



Генеральная Ассамблея

Distr.: Limited
13 September 2018
Russian
Original: English

**Комиссия Организации Объединенных Наций
по праву международной торговли
Рабочая группа IV (Электронная торговля)
Пятьдесят седьмая сессия
Вена, 19–23 ноября 2018 года**

Проект документа о трансграничном юридическом признании управления идентификационными данными и удостоверительных услуг — предложение Германии

Записка Секретариата

Германия представила в Секретариат документ для рассмотрения на пятьдесят седьмой сессии Рабочей группы. Этот документ воспроизводится в качестве приложения к настоящей записке в том виде, в котором он был получен Секретариатом.



Приложение

ПРОЕКТ ДОКУМЕНТА О ТРАНСГРАНИЧНОМ ЮРИДИЧЕСКОМ ПРИЗНАНИИ УПРАВЛЕНИЯ ИДЕНТИФИКАЦИОННЫМИ ДАННЫМИ И УДОСТОВЕРИТЕЛЬНЫХ УСЛУГ

подтверждая свою убежденность в том, что развитие информационно-коммуникационных технологий является условием устойчивого экономического роста и повышения качества жизни в целом;

отмечая, что электронная связь повышает эффективность государственного управления и коммерческой деятельности, укрепляет внешнеэкономические связи, открывает доступ к новым возможностям для ранее удаленных сторон и рынков и играет тем самым основополагающую роль в содействии экономическому развитию как на национальном, так и на международном уровнях;

учитывая, что неопределенность в отношении технологического и правового регулирования использования электронных документов при взаимодействии между государственными и муниципальными органами, физическими лицами и организациями государств-участников [проекта документа]¹ представляет собой препятствие для развития электронного взаимодействия;

будучи убеждены в том, что создание доверия между всеми участниками электронного взаимодействия является необходимым условием его развития;

полагая, что единообразные правила должны основываться на уважении свободы выбора сторонами соответствующих информационных носителей, технологий, идентификационных и удостоверительных услуг с учетом принципов технологической нейтральности и функциональной эквивалентности в той мере, в какой выбранные сторонами средства отвечают цели действующих норм права;

признавая возможность и целесообразность построения как централизованной, так и децентрализованной систем доверия и их использования для ускорения прогресса и развития цифровой экономики, в том числе в целях обеспечения основанных на доверии электронной торговли и транспорта, электронного урегулирования споров, создания электронного правительства и электронных государственных услуг, организации дистанционного обучения, электронного здравоохранения, электронных реестров всевозможного назначения, электронных финансовых услуг;

согласились о нижеследующем:

Раздел I. Сфера применения

Статья 1. Сфера применения

1. Настоящий [проект документа] определяет основные характеристики трансграничного пространства доверия, представляющего собой совокупность нормативных и организационно-технических условий по установлению доверия при трансграничном информационном взаимодействии публичных органов власти, физических лиц и корпоративных органов в электронном виде.
2. При определении сферы применения настоящего [проекта документа] не принимаются во внимание ни государственная принадлежность участников трансграничного электронного взаимодействия, ни их гражданский и правовой

¹ Формулировка «[проект документа]» заменяет наименование фактического текста, форма которого будет определена ЮНСИТРАЛ.

статус, ни характер электронных документов и электронных сообщений, которыми они обмениваются.

3. Трансграничное пространство доверия охватывает следующие сегменты:

1) централизованный сегмент, охватывающий нормативные и организационно-технические условия по установлению доверия при обмене электронными документами, что предполагает установление обязательных для государств-участников требований к порядку деятельности операторов удостоверяющих услуг, к программно-аппаратным средствам, используемым такими операторами в целях трансграничного электронного взаимодействия, удостоверяющим услугам, процедурам подтверждения соответствия операторов удостоверяющих услуг и программно-аппаратных средств;

2) саморегулируемый сегмент, охватывающий нормативные и организационно-технические условия по установлению доверия при обмене электронными сообщениями с использованием распределенных баз данных и формированием блоков данных, что предполагает организацию трансграничного электронного взаимодействия на принципах саморегулирования.

