



Генеральная Ассамблея

Distr.: Limited
2 September 2015
Russian
Original: English

Комиссия Организации Объединенных Наций

по праву международной торговли

Рабочая группа III (Урегулирование споров в режиме онлайн)

Тридцать вторая сессия

Вена, 30 ноября – 4 декабря 2015 года

Урегулирование споров в режиме онлайн применительно к трансграничным электронным коммерческим сделкам

Документ, представленный Российской Федерацией

Записка Секретариата

Правительство Российской Федерации представило в Секретариат документ с изложением видения и концептуальных подходов в отношении урегулирования споров в режиме онлайн применительно к трансграничным электронным коммерческим сделкам. Документ был представлен в Секретариат до проходившей ранее сессии Рабочей группы III (Урегулирование споров в режиме онлайн), но теперь он передан Рабочей группе. Полученный Секретариатом текст воспроизводится в приложении к настоящей записке в том виде, в котором он был получен.

* Переиздано по техническим причинам 4 ноября 2015 года.



Приложение

Видение и концептуальные подходы к разработке в специализированных учреждениях Организации Объединенных Наций и в соответствующих международных организациях совокупного свода рекомендаций по формированию и функционированию трансграничного пространства доверия

Введение

Под "трансграничным пространством доверия" (далее в тексте – ПД-Т) предлагается понимать сочетание правовых, **организационных и технологических условий, рекомендуемых соответствующими специализированными учреждениями (департаментами) Организации Объединенных Наций и** международными организациями с целью обеспечения доверия (уверенности в подлинности) при международном обмене электронными документами и данными между сторонами (субъектами), взаимодействующими в электронной форме.

Под "сторонами (субъектами), взаимодействующими в электронной форме" предлагается понимать всю совокупность публичных органов, физических и юридических лиц, взаимодействующих в рамках отношений, возникающих в результате создания, отправки, передачи, получения, хранения и использования электронных документов и данных.

Эти предложения преследуют цель определить подходы и вопросы, которые будут обсуждаться в контексте разработки свода рекомендаций по формированию и функционированию трансграничного пространства доверия (рекомендации по ПД-Т) в соответствующих организациях системы Организации Объединенных Наций. Они призваны облегчить создание технологической, институциональной и правовой инфраструктуры для практического использования рекомендаций по ПД-Т.

Принять участие в этом обсуждении приглашаются заинтересованные делегаты и эксперты из государственных учреждений и деловых кругов.

Возможная роль ВТО и ее вклад в формирование и функционирование ПД-Т. Создание ПД-Т будет способствовать упрощению процедур и развитию международной торговли, а внимание со стороны ВТО к вопросам ПД-Т поможет заручиться поддержкой со стороны правительств и деловых кругов в деле практической реализации этой идеи. Другой проблемной областью является отсутствие координации в работе (а зачастую и операционной совместимости конечных результатов) многочисленных международных и региональных организаций (например, ИСО, МСЭ, СЕФАКТ/ЕЭК ООН, ЮНСИТРАЛ, АТЭС и т.д.), которые занимаются разработкой электронных стандартов и смежными вопросами. Возложение на ВТО координирующей роли в этом процессе повысит эффективность и действенность усилий по осуществлению международной стандартизации в данной области.

Концептуальные подходы

1. Рекомендации по ПД-Т предлагается сориентировать на обеспечение гарантии прав и законных интересов граждан и организаций, находящихся под юрисдикцией государств – членов Организации Объединенных Наций, при осуществлении юридически значимых информационных операций в электронной форме с использованием Интернета и других открытых систем ИКТ массового использования.
2. Упомянутые институциональные гарантии предлагается обеспечивать в рамках коммерческой деятельности специализированных операторов, которые:
 - предоставляют пользователям набор доверенных услуг ИКТ;
 - работают в рамках авторитетных правовых режимов, которые включают – но не ограничиваются этим – ограничения, введенные в связи с обработкой персональных данных.
3. Предлагается дать описание различных возможных правовых режимов:
 - основанные на международных соглашениях (конвенциях) и/или на прямо применяемых международных нормах;
 - основанные на коммерческих соглашениях и/или общей торговой практике;
 - без специального международного регулирования.

Правовые режимы могут получать дополнительную поддержку со стороны традиционных институтов (правительственные органы, урегулирование в судебном порядке, страхование рисков, нотариат и другие) благодаря взаимному признанию электронных документов, подкрепляемых доверенными услугами в области ИКТ.

Авторитетные правовые режимы могут также предусматривать введение особых требований в отношении материальной и финансовой поддержки коммерческой деятельности специализированных операторов в случае причинения ими ущерба своим пользователям, включая случаи компрометации персональных данных.

