестве современной технологии, заменяющей бумажные документы, в нашу жизнь входит электронный документооборот (ЭДО), в котором вместо личной подписи используется ЭП.

Доверие к работе информационной системы (ИС) связано с качеством ее работы, которое определяется надежностью обслуживания запросов пользователей и информационной безопасностью выполнения бизнес-процессов. В связи с интенсивным развитием ИС в рамках государственных проектов информатизации общества [1] и предоставления государственных услуг в электронном виде [2] количество участников удаленного электронного взаимодействия (УЭВ), пользующихся ЭП, в совокупности уже превышает 10 млн. При этом весьма актуальна оценка доверия к результатам работы вовлеченных во взаимодействие ИС и предоставляемых пользователям сервисов.

Более точно постановку задачи сформулируем в виде оценки доверия к результатам обращения к сервисам безопасности, отвечающим за обеспечение юридической силы электронных документов, поскольку согласно [1], электронные документы с ЭП должны полностью заменить привычные всем бумажные уже к 2018 году.

О пространстве доверия к ЭД, обладающим ЮС

Если для бумажных документов и сообщений за столетия выработаны правила, регламенты, экспертиза, принят ряд международных соглашений и сформировано определенное пространство доверия, то для электронных документов с доверием пока плохо.

Такое положение сложилось по ряду причин, в частности, из-за отсутствия долгожданных законодательных актов. Один из вопиющих примеров – закон об электронных документах и сделках. Специалисты уже более 10 лет ждут, когда же появится такой федеральный закон и разъясняющие его положения нормативные акты (у нас, как правило, принятые законы требуют толкований) о том, что такое ЭД, имеющий правовые последствия.

Несмотря на бурный рост ЭДО, бумажные копии по-прежнему складываются в архивы на предприятиях, в организациях, ведомствах и министерствах. Даже после принятия указанного долгожданного закона рост бумажного оборота сразу не прекратится, но хотя бы можно будет говорить о едином пространстве доверия к ЭДО, в котором обращаются документы, обладающие ЮС.

О документе говорят, что он обладает юридической силой, если способен влиять на правовые отношения и порождать правовые последствия. Для того, чтобы ЭД обладал ЮС, одного сервиса безопасности в виде ЭП недостаточно. В минимально необходимый и достаточный набор сервисов безопасности для придания юридической силы электронному документу входит:

- наличие электронной подписи, связанной с документом;

- идентификация и аутентификация владельца подписи;
- валидность сертификата ключа проверки ЭП (СКПЭП);
- штамп доверенного времени;
- доказанная (проверенная) актуальность реестра полномочий ЭП, в который должна быть включена актуальная учетная запись подписанта.

Рассмотрим, насколько сейчас можно доверять этим сервисам безопасности. Начнем с ЭП.

Сеть УЦ – основа пространства доверия к ЭП

Одно из обязательных условий существования ЭП и оборота электронных документов, обладающих юридической силой, – наличие развитой инфраструктуры открытых ключей (PKI – public key infrastructure). PKI и решения на ее основе в России строятся уже более 13 лет, официально после выхода федерального закона №1-ФЗ [3]. В 2011 году ему на смену был принят №63-ФЗ, первая статья которого гласит, что закон "регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий" [4]. В целом требования закона выполняются. Однако отсутствие ряда технических требований к участникам УЭВ и, в частности, к удостоверяющим центрам (УЦ) по выполнению положений данного закона отрицательно сказывается на доверии как к самой ЭП, так и к развитию юридически значимого ЭДО в различных ИС.

По определению PKI – инфраструктура доверия к открытым ключам. Основа инфраструктуры – сеть УЦ и информационные ресурсы, которые должны быть "связаны одной цепью" проверки валидности сертификатов ключа проверки электронной подписи (СКПЭП). Главное назначение УЦ состоит в формировании и выдаче СКПЭП клиентам для того, чтобы они могли ставить свою ЭП, используя, как правило, сертифицированные средства подписи.

Насколько сейчас можно доверять ЭП? Основные вопросы доверия крутятся вокруг обязанности владельца СКПЭП "обеспечивать конфиденциальность ключей электронных подписей, в частности, не допускать использование принадлежащих им ключей электронных подписей без их согласия" (ст. 10 №63-ФЗ) и его права передавать ключ подписи другому лицу (ст. 14). К сожалению, эти процессы трудно формализуемы и пока не имеют общепринятой "линейки, позволяющей выполнить измерения" уровня доверия. В конкретных случаях можно оценить риск компрометации ключа подписи и использования просроченной или поддельной доверенности, но универсального подхода пока нет.

Заметим, что единое пространство доверия к ЭП строится в РФ не первый год, однако пока далеко от совершенства. Помимо упомянутых пробелов в нормативной базе, под большим вопросом остается доверие к ПО, на котором генерируется сервис безопасности ЭП – а ведь доверенная система должна состоять из доверенных компонентов.

Вопросы доверия к другим сервисам безопасности, необходимым для придания юридической силы электронному документу, рассмотрим в следующей части статьи.

ЛИТЕРАТУРА

1. Распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р "О государственной программе Российской Федерации "Информационное общество (2011–2020 годы)".
2. Федеральный закон РФ от 27 июля 2011 г. № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг".
3. Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи".
4. Федеральный закон РФ от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи".