Единое пространство доверия электронным подписям

В последнее время термин “единое пространство доверия электронной подписи” постоянно используется при организации юридически значимого электронного взаимодействия, в частности при организации электронного взаимодействия при предоставлении государственных и муниципальных услуг.

Что понимается под этим термином, что сделано и как пойдет дальнейшее развитие – это предмет данной статьи.

Формирование единого пространства доверия электронной подписи в целях организации взаимного признания электронной подписи при межведомственно взаимодействии при оказании государственных и муниципальных услуг представляет собой систему технологических, организационных и нормотворческих мероприятий, направленных на организацию юридически значимого и безопасного электронного взаимодействия органов власти, юридических и физических лиц с использованием технологии электронной подписи.

Необходимо отметить, что термин “единое пространство доверия электронной подписи” до настоящего времени нормативными правовыми документами не определен, что вносит некое разночтение в понимание данного термина. (Минкомсвязью России неоднократно предпринимались попытки нормативного закрепления данного термина, которые не находили понимания у других ведомств).

В результате построения единого пространства доверия достигается проверка информационными системами органов государственной власти и различных организаций сертификатов ключей проверки электронных подписей, сформированных различными удостоверяющими центрами, входящими в единое пространство доверия, а также электронных подписей, сформированных под электронными документами в процессе электронного взаимодействия.

В настоящее время в организации электронного взаимодействия для неопределенного круга лиц сертификат ключа проверки электронной подписи является единственным документом, подтверждающим принадлежность ключа проверки электронной подписи владельцу сертификата ключа электронной подписи, которым может выступать как физическое, так и юридическое лицо.

На основе положительного результата проверки сертификата и электронной подписи под электронным документом принимается решение о валидности конкретного электронного взаимодействия между субъектами взаимоотношений и принимается решение о совершении юридически значимого действия. Это может быть предоставление государственной услуги заявителю, предоставление сведений из одного органа власти другому и т.д. Таким образом, от результата проверки сертификата и ключа электронной подписи зависит непосредственно и благополучие конкретного физического или юридического лица, что накладывает ответственность на

построение информационных систем проверки и разработку критериев и требований на основании которых происходит признание и проверка, а также требований к работе удостоверяющих центров, включая требование по удостоверению личности при формировании сертификатов ключей проверки электронной подписи (далее - ЭП) и по информационной безопасности.

Необходимо отметить, что в апреле 2011 года вступил в силу ФЗ №63 «Об электронной подписи», при этом ФЗ №1 «Об электронной цифровой подписи», до 2011 года регулировавший деятельность в области электронной цифровой подписи, утратит силу только в июле 2012 года. В настоящее время Правительством Российской Федерации ведется активная нормотворческая деятельность, направленная на реализацию ФЗ № 63 и раскрытие его отдельных положений.

Надо отдать должное ФЗ №1 «Об электронной цифровой подписи», на основании которого с 2002 года сформировался рынок удостоверяющих центров, были определенны некоторые правила взаимодействия между удостоверяющими центрами и информационными системами, сформированы ведомственные домены доверия. Можно отметить ФНС России, Федеральное казначейство, Пенсионный фонд России. Основным недостатком ФЗ № 1 было отсутствие положений о формировании единых принципов признания электронных подписей, или, как иногда говорят, чтобы сертификат, выпущенный любым из удостоверяющих центров на территории России, мог быть использован и для сдачи налоговой отчетности, и для получения государственных услуг в электронном виде.

Развитие всех недостающих положений по построению доверия к электронному взаимодействию, уточнение всех вопросов было также инициировано развитием предоставления государственных и муниципальных услуг в электронном виде, определенных Федеральным законом № 210 (ФЗ № 210).

ФЗ № 63 «Об электронной подписи» ввел понятие уполномоченного федерального органа в сфере использования электронной подписи, головного удостоверяющего центра, аккредитации удостоверяющих центров, квалифицированного сертификата, сервисов проверки ЭП удостоверяющими центрами, определил, что должен быть зафиксирован момент подписания (т.е. фиксация даты и времени). При этом закон не раскрыл механизмов реализации взаимодействия аккредитованных удостоверяющих центров, ввел очень ограниченные требования по аккредитации удостоверяющих центров, и опять не определил термин “единое пространство доверия электронной подписи”.