Вопросы институциональных гарантий и правовых режимов, связанных с формированием и функционированием региональных и глобальных кластеров ПД-Т, а также с функциональными услугами, предоставляемыми в рамках этих кластеров, предлагается рассмотреть в отдельной рекомендации ЮНСИТРАЛ.

4. Предлагается дать описание возможных наборов доверенных инфраструктурных услуг в области ИКТ с учетом степени важности функциональных прикладных применений. Услуги и нынешний уровень доверия к ним могут определяться операторами функциональных информационных систем с учетом угроз, рисков, согласованных правовых режимов и потребностей пользователей. Для того чтобы обеспечить необходимый уровень доверия операторы функциональных информационных систем могли бы работать в нейтральных международных условиях, определяемых конкретными правовыми режимами. Предлагается дать описание организационных инфраструктур, необходимых для создания и поддержания нейтральных международных условий.

Общие положения, касающиеся формирования и функционирования региональных и глобальных кластеров ПД-Т, функциональных услуг, предоставляемых в рамках этих кластеров, а также наборов доверенных инфраструктурных услуг в области ИКТ можно рассмотреть в рамках разработанной СЕФАКТ/ЕЭК/ООН "Рекомендации по обеспечению юридически значимого доверительного трансграничного электронного взаимодействия".

Описание отдельных доверенных услуг в области ИКТ может стать предметом технических стандартов и рекомендаций МСЭ, ОТК 1, ЕТСИ и других структур.

5. Наборы отличительных признаков для целей идентификации могут определяться правовыми режимами, регулирующими коммерческую деятельность операторов, специализирующихся на выполнении задач идентификации, и функциональных операторов, и могут подкрепляться соответствующими доверенными услугами в области ИКТ. Деятельность операторов может регулироваться специальными организационными и техническими требованиями, направленными, помимо прочего, на защиту персональных данных.

Наборы отличительных признаков для целей идентификации и сами процедуры идентификации могут служить основой для определения уровней доверия в системах идентификации. Такие уровни доверия могут иметь важнейшее значение для регулирования взаимодействия между различными кластерами доверия (см. пункт 9).

6. Предлагается дать описание механизмов взаимодействия отдельных государств и их международных объединений с другими международными структурами в рамках формирования общего ПД-Т:

6.1. на основе присоединения к существующему правовому режиму, который обеспечивает институциональные гарантии субъектам электронного взаимодействия:

- полное присоединение государства к существующему правовому режиму на основе международных договоров и/или прямо применяемых международных норм, в которых уже поставлена или решена задача по формированию регионального ПД-Т, включая функциональные услуги, предоставляемые в рамках этого ПД-Т;
- частичное присоединение государства к существующему правовому режиму на основе международных договоров и/или прямо применяемых международных норм в части положений, касающихся формирования регионального и/или функционального ПД-Т;

6.2. на основе взаимодействия между различными международными объединениями:

- на первом этапе группа государств создает изолированный региональный кластер ПД-Т, включая функциональные услуги ПД-Т, предоставляемые в рамках этого ПД-Т, предоставляя институциональные гарантии субъектам электронного взаимодействия в рамках правового режима, определяемого этими государствами;

- на втором этапе определяются протоколы доверительного взаимодействия с другими международными объединениями в связи с взаимным признанием различных правовых режимов. Такое взаимное признание должно учитывать институциональные гарантии и требования информационной безопасности, относящиеся к каждой из международных структур, возможно, на основе шлюзов информационной безопасности (ШИБ), функционирующих в рамках специальных правовых режимов;

6.3. на основе взаимодействия государства с другими государствами или международными объединениями:

- на первом этапе государство создает изолированный национальный кластер ПД-Т, функционирующий в рамках национального правового режима, определяемого этим государством;
- на втором этапе определяются протоколы доверительного взаимодействия с другими государствами и/или международными объединениями в связи с взаимным признанием различных правовых режимов. Такое взаимное признание должно учитывать институциональные гарантии и требования информационной безопасности, относящиеся к этим государствам и международным структурам, возможно, на основе шлюзов информационной безопасности (ШИБ), функционирующих в рамках специальных правовых режимов.

7. Предлагается дать описание механизмов создания кластеров по аналогии с пунктом 6 для правовых режимов, основанных на коммерческих соглашениях и/или общей торговой практике.

8. Предлагается дать описание механизмов формирования глобального ПД-Т на основе объединения различных кластеров в одну матрицу, построенную в соответствии со следующими характеристиками:

- функциональные услуги и региональная сфера охвата;
- различные правовые режимы и их разновидности.

9. Предлагается дать описание подходов к созданию нескольких видов шлюзов информационной безопасности (ШИБ) как ключевых элементов построения глобальной матрицы ПД-Т.

Целью создания таких шлюзов может быть обеспечение условий для взаимодействия между различными кластерами глобального ПД-Т. При создании шлюзов можно рассмотреть все необходимые аспекты: правовые, организационные и технологические.

