
Министерство связи и массовых коммуникаций Российской Федерации

Министерство по чрезвычайным ситуациям Российской Федерации

Федеральное агентство по информационным технологиям

Федеральная антимонопольная служба

Федеральная служба безопасности Российской Федерации

Федеральная налоговая служба

Управление специальной связи и информации Федеральной службы охраны Российской Федерации в Северо-Западном федеральном округе

Правительство Санкт-Петербурга

Комиссия таможенного союза

Центральный Банк Российской Федерации

ОАО «Газпром»

ОАО «Ростелеком»

Межрегиональная общественная организация

«Ассоциация защиты информации»

**Технический комитет по стандартизации (ТК 26)
«Криптографическая защита информации»**

Ассоциация Электронных Торговых Площадок

МЕМОРАНДУМ

восьмой международной научно-практической конференции

«РКИ-Форум Россия 2010»

28 сентября – 01 октября 2010 года в Санкт-Петербурге, при поддержке Министерства связи и массовых коммуникаций Российской Федерации состоялась восьмая ежегодная международная научно-практическая конференция «РКИ-Форум Россия 2010».

В ней приняли участие более 160 представителей из 8 стран Европы и СНГ, включая Беларусь, Бельгию, Казахстан, Латвию, Литву, Польшу, Российскую Федерацию, Украину.

От Российской Федерации в работе конференции участвовали руководители и специалисты 38 удостоверяющих центров, 14 федеральных органов власти, 6 региональных органов власти, 32 предприятий различных форм собственности, 3 учебных заведений, 6 общественных организаций.

На пленарном и четырех секционных заседаниях «PKI-Форум Россия 2010» были представлены 34 доклада, проведено 3 круглых стола и заседание экспертного совета.

В рамках работы секций и круглых столов был рассмотрен опыт удостоверяющих центров, производителей, интеграторов, эксплуатирующих организаций по вопросам внедрения и эксплуатации систем, использующих сервисы инфраструктуры открытых ключей. Участники конференции подвели итоги за год практической деятельности в сфере применения PKI в информационных системах предприятий и организаций, выявили проблемные вопросы отрасли, а также наметили конкретные цели по развитию PKI, расширению практики применения данных технологий на 2011 год.

Главной особенностью «PKI-Форума» в 2010 году явилось то, что он проходил в период подготовки ко второму чтению законопроекта «Об электронной подписи» и в период передачи функций федерального уполномоченного органа в области ЭЦП от Федерального агентства по информационным технологиям в Министерство связи и массовых коммуникаций Российской Федерации.

На форуме рассмотрены и обсуждены новые документы нормативно-правового регулирования в области электронного правительства, предоставления государственных и муниципальных услуг в электронном виде (Распоряжение правительства РФ от 13 мая 2010 г № 722-р «О подписании Соглашения о применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории таможенного союза», Федеральный закон от 27.07.2010 №210-ФЗ «Об организации оказания государственных и муниципальных услуг», Постановление Правительства от 8 сентября 2010г № 697 «О единой системе межведомственного электронного взаимодействия», Постановление Правительства РФ от 15 июня 2009 г № 478 «О единой системе информационно-справочной поддержки граждан и организаций по вопросам взаимодействия с органами исполнительной власти и органами местного самоуправления с использованием информационно-справочной сети Интернет» , нормативно-правовые акты Минкомсвязи России и Росинформтехнологии, определяющие порядок подтверждения соответствия УЦ для работы в системах оказания государственных и муниципальных услуг (Приказ Минкомсвязи России № 41 (зарегистрирован Минюстом России № 13831 от 24.04.2009) «Об утверждении Требований к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам

подсистемы удостоверяющих центров общероссийского государственного информационного центра» и приказ Росинформтехнологии № 144 «Об утверждении временного порядка присоединения удостоверяющих центров к подсистеме удостоверяющих центров общероссийского государственного информационного центра»). Признано, что данные нормативно-правовые акты являются значительным шагом в области регулирования деятельности удостоверяющих центров и упорядочивания использования сервисов PKI в информационных системах электронного правительства.