В условиях коренных изменений нормативной правовой базы в области электронной подписи, работы 2011 года, проводимые Минкомсвязью России в рамках Государственной Программы Российской Федерации «Информационное общество (2011-2020 годы)» по мероприятию "формирование единого пространства доверия электронным подписям", были направлены в первую очередь на:

разработку модели единого пространства доверия электронной подписи при межведомственном взаимодействии при предоставлении государственных и муниципальных услуг на основе положений ФЗ №63 и ФЗ № 210;

формирование технологических компонент, нормативного правового и технического обеспечения реализации ФЗ №63, инкорпорирование унаследованных технологических компонент, использовавшихся при реализации ФЗ №1.

При этом учитывались принципы гармонизации с международными принципами создания и развития инфраструктуры открытых ключей для создания электронной подписи (далее – ИОК), с общими тенденциями мирового развития в данной области в целях создания интероперабельности в области взаимного международного и национального признания электронных подписей в рамках международных доменов доверия.

Основные принципы и состав необходимых элементов инфраструктуры открытых ключей ИОК определены международными рекомендациями X.842, X.843, RFC 5280.

К базовым элементам ИОК относятся:

- служба управления ключами и сертификатами (удостоверяющие центры) ,
- служба фиксации времени,
- служба реализации проверки подлинности ЭП;
- службы реализации политик безопасности
- службы каталогов сертификатов (реестры сертификатов, реестры отозванных сертификатов, реестр состояния сертификата по сети (OCSP);
- служба атрибутирования (для часто изменяемых атрибутов пользователей);
- служба архивирования электронных документов, переданных на временное или постоянное хранение.

Сравнивая требования ФЗ № 63 и состав ИОК, определенный международными рекомендациями, можно сказать о их гармонизации и едином направлении вектора развития.

Если говорить о конкретных результатах 2011 года, то в первую очередь необходимо отметить:

- создание первой очереди “единого пространства доверия” (далее – ЕПД). В данное пространство доверия вошли 156 удостоверяющих центров различной формы собственности. Работы в рамках создания и апробирования ЕПД показали возможность выработки и использования единой политики в области применения сертификатов, включая использование единой структуры сертификатов и единых политик применения сертификатов, единых критериев реализации ЭП в большом количестве информационных систем различных органов власти, единые и режимы обеспечения работы ЕПД и исполнение норм закона.

Также проведенные работы в 2011 году в рамках создания ЕПД показали возможность выработки консолидированных и единых подходов различных государственных органов власти к решению задач по модернизации и созданию информационных систем с использованием сертификатов и ключей ЭП.

-создание информационной системы головного удостоверяющего центра (ГУЦ) (данный организационно-технический элемент предусмотрен 63-ФЗ), интеграцию с ней информационной системы удостоверяющих центров единого пространства доверия, созданной в рамках Федеральной целевой программы «Электронная Россия (2002-2010 годы)»;

- реализацию и запуск в ГУЦ ряда необходимых для использования электронной подписи сервисов. В их числе: единый сервис проверки сертификата ключа проверки электронной подписи (далее - СКП); сервис фиксации даты и времени; сервис мониторинга функционирования удостоверяющих центров. Указанные результаты имеют высокую практическую значимость, что подтверждается их непосредственным применением при реализации 210-ФЗ, ряд положений которого вступил в силу с 1 октября 2011 года: например, переход на межведомственное электронное взаимодействие при оказании государственных услуг федеральными органами власти был бы невозможен без обеспечения юридической значимости информационного обмена, которая достигается в том числе использованием единого сервиса проверки СКП со стороны единой системы межведомственного электронного взаимодействия (СМЭВ) и самих органов власти.

Элементы инфраструктуры головного удостоверяющего центра по генерации сертификатов и ключей электронной подписи, сервиса проверки прошли апробирование в системе межведомственного взаимодействия на основе созданного Минкомсвязью России единого пространства доверия в целях признания ЭП.

Таким образом, можно сказать, что технологическая основа инфраструктуры открытых ключей, как элемент единого пространства доверия для взаимного признания ЭП в России создана. На последующие годы намечено создание дополнительных сервисов, описанных международными рекомендациями, развитие трансграничного взаимодействия и межведомственного взаимодействия.