Подходы к созданию типичных шлюзов информационной безопасности могут учитывать наличие различных возможных уровней взаимодействия между различными кластерами ПД-Т. В частности, создание шлюзов может осуществляться только на правовом и организационном уровнях и на комплексном уровне: правовом, организационном и технологическом.

Подходы к созданию типичных шлюзов информационной безопасности могут учитывать использование профилей перехода, описывающих и определяющих переход из одного кластера в другой. В этих профилях перехода

можно учитывать уровни доверия в системах идентификации, используемых внутри взаимодействующих кластеров, см. пункт 5.

Описание нескольких типов шлюзов информационной безопасности (ШИБ) может быть предметом технических стандартов и рекомендаций МСЭ и ОТК 1.

Резюме

Проблема трансграничного обмена электронными документами является весьма актуальной и отмечается в глобальных и региональных заявлениях, например:

- содействие исследованиям и сотрудничеству, делающим возможным эффективное использование данных и программного обеспечения, в частности электронных документов и операций, включая электронные средства удостоверения подлинности и совершенствование методов обеспечения безопасности (разработанная ВВУИО+10 концепция ВВУИО на период после 2015 года, C5. Укрепление доверия и безопасности при использовании ИКТ, пункт f);
- содействие укреплению уверенности и доверия в электронной среде в глобальном масштабе путем поощрения защищенных трансграничных потоков информации, включая электронные документы, и усилиям по расширению и укреплению Азиатско-Тихоокеанской информационной инфраструктуры и укреплению доверия и безопасности при использовании ИКТ (Декларация лидеров участниц АТЭС 2012 года, Владивостокская декларация: Интеграция – чтобы расти, инновации – чтобы процветать).

В настоящее время в мире существует несколько успешных методов решения такой задачи:

- в Европейской комиссии – на основании Постановления Европейского парламента и Совета ЕС об оказании электронных услуг по идентификации и обеспечению надежности электронных операций на внутреннем рынке (проект - eIDAS¹);
- в Евразийском экономическом союзе – на основании Договора о Евразийском экономическом союзе и Концепции использования услуг и юридически значимых электронных документов при межгосударственном информационном взаимодействии²;
- в Азиатско-Тихоокеанском регионе – на основе Паназиатского альянса за развитие электронной торговли (ПАА)³.

Потребности, связанные с развитием глобальной экономики, особенно в кризисные периоды, требуют активизации интеграционных процессов в различных экономических и социальных областях, в том числе путем

¹ <http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond>.

² www.eurasiancommission.org/docs/Download.aspx?IsDlg=0&print=1&ID=5713.

³ www.paa.net/.

использования современных ИКТ-технологий, основанных на инновациях. Именно эти задачи призван решить совокупный свод рекомендаций по ПД-Т, которые и предлагается разработать.

**Комментарий для сведения экспертов Рабочей группы III ЮНСИТРАЛ
"Урегулирование споров в режиме онлайн – УСО"**

Проблема идентификации заявителей требований и ответчиков в процессе УСО может быть решена в контексте предложенной выше модели (модель формирования и функционирования трансграничного пространства доверия в виде матрицы, построенной на основе региональных и глобальных кластеров, связанных между собой и включающих функциональные услуги, предоставляемые в рамках этого ПД-Т) следующим образом:

- создается функциональный кластер ПД-Т, специализирующийся на поддержке процедур УСО применительно к трансграничным электронным коммерческим сделкам;
- в географическом плане в этот кластер могут входить все государства – члены Организации Объединенных Наций;
- функционирование этого кластера обеспечивается с помощью коммерческой деятельности специализированного оператора или группы связанных между собой операторов;
- предметом коммерческой деятельности специализированных операторов может быть предоставление пакетов доверенных услуг по идентификации, основанных на наборе идентификационных схем, принятых в рамках платформ для электронной торговли;
- правовой режим коммерческой деятельности специализированных операторов устанавливается соглашениями с торговыми платформами.

На основании вышеизложенного предлагаются следующие поправки к проекту процессуальных правил для УСО:

пункт 4 (h) статьи 4А следует изменить следующим образом:

Подпись или другие средства идентификации и удостоверения подлинности личности заявителя требования и/или представителя заявителя требования, изложенные в разработанной СЕФАКТ/ООН "Рекомендации по обеспечению юридически значимого доверительного трансграничного электронного взаимодействия";

пункт 2 (g) статьи 4В следует изменить следующим образом:

Подпись или другие средства идентификации и удостоверения подлинности личности ответчика и/или представителя ответчика, изложенные в разработанной СЕФАКТ/ООН "Рекомендации по обеспечению юридически значимого доверительного трансграничного электронного взаимодействия".