Одной из главных тем Форума стала тема единого пространства доверия сертификатам ключей подписей (ЕПД). Рассмотрены правовые и технологические аспекты создания и функционирования ЕПД, информация о имеющихся решениях, в частности о статусе системы УЦ (СУЦ) ОГИЦ как возможной технологической основы создания ЕПД. Отмечено, что для эффективного функционирования ЕПД необходим целый комплекс первоочередных мер, в частности:

- На уровне федерального закона необходимо урегулировать нормативно –правовые и технологические аспекты установления доверия сертификату открытого ключа, а также доработать в целом нормативную правовую, нормативную техническую и технологическую базу PKI с привлечением к этому процессу уполномоченных органов в части касающейся;
- определить границы ЕПД и регламент его функционирования при создании систем электронного правительства;
- определить требования по интеграции с технологиями ЕПД универсальной электронной карты (УЭК), как средства доступа гражданина к электронному правительству, а именно определить необходимость использования в УЭК сертификатов открытых ключей и российской криптографии, как наиболее эффективного и легитимного средства идентификации физического лица в информационной среде.
- стандартизировать форматы контейнеров для хранения закрытых ключей;
- стандартизировать интерфейсы взаимодействия СКЗИ со средой функционирования;
- использовать положительный опыт создания крупных корпоративных ЕПД (Федеральной налоговой службы, Пенсионного фонда РФ, ОАО «Газпром», ОАО «РЖД» и др.)

Вместе с тем отмечено, что ведомственный подход в вопросах аккредитации УЦ приводит к «лоскутности» ЕПД и, как следствие, подмене самого понятия ЕПД. Ведомственные системы аккредитации в современных условиях приводят к еще большей фрагментации ЕПД, что противоречит поручению Президента Российской Федерации от 01.08.2008 № 1572ГС о создании единой системы удостоверяющих центров в интересах «электронного правительства». Ярким примером такого ведомственного подхода является система аккредитации удостоверяющих центров на электронных торговых площадках, предложенная Министерством экономического развития Российской Федерации, Федеральной антимонопольной службой и ЗАО «Сбербанк-АСТ».

На форуме неоднократно отмечено, что наблюдается прирост PKI-ориентированных систем в различных сегментах рынка. Возрастает количество федеральных законов и нормативных актов Президента Российской Федерации и Правительства Российской Федерации, определяющих необходимость использования ЭЦП. Возрастает и количество пользователей таких систем. Ярким примером здесь является Федеральный закон № 94-ФЗ, Концепция создания Интегрированной информационной системы внешней и взаимной торговли таможенного союза, одобренная Решением Межгосударственного Совета ЕврАзЭС (высшего органа таможенного союза) на уровне глав государств от 27 ноября 2009 г. № 22, постановление Правительства Российской Федерации № 697 от 08.09.2010 и др.

Большое внимание участники конференции уделили теме Трансграничной интероперабельности PKI. Актуальность этой темы определяется рядом межгосударственных инициатив (в рамках АТЭС, ЕврАзЭС, КТС, ШОС и др. объединений), требованиями ряда нормативных актов, определяющих порядок взаимодействия с иностранными контрагентами, а так же интересами B2B. В этой связи отмечено, что технологии PKI являются эффективным решением, на базе которого безопасные интероперабельные решения успешно строятся в трансграничных информационных процессах прогрессивных стран, в том числе в проектах электронного правительства и информационного общества. В ряде докладов отечественных и зарубежных экспертов прозвучало подтверждение того факта, что поиск эффективных решений задачи трансграничной интероперабельности электронной цифровой подписи и строгой идентификации одинаково актуальны для России, Союзного государства Россия-Белорусь, Евросоюза, стран СНГ, ЕврАзЭС, ШОС и других межгосударственных объединений. В частности представители стран Евросоюза обратили внимание на эффективность применения браузерной модели доверия при построении ЕПД на основе списков доверенных сервисов – TSL, в соответствии со стандартом ETSI TS 102 231 V3.1.2 и Решением Комиссии ЕС 2009/767/ЕС от 16 октября 2009 года. Значительный интерес участников форума в этой части вызвали представленные Международной ассоциацией «Электронная подпись без границ» практические решения по обеспечению интероперабельности PKI, инвариантные к используемым криптографическим алгоритмам, позволяющие учесть особенности локальных законодательств в области электронной подписи и электронного документооборота.

Основными прикладными задачами, требующими трансграничной интероперабельности на протяжении ряда последних лет были и остаются задачи электронной торговли и задачи предварительного декларирования. Требование ст. 13 Федерального закона № 94-ФЗ, определяющее равный правовой режим для товаров и услуг, происходящих из иностранных государств, предполагает наличие технологий трансграничной интероперабельности ЭЦП участников электронных торговых площадок государственного заказа. Представители организаций – участников рынка электронных торговых площадок (Ассоциация электронных торговых площадок, удостоверяющий центр «Газинформсервис» и др.) доложили на форуме о своей готовности оказания трансграничных услуг PKI участникам электронных торгов.