Нормативное правовое обеспечение единого пространства доверия в настоящее время определяется нормами ФЗ № 63.

Во исполнение ФЗ № 63 подготовлены, разработаны и находятся в стадии согласования нормативные правовые документы:

Постановление Правительства Российской Федерации «О видах электронных подписей, используемых органами исполнительной власти и органами местного самоуправления, порядке их использования, а также об установлении требований об обеспечении совместимости средств

электронных подписей при организации электронного взаимодействия указанных органов между собой»;

Постановление Правительства Российской Федерации «О порядке использования электронной подписи при обращении за получением государственных и муниципальных услуг»;

Приказ Минкомсвязи России «Об утверждении Правил аккредитации удостоверяющих центров, в том числе порядка проверки соблюдения удостоверяющими центрами требований, которые установлены Федеральным законом «Об электронной подписи» и на соответствие которым эти удостоверяющие центры были аккредитованы»;

Приказ Минкомсвязи России «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи в случае прекращения деятельности аккредитованного удостоверяющего центра» (зарегистрирован в Минюсте России под регистрационным номером № 22329 от 17 ноября 2011 г.);

Приказ Минкомсвязи России «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов а также предоставления информации из таких реестров» (зарегистрирован в Минюсте России от 28.11.2011 под регистрационным номером № 22406).

Также в рамках НИР 2011 года Минкомсвязью России проведены работы по аутентичному переводу необходимых международных технических документов по работе с ЭП, которые могут рассматриваться как основы российских стандартов в области ЭП.

Построение единого пространства доверия в 2012 году

Взаимодействие ГУЦ с другими удостоверяющими центрами.

Модель единого пространства доверия электронной подписи при межведомственном взаимодействии при предоставлении государственных и муниципальных услуг на основе положений ФЗ №63, т.е. взаимодействия удостоверяющих центров, непосредственно связана с технологическими аспектами функционирования удостоверяющих центров определенными международными рекомендациями:

Вариант “а”. “Жесткая” иерархия. Для подчиненного УЦ корневой сертификат выдается головным УЦ. Достоинство – хорошая управляемость системы, но плохая устойчивость. Проверка пользовательского сертификата осуществляется до корневого сертификата головного УЦ. Отказ в любом звене цепи ведет к невозможности проверки пользовательского сертификата. В связи с этим, появляется большие требования к бесперебойному функционированию отдельных звеньев, включая головной УЦ. Данная модель хорошо работает в ведомственных информационных системах с единой системой администрации.

Вариант “б”. Построение иерархии удостоверяющих центров на основе выпуска кроссертификатов, т.е. сертификатов связывающих два удостоверяющих центра с корневыми самоподписанными сертификатами.

Такая система более устойчива, но менее управляема. Устойчивость обеспечивается за счет возможности замены кроссертификатов без потери функционирования удостоверяющего центра, взаимодействующего с головным удостоверяющим центром. При этой модели в целях организации проверки пользовательского сертификата необходимо актуальное отслеживание изменения кроссертификатов.

В связи с тем, что ФЗ № 63 не определил в явном виде модель взаимодействия удостоверяющих центров, то для межведомственного взаимодействия при предоставлении государственных и муниципальных услуг предлагается использовать модель однонаправленной кроссертификации от ГУЦ к любому аккредитованному УЦ. Это позволит организовать взаимодействие ГУЦ с уже существующими удостоверяющими центрами России без существенных финансовых издержек и перевыпуска большого количества ранее выпущенных сертификатов. Данная модель также позволяет организовать проверку пользовательских сертификатов с определенной степенью зависимости от актуальности кроссертиифката и наличия количества звеньев в цепи кроссертификации.

Возможен также и вариант “а” при желании удостоверяющего центра. В соответствии с ФЗ № 63 этот УЦ будет выступать как доверенное лицо ГУЦ.

Сервис проверки сертификатов и электронной подписи.

Как было отмечено ранее, сервис проверки является связующим звеном между информационными системами органов власти, использующих ЭП при межведомственном взаимодействии, и удостоверяющими центрами.