Добавление
к видению и концептуальным подходам к разработке
в специализированных учреждениях Организации Объединенных Наций и
в соответствующих международных организациях совокупного свода
рекомендаций по формированию и функционированию трансграничного
пространства доверия

Общая инфраструктура доверия для юридически значимого трансграничного электронного взаимодействия

Белый документ

Цель разработки

Интернет стал привычным инструментом для получения электронных услуг физическими и юридическими лицами различных государств. Преимущества таких услуг очевидны, однако существует ряд организационных и правовых проблем, которые препятствуют их широкому использованию в тех областях деятельности, где пользователям нужен определенный уровень доверия к этим услугам. Одной из главных проблем является **обеспечение действительности электронных документов и юридической значимости электронного взаимодействия в целом**. Эта проблема актуальна как на национальном уровне – в рамках отдельных правовых систем, так и в трансграничном контексте – при взаимодействии участников, подпадающих под юрисдикцию различных государств. Эти вопросы неоднократно рассматривались на различных международных форумах, включая Организацию Объединенных Наций (СЕФАКТ/ООН, ЮНСИТРАЛ), а также на региональном уровне – в странах СНГ, ЕС и АТЭС. Тем не менее удовлетворительное решение пока не найдено.

Для того чтобы создать условия для доверительного трансграничного электронного взаимодействия, эксперты РСС⁴ выступили с инициативой создания трансграничного пространства доверия (далее в тексте – ПД-Т) на основе общей инфраструктуры доверия (далее – ОИД). Его **основная цель заключается в предоставлении доверенных услуг различного уровня (базового, среднего, высокого) пользователям ОИД в процессе их электронного взаимодействия**. Это позволит придавать юридическую значимость электронному взаимодействию по усмотрению пользователей независимо от их местоположения и юрисдикции.

Система ПД-Т представляет собой фундаментальную, легко масштабируемую платформу, обеспечивающую унифицированный доступ к доверенным электронным услугам. При этом учитываются существующие электронные системы, так что требования к их обновлению для включения в ПД-Т, как ожидается, будут минимальными.

В процессе работы над системой ПД-Т была предложена архитектура ОИД, описаны взаимосвязи между ее различными компонентами и их

⁴ Региональное содружество в области связи. www.rcc.org.ru.

взаимодействие с пользователями, причем работа одновременно велась по трем направлениям: правовому, организационному и технологическому. Анализ вариантов практической реализации и сценарии использования ОИД позволили подготовить перечень документов, необходимых для полного технического описания системы.

Следующим шагом по продвижению нового продукта видится обсуждение накопленного опыта и знаний с различными партнерами (экспертами и организациями), заинтересованными в облегчении, упрощении и одновременно придании юридической силы трансграничным электронным услугам.

Следует также разработать комплекты нормативных, организационных и технологических документов, обеспечивающих операционную совместимость в рамках соответствующего "домена доверия"⁵ (см. главу 4 § 3).

Далее планируется приступить к конкретным работам по формированию трансграничного пространства доверия, начиная с создания международных координационных структур и архитектуры ОИД в рамках соответствующего "домена доверия", после чего начнется практическая реализация систем трансграничного юридически значимого электронного взаимодействия.

Обеспечение международного доверия: архитектура ОИД

Разработка ПД-Т осуществляется на трех уровнях: правовом, организационном и технологическом. Комплексное описание позволяет обеспечить корректное функционирование как системы в целом, так и отдельных ее элементов.

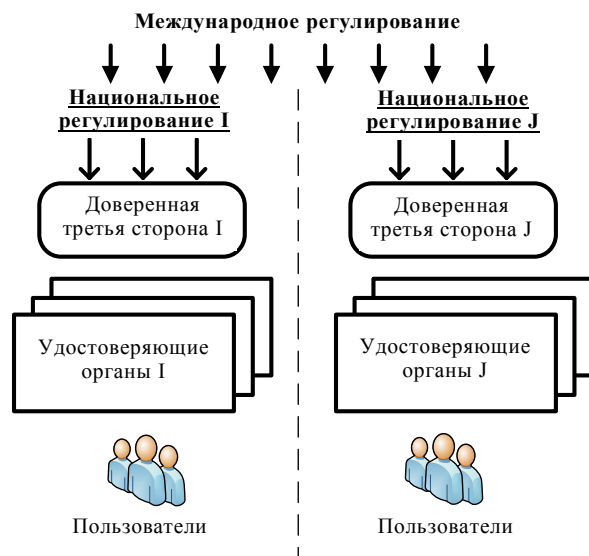
Архитектура ОИД выбрана так, что ее можно легко масштабировать. Она легко расширяется на любом уровне рассмотрения за счет входа в нее новых участников, таких как новых правовых систем, новых наднациональных участников, новых операторов услуг доверия и учетных систем.