4. Трансграничное пространство доверия используется его участниками в целях обеспечения необходимого уровня доверия между сторонами электронного взаимодействия. Выбор конкретного сегмента трансграничного пространства доверия или их комбинации в соответствии с пунктом 3 статьи 1 настоящего [проекта документа] зависит от характера конкретных цифровых услуг, требующих доверия, которое призвано обеспечить трансграничное пространство доверия.

Раздел II. Общие положения

Статья 2. Определения

1. Для целей настоящего [проекта документа]:

1) «участники трансграничного пространства доверия» означают публичные органы власти, Координационный совет, операторов удостоверяющих услуг, операторов распределенных баз данных и физических лиц и организации;

2) «электронное сообщение» означает любую информацию, подготовленную, отправленную, полученную или хранимую с использованием информационных и телекоммуникационных сетей;

3) «электронный документ» означает электронное сообщение, обладающее необходимыми и достаточными реквизитами для признания его юридически значимым, достоверность и подлинность которого удостоверена оператором удостоверяющих услуг в соответствии с настоящим [проектом документа];

4) «записи операций» означают электронные сообщения, прошедшие проверку подлинности у операторов распределенных баз данных и включенные этими операторами в значимый (действительный) блок данных;

5) «значимый (действительный) блок данных» означает совокупность записей операций, подготовленных в соответствии с правилами, установленными оператором распределенной базы данных, не подлежащих изменению и дополнению;

6) «удостоверяющие услуги» означают услуги, подтверждающие достоверность и подлинность электронных документов и/или их отдельных реквизитов, включая, но не ограничиваясь ими, услуги, связанные с созданием и использованием электронных подписей, электронных печатей, электронных отметок времени, электронной доставки и аутентификации веб-сайтов;

7) «трансграничное электронное взаимодействие» означает осуществляемый с помощью информационных систем обмен электронными сообщениями и/или электронными документами между участниками трансграничного пространства доверия;

8) «Координационный совет» означает создаваемый в соответствии с настоящим [проектом документа] орган, который устанавливает обязательные для членов общие требования к порядку деятельности операторов удостоверяющих услуг, к программно-аппаратным средствам, используемым в целях осуществления трансграничного электронного взаимодействия операторами удостоверяющих услуг, и процедуры подтверждения соответствия операторов удостоверяющих услуг и программно-аппаратных средств установленным требованиям, а также выполняет иные функции, установленные настоящим [проектом документа];

9) «место нахождения» означает место, указанное участником трансграничного пространства доверия как место жительства, а при отсутствии такового — место жительства физического лица или место регистрации юридического лица;

10) «оператор удостоверяющих услуг» означает физическое или юридическое лицо, которое соответствует требованиям, установленным Координационным советом, получило подтверждение о соответствии таким требованиям в порядке, установленном Координационным советом, и предоставляет удостоверяющие услуги в рамках централизованного сегмента трансграничного пространства доверия;

11) «операторы распределенной базы данных (майнеры)» означают физических или юридических лиц (в том числе действующих анонимно), которые используют необходимые программно-аппаратные средства для участия в саморегулируемом сегменте трансграничного пространства доверия путем записи операций и проверки их подлинности, путем формирования блоков данных в распределенных базах данных и проверки их полноты;

12) «пользователь» означает публичный орган власти, физическое лицо или организацию, являющиеся отправителем или получателем электронных сообщений и/или электронных документов, в том числе с использованием услуг, предоставляемых в рамках саморегулируемого сегмента трансграничного пространства доверия;

13) «информационные системы» означают совокупность информационных технологий и оборудования, предназначенных и используемых для подготовки, отправления, получения, хранения или иной обработки электронных сообщений, включая электронные документы, в целях трансграничного электронного взаимодействия;