Архитектурно, сервис проверки строится в соответствии с положениями ETSI TS 102 231 v2.1.1 Provision of harmonized Trust Service Provider status information" на основе использования однорангового списка (TSL, Trust Service List). В данный момент это наиболее применяемая модель в западных информационных системах. Причем эта модель выходит за рамки взаимодействия только национальных информационных систем и позволяет строить транснациональное взаимодействие доверия удостоверяющим центрам. Естественно, в основе включения удостоверяющих центров в TSL лежит их соответствие определенным критериям. Это наиболее гибкая на сегодняшний день модель, позволяющая удостоверяющим центрам включать свои корневые сертификаты в TSL вне привязки к национальным головным удостоверяющим центрам. Данная модель еще называется браузерной.

Как работает данная модель? В какой-то момент в TSL-списке появляется более одного УЦ, соответствующего определенным критериям безопасности, качеству предоставления услуг, единой структуре сертификата

и т.д. Информационная система (это может быть сервис проверки) знает этот TSL и доверяет тому, что корневые сертификаты в нем актуальны. Далее, сервис проверки, когда к нему приходит электронный документ с ЭП, проверяет пришедший сертификат пользователя на наличие в нем корневого сертификата из TSL. Если с корневым сертификатом все в порядке, проверяется отсутствие/наличие пользовательского сертификата в списке отозванных сертификатов по точке доступа к выпустившему эти сертификаты УЦ. После этого выносится решение, проверять ЭП на корректность или нет и т.д.

Таким образом, TSL являлся реестром-эталоном, из которого можно брать и актуальные кроссертификаты при проверке ЭП. По этой гибкой модели работает сервис проверки головного УЦ. Производительность данного сервиса ~ 100 обращений/сек. Этот сервис прошел апробацию и в настоящее время постоянном режиме обеспечивают функционирование СМЭВ.

Важной функцией данного сервиса является проверка качества деятельности удостоверяющего центра. Это в первую очередь относится к актуальности и возможности доступа к спискам отзыва сертификатов. Для оценки возможности доступа разработан сервис мониторинга, который с определенной скважностью (~5 мин.) проверяет доступность списков отзыва.

На 2012 год намечено расширение функциональных возможностей данного сервиса, его производительности и взаимодействия не только со СМЭВ, но и с другими информационными системами.

Сервис фиксации даты и времени под электронным документом

Требование по фиксации даты и времени заложены как в мировых рекомендациях, так и в ФЗ № 63.

На сегодняшний день вопрос обеспечения единого времени приобрел особую актуальность. Единое время необходимо для работы транспорта, связи, энергетики, различных финансовых учреждений и банков. В связи с широким применением компьютерных сетей возникла проблема достижения единого времени во всех устройствах сети. Правильная обработка данных в системах реального времени невозможна без синхронизации по времени. В системах защиты информации привязка сообщения к конкретной временной метке позволяет защитить сообщение от изменения при передаче по сети. Для решения этих задач системная шкала времени компьютеров сети должна быть синхронизирована с всемирно шкалой времени UTC.

Единое время (метки/штампы времени) также играют важную роль и в рамках инфраструктуры открытых ключей. Так необходимыми атрибутами каждого сертификата открытого ключа, выдаваемого Удостоверяющим Центром, являются сроки и дата начала действия сертификата, определяющие/задающие временные рамки ограничивающие его использования в качестве средства обеспечения доверительных отношений. Аналогичные атрибуты включают в себя и списки отозванных сертификатов.

В последнее время в эксплуатацию вводятся системы, оперирующие со службами штампов времени (TSP), службами OCSP, связанные в частности с активным внедрением стандартов улучшенной (расширенной) ЭП (CAdES), которые предполагают для своего функционирования активное использование штампов времени и OCSP ответов. Поставщиками штампов времени и OCSP ответов при этом являются территориально-распределённые системы, часто организационно-независимые. Потребитель услуг служб при этом часто является пользователем нескольких информационных систем. Соответственно, такой потребитель имеет дело с несколькими независимыми шкалами времени, каждая из которых определяет/задает независимые временные ограничения на степень доверия.