Правовой уровень

ПД-Т может строиться на одно- или многодоменной основе. С точки зрения правового и организационного регулирования многодоменная основа является более сложным вариантом. Многодоменность предполагает применение средств доверенной третьей стороны (далее в тексте – ДТС). На рис. 1 представлена общая схема правового регулирования.

⁵ Информационно-правовое пространство, в котором используется одна и та же ОИД.

Рис. 1

Схема правового регулирования трансграничного пространства доверия

Правовое регулирование юридически значимого трансграничного информационного взаимодействия можно разделить на две части: международную и национальную. Международное правовое регулирование осуществляется на основе следующих видов документов:

- международные договоры/соглашения;
- акты различных международных организаций;
- международные стандарты и регламенты;
- соглашения между участниками трансграничного информационного взаимодействия по конкретным вопросам;
- типовые правовые акты.

В свою очередь национальное правовое регулирование также строится на комплексе нормативных документов, характерных для каждой отдельной правовой системы.

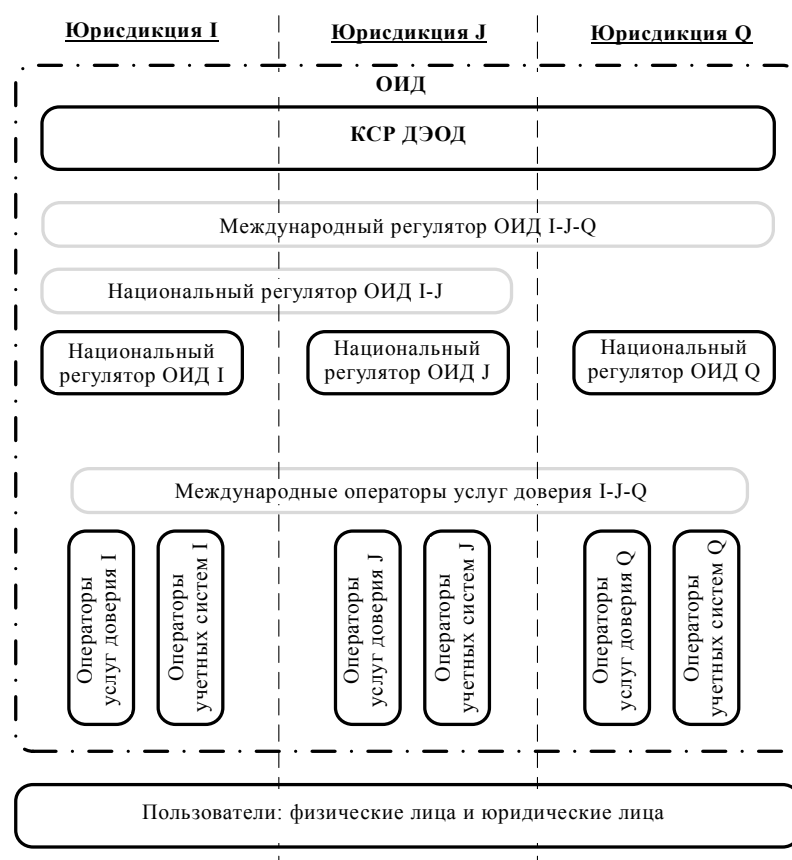
Организационный уровень

Взаимное юридически значимое признание услуг доверия, предоставляемых под юрисдикцией разных государств, достигается путем создания и функционирования Координационного совета регуляторов доверенного электронного обмена данными (далее – КСР ДЭОД). Деятельность данной организации регламентируется уставом КСР ДЭОД, который должны признать и подписать все его уполномоченные члены – т.е. регулирующие органы электронного обмена данными, представленные в первую очередь национальными регуляторами ОИД.

Организационное регулирование можно представить в виде следующей схемы (см. рис. 2):

Рис. 2

Схема организационного регулирования трансграничного пространства доверия (опциональные элементы обозначены серой рамкой)



КСР ДЭОД издает ряд документов, взаимосвязанных с его уставом:

- требования к членам КСР ДЭОД, соответствие которым является необходимым условием полноправного членства в КСР ДЭОД;
- руководящие принципы по проведению сопровождения "теневое" надзора для приема в КСР ДЭОД и взаимного периодического аудита для сохранения добровольного членства в КСР ДЭОД;
- критерии соответствия, которым должны удовлетворять операторы услуг ОИД и операторы учетных систем, и методология применения этих критериев;
- схема оценки/проверки операторов услуг ОИД и операторов учетных систем на соответствие этим критериям.

В ПД-Т каждая правовая система представлена национальным регулятором ОИД (см. рис. 2, национальные регуляторы ОИД I, J, Q), который регламентирует работу операторов услуг доверия и операторов учетных систем в рамках своей юрисдикции.

Для групп государств с большой степенью интеграции (например, ЕврАзЭС или ЕС) существует вероятность образования наднационального регулятора ОИД (см. рис. 2, наднациональный регулятор ОИД I-J). Таким образом, один наднациональный регулятор ОИД I-J заменяет группу национальных регуляторов ОИД I и J.