При этом на Форуме отмечено, что проблемы интероперабельности информационных технологий и средств защиты информации различных производителей

частично могут быть решены в рамках деятельности технических комитетов (ТК) по стандартизации, действующих в системе технического регулирования России. В частности, в ТК26 «Криптографическая защита информации» уже ведутся работы по выработке согласованной позиции в части использования контейнеров хранения криптографических ключей, которая актуальна как для реализации положений ФЗ-1, в части касающейся функций уполномоченного федерального органа по проверке подписей уполномоченных лиц органов государственной власти, так и в части обеспечения ЕПД.

В ряде докладов участников процесса подготовки ко второму чтению законопроекта «Об электронной подписи» отмечено множество слабых мест законопроекта (см. Приложение).

Значительный интерес участников форума вызвал доклад директора проекта «Электронное Правительство» ОАО «Ростелеком» В.С.Зубахи. Положительно оценены представленные позиции единого оператора в области создания электронного правительства по вопросам технологий ЕПД, универсальной электронной карты с сертификатами ключей подписей в качестве средства идентификации при получении государственных и муниципальных услуг, использования СУЦ ОГИЦ в качестве технологической основы для создания ЕПД.

В докладах по проблематике электронного правительства, как одной из базовых сфер применения сервисов PKI, неоднократно прозвучала необходимость использования широкого спектра сервисов PKI в интересах прикладных задач, в том числе сервисов подтверждения подлинности (Validation), сервисов меток времени, атрибутивных сертификатов и пр., в соответствии с международным стандартом X.842. При этом экспертным сообществом отмечена, при широком использовании данных сервисов, необходимость обязательного технического регулирования данной проблемной области, которое в России в настоящее время отсутствует.

В ходе Форума обсуждены актуальные нормативно-правовые акты в области межведомственного электронного взаимодействия органов государственной власти. Большой интерес вызвало типовое решение по организации и построению регионального сегмента таких электронных сервисов, как элементов сервисов доверенной третьей стороны (ДТС), реализованное в Ставропольском крае.

Значительное внимание участников Форума было уделено вопросам организации работы уполномоченного федерального органа по ЭЦП в переходный период и основным тенденциям во взаимоотношениях уполномоченного федерального органа и участников рынка. В частности, отмечено повышение потребительской активности в отношении функций УФО, в том числе в вопросах подтверждения подлинности сертификатов ключей подписей, предоставления сведений из единого реестра сертификатов ключей подписей уполномоченных лиц удостоверяющих центров.

Участники форума отметили значительное продвижение в вопросах стандартизации и трансграничной интероперабельности PKI в результате работы технического комитета ТК26, основным результатом работы которого в части трансграничного взаимодействия является последовательное включение российских криптографических стандартов в число международных стандартов.

Одной из ключевых тем Форума стал вопрос о возможности и целесообразности использования механизмов саморегулирования (СРО) деятельности удостоверяющих центров. На круглом столе, посвященном этой теме, был рассмотрен международный опыт регулирования отрасли услуг доверенной третьей стороны, рассмотрены актуальные проблемы отрасли, которые могли бы быть разрешены в рамках СРО, озвучены требования участников рынка услуг УЦ к возможным условиям участия в СРО. По мнению участников круглого стола, в рамках которого обсуждался вопрос СРО удостоверяющих центров, исследование вопросов целесообразности саморегулирования деятельности удостоверяющих центров в настоящее время актуально.

С особым вниманием представители РКІ-сообщества восприняли доклады потребителей - экспертов в области информатизации здравоохранения, банковской деятельности и систем электронного документооборота, с изложением требований прикладных задач к функционалу РКІ. Отмечены следующие наиболее важные аспекты:

- РКІ в ряде прикладных задач становится элементом систем реального времени и к ней предъявляются соответствующие требования по надежности и живучести;
- Совместимость технологий РКІ и электронного правительства с решениями на основе технологий мобильной связи. Рассмотрение мобильного телефона как наиболее распространенного вычислительного и коммуникационного устройства.
- Использование РКІ в системах документооборота требует комплексного системного подхода к обеспечению базовых характеристик электронных документов (аутентичность, целостность, достоверность, юридическая сила) на протяжении всего жизненного цикла электронного документа.

На проведенном в рамках «РКІ-Форум 2010» совещании экспертов по вопросам нотариата и электронных государственных услуг были рассмотрены вопросы аутентификации участников процессов оказания и получения государственных услуг в электронной форме, проблемы неправомерного ограничения конкуренции в системах электронных закупок в связи с применением электронных систем (проблемы, способы и пути решения), иные актуальные вопросы практического применения РКІ при размещении государственного и муниципального заказа.