Иными словами каждая независимая третья доверенная сторона (УЦ, службы TSP, OCSP, т.д.) гарантирует/предоставляет пользователю средства обеспечения мер доверия, но только в рамках *своей* независимой шкалы времени!

Таким образом, задача ведения единой шкалы времени для служб Удостоверяющих Центров, объединяемых общим пространством доверия (аккредитованных УЦ), а также для потребителей услуг УЦ является задачей актуальной.

В рамках работ 2011 года были проведены мероприятия по созданию элементов инфраструктуры – источников точного времени и их синхронизации с общероссийскими системами точного времени. На 2012 год намечено продолжение работ по разработке методологии использования точного времени и штампов времени в части включения в состав электронной подписи и в сообщения, используемые в межведомственном электронном документообороте.

Сервисы реестров.

В рамках ФЗ №1 в функции уполномоченного органа в области электронной цифровой подписи было включено ведение реестров сертификатов ключей подписей уполномоченных лиц удостоверяющих центров и реестра сертификатов уполномоченных лиц федеральных органов государственной власти. Если первый реестр полностью был востребован в связи с формулировкой ФЗ №1, что до начала своей деятельности удостоверяющие центры обязаны внести корневые сертификаты в реестр, то второй реестр только сейчас начинает развиваться в связи с реализацией ФЗ № 210 и найдет свое развитие в ЕСИА - Единой системе идентификации и аутентификации, определенной Постановлением Правительства № 977.

В рамках мероприятий ГП “Информационное общество” проводятся работы по разработке программного обеспечения ведения данных реестров и предоставления доступа к информации и использованием информационно-телекоммуникационной сети Интернет.

Единая структура сертификата ключа проверки электронной подписи

Единая структура сертификата ключа проверки электронной подписи, наряду с сервисом проверки является наиболее важной частью ЕПД. Однозначное чтение и толкование значений полей сертификата является залогом правильной работы как отдельных информационных систем, так и взаимодействия нескольких систем. В мировой практике структура сертификата определена рекомендациями ITU-T X.509 и IETF rfc 5280, 3739. В целях выработки данных рекомендаций были реализованы мировые проекты, в которых участвовали производители программного обеспечения удостоверяющих центров различных стран мира.

Во исполнение ФЗ № 63 приказом ФСБ России «Об утверждении требований к форме квалифицированного сертификата ключа проверки подписи» (рег.№ 23041 от 27.01.2012» определены основные поля квалифицированного сертификата, который будут формировать аккредитованные удостоверяющие центры.

В дополнение к стандартным полям, определенными международными рекомендациями, добавлены поля, описывающие требования по информационной безопасности, требования ФЗ № 63 по идентификации физических и юридических лиц. Также в сертификат в соответствие с ФЗ № 63 вносятся требования по возможности включения различной информации по желанию заявителя. Эти требования отличаются от международных и требуют проработки вопроса по выработке рекомендаций по заполнению этих полей для однозначного толкования разработчиками программного обеспечения информационных систем и удостоверяющих центров. Данные рекомендации должны быть подготовлены в течение ближайшего времени и представлены общественности. До согласования этих рекомендаций структура сертификата, используемого в СМЭВ, размещена на техническом портале СМЭВ в составе Методических рекомендаций по использованию электронной подписи при межведомственном электронном взаимодействии.

Вопросов, которые возникли и возникают по построению единого пространства доверия и в связи с принятием ФЗ № 63 «Об электронной подписи» много. В целом же, принятие нового закона об электронной подписи "перезапустило" формирование единого пространства доверия электронной подписи, изменив условия, в которых формировались и использовались обеспечивающие технологические элементы электронной подписи.

В этой связи говорить о завершении формирования ЕПД можно будет только после выпуска всех нормативных правовых актов, предусмотренных 63-ФЗ, введения в действие процедуры аккредитации удостоверяющих центров, приведения программно-технических средств действующих УЦ в соответствие требованиям, выдвигаемым ФСБ России, как органом,

уполномоченным в области безопасности, и Минкомсвязи России, как органом, уполномоченным в области ЭП.

Необходимые для реализации ФЗ №63 технологические элементы, относящиеся к инфраструктуре электронного правительства, уже созданы в 2011 году в рамках программы «Информационное общество», и будут развиваться в 2012 году в рамках этой же программы.