Естественная масштабируемость ОИД обеспечивается процедурой приема новых членов в КСР ДЭОД (новые правовые системы и наднациональные участники) и схемой проверки операторов услуг ОИД и операторов учетных систем на соответствие критериям, опубликованным КСР ДЭОД (новые операторы услуг доверия и учетных систем).

Если члены КСР ДЭОД (см. ниже) достигли условно "среднего" уровня доверия, они могут инициировать создание международного регулятора ОИД и международных операторов услуг доверия (см. рис. 2, международный регулятор ОИД I J Q и международные операторы услуг доверия I J Q). Международный регулятор ОИД будет осуществлять координацию взаимодействия международных операторов услуг доверия, а также национальных регуляторов ОИД (согласно уставу КСР ДЭОД) и/или наднациональных регуляторов ОИД.

Чтобы стать национальным оператором услуг доверия или оператором учетной системы, поставщику соответствующих услуг необходимо пройти аккредитацию у национального регулятора ОИД в том же государстве. Международные операторы услуг доверия обязаны проходить аккредитацию у международного регулятора ОИД. Требования к аккредитации операторов услуг доверия и операторов учетных систем, а также требования к их деятельности регулируются критериями соответствия, опубликованными КСР ДЭОД, и возможными национальными дополнениями, изданными соответствующим регулятором.

Пользователями электронных услуг в рамках ПД-Т могут выступать как физические, так и юридические лица. Пользователи выбирают по их усмотрению или по договоренности необходимый им уровень квалификации услуг доверия.

Услуги предоставляются соответствующими поставщиками – операторами услуг доверия. В ряде случаев услуги могут предоставлять и операторы учетных систем. Операторы услуг доверия и операторы учетных систем объединены общей инфраструктурой доверия.

Услуги доверия, являющиеся элементами ПД-Т, могут иметь различные варианты реализации в зависимости от уровня доверия между участниками информационного взаимодействия. Например, при условно "высоком" и "среднем" уровне взаимного доверия между членами КСР ДЭОД можно эффективно использовать централизованные международные услуги, предоставляемые в соответствии с согласованными стандартами. В случае условно "низкого" уровня доверия предоставление услуг доверия будет организовано по децентрализованному принципу – на основе национальных услуг в каждом государстве.