Участники отметили возросший уровень Форума и глубину рассматриваемых на мероприятиях Форума вопросов, степень зрелости представляемых на конференции РКІ-ориентированных продуктов и решений. По общему мнению «РКІ-Форум Россия» за свою восьмилетнюю историю стал эффективной площадкой для обмена мнениями и рассмотрения актуальных вопросов в области РКІ-проблематики как на национальном, так и на международном уровне. Это обусловлено множеством факторов, в том числе тем, что проблематика РКІ насыщена нетривиальными и многогранными вопросами, важность эффективного решения которых в настоящее время в условиях общемировых тенденций динамичного развития технологий электронного правительства и информационного общества трудно переоценить.

Заслушав и обсудив круг вопросов, связанных с использованием инфраструктуры открытых ключей, участники Конференции решили:

1. Представить настоящий Меморандум в Комитеты Государственной Думы по финансовому рынку и по безопасности, в ведении которых в настоящее время находится законопроект «Об электронной подписи».
2. Привлечь внимание участников процесса создания ЭП (ОАО «Ростелеком», ООО «Универсальная электронная карта») к позиции РКІ-сообщества по ключевым вопросам, затронутым в настоящем Меморандуме и других материалах Форума, с целью рассмотрения ими возможностей использования предложений и компетенций РКІ-сообщества при решении базовых задач создания электронного правительства, в том числе работ по созданию единого пространства доверия СКП и универсальных средств идентификации граждан при получении государственных (муниципальных) услуг.
3. Привлечь внимание Минкомсвязи России к проблемным вопросам организации эксплуатации СУЦ ОГИЦ, как возможной технологической основы ЕПД, включая необходимость функционирования и развития федерального удостоверяющего центра на базе уполномоченного органа исполнительной власти в области использования ЭЦП.
4. Проинформировать Росстандарт и Минкомсвязи России о необходимости разрешения проблемы двойственной идентификации в системах объектных идентификаторов ISO и ITU отечественных криптографических алгоритмов.
5. Признать целесообразным подход, ориентированный на адаптацию международных стандартов в области РКІ и криптографии регламентирующих вопросы применения криптографических механизмов защиты.
6. Программному комитету РКІ-Forum в рамках работы интернет-портала РКІ-Forum организовать раздел для обсуждения темы СРО удостоверяющих центров.
7. Рекомендовать МОО «АЗИ» рассмотреть вопрос об обращении в Минкомсвязи России с предложением по разработке концептуальных вопросов СРО удостоверяющих центров в рамках финансирования ФЦП «Электронная Россия» и последующего привлечения потенциала СРО к разработке проектов нормативных технических документов по формированию и функционированию ЕПД.
8. Предложить МОО «АЗИ» обратиться в Росстандарт и Росархив с обоснованием необходимости ускорения процесса разработки стандарта контейнера ЭД, включающего форматы для идентификационной информации и реквизитов ЭД с целью унификации обмена ЭД между различными системами ЭДО на межкорпоративном и государственном уровне и создания единого российского пространства ЭДО.
9. С целью дальнейшей совместимости СКЗИ различных разработчиков и повышения удобства потребителей в части возможности работы с одним закрытым ключом и сертификатом в различных защищенных системах с одним уровнем требований по информационной безопасности, рекомендовать при построении государственных систем с применением ЭЦП использовать СКЗИ с поддержкой формата хранения ключевого носителя, разрабатываемого в рамках ТК26.
10. Проинформировать Минкомсвязи России и ФСБ России в части касающейся о целесообразности активного использования лучших практик и наработок, полученных в рамках реализации крупных европейских проектов по интероперабельности взаимодействия информационных систем, электронным закупкам и использованию электронной подписи, в ходе формирования единой правовой и технической политики в стране.
11. Проинформировать Секретариат Комиссии Таможенного союза по следующим вопросам:

- a. При формировании Координационного совета по информационным технологиям при Комиссии Таможенного союза, целесообразно в его состав высококвалифицированных специалистов в области защиты информации от соответствующих ведомств государств-членов Таможенного союза.
 - b. При разработке и внедрении информационной интегрированной системы внешней и взаимной торговли целесообразно обратить внимание на использование передовых технологий информационной безопасности, которые не были бы обременительны для бизнеса.
12. С целью оптимизации затрат на использование и внедрение прикладных сервисов РКІ в различные информационные, в том числе - государственные системы предложить сообществу рассмотреть возможность разработки и адаптации пакета рекомендаций, определяющих зависимость таких затрат от качества реализуемых сервисов и требований по информационной безопасности.
 13. Проинформировать Министерство экономического развития Российской Федерации, Федеральную антимонопольную службу и операторов электронных торговых площадок государственного заказа о противоречивости реализуемого в настоящее время подхода по созданию ведомственных систем аккредитации УЦ и поручения Президента РФ от 01.08.2008 № 1572ГС о создании единой системы удостоверяющих центров в интересах «электронного правительства», а также на то, что реализация ведомственных правил аккредитации УЦ является способом неправомерного ограничения конкуренции на рынке услуг РКІ.
 14. Поддерживать инициативы компаний ИнфоТеКС и СигналКом по бесплатному распространению СКЗИ собственного производства для физических лиц и государственных структур в рамках систем государственных услуг и государственных функций в электронном виде.
 15. Проинформировать Федеральное агентство по техническому регулированию и метрологии о необходимости разработки значительного количества стандартов в области РКІ в интересах создания ЕПД и обеспечения интероперабельности технологий РКІ, подготовить и направить в ТК26 соответствующие предложения в Программу разработки национальных стандартов.
 16. Проинформировать Минкомсвязи России о целесообразности проработки и представления на очередной совет Ростехрегулирования в ноябре 2010 года предложений по активизации в рамках профильных технических комитетов решения вопросов разработки пакета стандартов в области РКІ.
 17. Проинформировать Минкомсвязи России о целесообразности войти в ТК26 с инициативой о включении представителя Минкомсвязи России в состав ТК26.
 18. Проинформировать Минкомсвязи России о целесообразности развертывания общенациональной рекламной компании по вопросам формирования нового менталитета в отношении использования электронных государственных услуг и средств строгой аутентификации и электронной цифровой подписи.
 19. Считать целесообразным проведение очередной IX международной научно-практической конференции «РКІ-Форум Россия 2011» в Санкт-Петербурге в 2011 году.

Участники конференции выражают искреннюю **благодарность**:

Устроителям Форума за проделанную на высоком уровне работу по организации и проведению мероприятия.

Представителям иностранных делегаций за неоценимую информацию, предоставленную в докладах и презентациях, об опыте стран ЕС и СНГ в области использования РКІ.

Официальным партнерам Форума - компаниям Ростелеком, Газинформсервис, ИнфоТекС, партнерам деловой программы компаниям ОКБ «САПР», «Центр Информ», «Актив», информационным партнерам за финансовую, информационную и организационную поддержку конференции.

Правительственным организациям и жителям Санкт-Петербурга за теплый прием и заботу об участниках конференции в рамках деловых и культурных мероприятий программы Форума.

По поручению Оргкомитета восьмой ежегодной международной научно-практической конференции «РКІ-Forum Россия 2010»

Сопредседатель оргкомитета «РКІ-Форум Россия 2010», Председатель
МОО «Ассоциация защиты информации»

Емельянов Г.В.

Сопредседатель оргкомитета «РКІ-Форум Россия 2010», И.о.
Руководителя Росинформтехнологии

Лапшин А.В.

Замечания и предложения участников восьмой международной научно-практической конференции «РКИ-Форум Россия 2010» по законопроекту «Об электронной подписи»

1. Непроработанность вопросов информационной безопасности технологий, предусмотренных законопроектом. В этой связи отмечено, что без учета вопросов безопасности – технология нежизнеспособна.
2. Эксперты рассматривают введение понятия простой электронной подписи как попытку введения в заблуждение массового потребителя.
3. Недооценка криптографических технологий, как средства, позволяющего внедрить в информационный процесс человеконезависимый элемент, позволяющих тем самым, повысить надежность функционирования механизмов электронной подписи.
4. Отсутствие в законопроекте критериев выбора вида электронной подписи в зависимости от области применения и других условий.
5. Не раскрыты правовые последствия признания равнозначности собственноручной подписи и каждого из трех видов электронной подписи.
6. Необходимо введение нормы, определяющей, что необходимым условием признания равнозначности ЭП и собственноручной подписи является положительный результат проверки ЭП.
7. Неопределенность собственно понятия равнозначности собственноручной подписи и трех видов электронной подписи;
8. Отсутствие в законопроекте указаний на разработку соответствующих подзаконных актов;
9. Необходимость четкого определения сфер, где применять простую электронную подпись нельзя. Участники Форума акцентируют внимание Законодателей, что простая электронная подпись ни при каких обстоятельствах не может быть признана аналогом собственноручной.
10. Применение простой ЭП не меняет ничей правовой статус, следовательно, не требует законодательного регулирования.
11. В увязке с вопросами интероперабельности технологий, а также в связи с тем, что одной из идей введения новых типов подписей – простой и усовершенствованной, является гармонизация с соответствующими подходами в Евросоюзе, отмечено, что в соответствии с директивой 1999/93/ЕС только квалифицированная подпись является трансграничной.