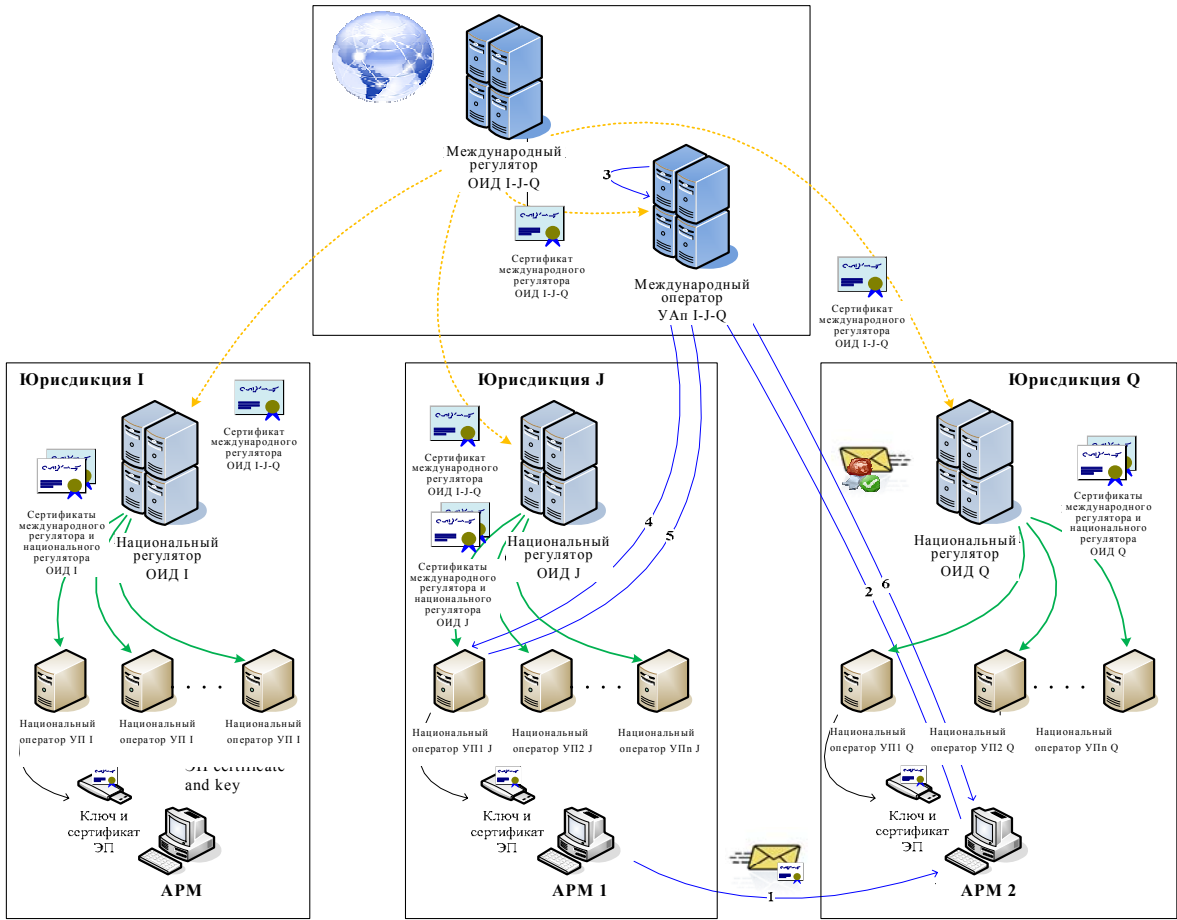
Технико-технологический уровень

Технологических вариантов оказания услуг доверия может быть великое множество. Главным требованием, предъявляемым к элементам ОИД, является

Технологическое функционирование служб по предоставлению услуг доверия можно показать на примере проверки электронной подписи (далее в тексте – ЭП) при трансграничном электронном взаимодействии. Для сравнения представлены два варианта реализации ОИД: децентрализованная схема при условно "низком" уровне доверия между участниками информационного взаимодействия (см. рис. 3) и централизованная схема при "среднем" уровне доверия между ними (см. рис. 4).

[illegible]

Рис. 4
Схема проверки ЭП в рамках ПД-Т со "средним" уровнем доверия
(децентрализованная схема)



В таблице 1 отражены особенности построения децентрализованной и централизованной схем ОИД. Процедура проверки ЭП для двух вариантов реализации ОИД описана в таблице 2.

Таблица 1
Особенности ОИД для информационного взаимодействия с "низким" и "средним" уровнем доверия

Низкий уровень доверия (рис. 3)	Средний уровень доверия (рис. 4)
1. Услуги апостилирования предоставляют национальные операторы услуг апостилирования (УАп).	1. Услуги апостилирования предоставляются международным оператором УАп.
2. Международные организации (операторы и регуляторы) отсутствуют.	2. Присутствуют международные организации: международный регулятор ОИД и международные операторы услуг доверия.

Низкий уровень доверия (рис. 3)	Средний уровень доверия (рис. 4)
3. Национальные регуляторы взаимодействуют напрямую, обмениваясь между собой сертификатами (----->). 4. Национальные регуляторы обеспечивают национальных операторов услуг доверия, на которых распространяется юрисдикция в отношении их сертификатов и сертификатов национальных регуляторов, на которых распространяется другая юрисдикция (----->).	3. Национальные регуляторы ОИД взаимодействуют только через международного регулятора ОИД. Также и национальные операторы услуг доверия взаимодействуют через соответствующего международного оператора. 4. Международный регулятор ОИД централизованно обеспечивает сертификатами национальных операторов услуг доверия и национальных регуляторов ОИД (----->). 5. Национальные регуляторы обеспечивают национальных операторов услуг доверия, на которых распространяется их юрисдикция в отношении их сертификатов и сертификатов международного регулятора (----->).

Таблица 2

Процедура проверки ЭП в схемах с "низким" и "средним" уровнем доверия

Низкий уровень доверия (рис. 3)	Средний уровень доверия (рис. 4)
1. Физическое/юридическое лицо 1 отправляет документы, подписанные ЭП в рамках юрисдикции J, выбирая при этом необходимый уровень квалификации используемых услуг доверия, предоставляемых ОИД (базовый, средний или высокий). 2. Запрос на проверку документов с ЭП в рамках юрисдикции J направляется национальному оператору услуг апостилирования (УАп), на который распространяется юрисдикция Q. 3. Запрос на проверку документов перенаправляется национальному оператору УАп, на которого распространяется юрисдикция J. 4. Осуществляется математическая проверка ЭП в рамках юрисдикции J. 5/6. Отправляется запрос/ответ о статусе сертификата национальному оператору услуг подписи (УП), на которого распространяется юрисдикция J. 7. Национальный оператор УАп, на которого распространяется юрисдикция Q, получает подтверждение корректности ЭП в рамках юрисдикции J. 8. Национальный оператор УАп, на которого распространяется юрисдикция Q, удостоверяет полученный запрос и направляет его физическому/юридическому лицу 2.	1. Физическое/юридическое лицо 1 отправляет документы, подписанные ЭП в рамках юрисдикции J, выбирая при этом необходимый уровень квалификации используемых услуг доверия, предоставляемых ОИД (базовый, средний или высокий). 2. Запрос на проверку документов с ЭП в рамках юрисдикции J направляется международному оператору УАп I-J-Q. 3. Осуществляется математическая проверка ЭП в рамках юрисдикции J. 4/5. Отправляется запрос/ответ о статусе сертификата национальному оператору услуг подписи (УП), на которого распространяется юрисдикция J. 6. Международный оператор УАп I-J-Q удостоверяет полученный запрос и направляет его физическому/юридическому лицу 2.

Идентификация заявителей требований и ответчиков при урегулировании споров в режиме онлайн

В контексте упомянутой выше модели формирования и функционирования трансграничного пространства доверия в виде матрицы, построенной на основе региональных и глобальных кластеров, связанных между собой и включающих функциональные услуги, предоставляемые в рамках этого ПД-Т, проблема идентификации заявителей требований и ответчиков при урегулировании споров в режиме онлайн (далее УСО) может решаться следующим образом:

- создается функциональный кластер ПД-Т, специализирующийся на поддержке процедур УСО применительно к трансграничным электронным коммерческим сделкам;
- в географическом плане в этот кластер могут входить все государства – члены Организации Объединенных Наций;
- функционирование этого кластера обеспечивается с помощью коммерческой деятельности специализированного оператора или группы связанных между собой операторов;
- предметом коммерческой деятельности специализированных операторов может быть предоставление пакетов доверенных услуг по идентификации, основанных на наборе идентификационных схем, принятых в рамках платформ для электронной торговли;
- правовой режим коммерческой деятельности специализированных операторов устанавливается соглашениями с торговыми платформами.

Дальнейшие шаги

1. Следующим шагом по продвижению разработки видится обсуждение накопленного опыта и знаний с различными партнерами (экспертами и организациями), заинтересованными в облегчении, упрощении и одновременно придании юридической силы трансграничным электронным услугам.

Таковыми заинтересованными партнерами могут быть в первую очередь как политические, так и экономические структуры⁶. К политическим структурам, уже частично вовлеченным в работу по этому направлению, можно отнести как наднациональные организации (например, СНГ, АТЭС, ЕС, ШОС), так и структуры, созданные в рамках двусторонних отношений между некоторыми государствами. К экономическим структурам, заинтересованным в достижении этой цели, относятся, например, соответствующие подразделения Организации Объединенных Наций, такие как СЕФАКТ/ООН/ЕЭК, ЮНСИТРАЛ (рабочие группы III и IV), а также ЕЭК ООН, ЕЭП, ЕврАзЭС и другие.

⁶ В этом продукте могут быть заинтересованы также и другие гуманитарные структуры, например в области права, Гагская конференция по международному частному праву, а также структуры в области медицины и образования; однако, на наш взгляд, такие организации будут скорее пользоваться уже созданным ПД-Т, чем поддерживать его разработку нового продукта.

2. Далее планируется приступить к конкретным работам по формированию трансграничного пространства доверия, начиная с создания международной координационной структуры (Координационный совет регуляторов доверенного электронного обмена данными) (см. рис. 2). Этот Совет должен будет принять свой устав и другие основополагающие документы, регламентирующие его деятельность (см. главу 3.2), а затем определиться с конкретной архитектурой общей инфраструктуры доверия (ОИД), с набором предоставляемых ОИД услуг доверия и возможными уровнями их квалификации (возможно, в зависимости от юрисдикции, которая распространяется на операторов, предоставляющих эти услуги).

Можно предположить, что существующие естественные особенности (исторические, культурные, политические, экономические, технические и т.д.) различных регионов мира приведут к тому, что различные форматы создадут "свои собственные" координационные структуры (КСР ДЭОД) и архитектуры ОИД в зависимости от степени доверия внутри каждого формата и упомянутых естественных особенностей.

Поэтому мы исходим из того, что на первых этапах реализации этого проекта будет существовать не единый "домен доверия" для всей планеты (например, на уровне какой-либо из структур Организации Объединенных Наций), а несколько "доменов доверия"⁷.

3. После того, как будет определена архитектура ОИД (в соответствующем "домене доверия"), можно будет приступить к написанию дальнейшего пакета документов организационного, нормативного и технологического характера, согласованного в рамках КСР ДЭОД. Системность этого документа может определяться результатами этапа 2. Таким образом, будет обеспечена операционная совместимость в рамках соответствующего "домена доверия".

Международные организации, занимающиеся выработкой и согласованием стандартов, могут внести существенный вклад в поддержку этих проектов.

4. Принятие этого пакета документов членами КСР ДЭОД (в соответствующем "домене доверия") позволит перейти к заключительному этапу практического внедрения систем трансграничного юридически значимого электронного взаимодействия.

⁷ Информационно-правовое пространство, в котором используется одна и та же ОИД.