14) «электронная подпись/печать» означает данные в электронной форме, физически или логически ассоциированные с другими электронными данными, которые используются подписавшей стороной для подписания и которые документируют определенное отношение между подписавшей стороной и этими электронными данными таким образом, что третье лицо может впоследствии установить наличие этого отношения;

15) «подписавшая сторона» означает физическое (для электронной подписи) или юридическое (для электронной печати) лицо, которое подписывает электронный документ с помощью своей электронной подписи/печати;

16) «квалифицированный сертификат электронной подписи/печати» означает подтверждение в электронной форме, связывающее данные для проверки электронной подписи/печати с физическим (подпись) или юридическим (печать) лицом и подтверждающее по меньшей мере его личность, выданное оператором удостоверяющих услуг, прошедшим процедуру подтверждения

соответствия согласно пункту 6 статьи 8 настоящего [проекта документа] и удовлетворяющим требованиям, установленным Координационным советом;

17) «электронная отметка времени» означает данные в электронной форме, связывающие другие электронные данные с определенным моментом времени и документирующие, что эти электронные данные в этот момент времени существовали, что позволяет участникам электронного взаимодействия или третьей стороне впоследствии установить этот факт;

18) «электронный сервис доставки с подтверждением получения» означает сервис, который позволяет передавать данные между третьими сторонами электронными средствами и предоставлять доказательство относительно обработки передаваемых данных, включая подтверждение отправления и получения данных, и который защищает переданные данные от рисков утраты, кражи, повреждения или несанкционированных изменений;

19) «квалифицированный сертификат аутентификации веб-сайтов» означает подтверждение в электронной форме, позволяющее аутентифицировать веб-сайты, связывая веб-сайт с физическим или юридическим лицом, которому это подтверждение было выдано оператором удостоверяющих услуг, прошедшим процедуру подтверждения соответствия согласно пункту 6 статьи 8 настоящего [проекта документа] и удовлетворяющим требованиям, установленным Координационным советом;

20) «идентификационные данные» означают информацию о конкретном субъекте (в данном случае: пользователе) в виде одного или нескольких атрибутов, позволяющих субъекту быть в достаточной степени отличимым в определенном контексте;

21) «средства идентификации» означают материальную и/или нематериальную единицу, содержащую идентификационные данные конкретного субъекта (в данном случае: пользователя);

22) «управление идентификационными данными» означает набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и увязка, обеспечение реализации, аутентификация и подтверждения), используемых для: i) гарантирования идентификационной информации (например, идентификаторов, регистрационных данных, атрибутов); ii) подтверждения идентификационных данных субъекта; и iii) активации коммерческих приложений и приложений безопасности;

23) «первичная (фундаментальная) идентификация» означает процесс сбора, проверки и подтверждения действительности атрибутов идентификационных данных по конкретному субъекту (в данном случае: пользователю) для определения и подтверждения его идентификационных данных вне какого-либо конкретного контекста.

Первичная идентификация обычно выполняется органом, выдающим затем соответствующий первичный сертификат удостоверения личности (например, свидетельство о рождении, национальная идентификационная карта, паспорт и т.д.);

24) «вторичная (операционная) идентификация» означает процесс сбора, проверки и подтверждения действительности атрибутов идентификационных данных по конкретному субъекту (в данном случае: пользователю) для определения и подтверждения его идентификационных данных в конкретном контексте.

Вторичная идентификация выполняется оператором удостоверяющих услуг и может быть либо а) идентификацией заявителя при регистрации, чтобы стать пользователем удостоверяющей услуги (услуг), предоставляемых оператором удостоверяющих услуг, или б) идентификацией пользователя для использования конкретной удостоверяющей услуги.

а) для целей идентификации заявителя при регистрации оператор удостоверяетелных услуг обычно использует либо первичный сертификат удостоверения личности, либо уже существующий результат другой предыдущей идентификации заявителя. После успешной идентификации заявителя оператор удостоверяетелных услуг создает/выдает собственную учетную запись вторичной идентификации пользователя (вторичный сертификат удостоверения личности);

б) для целей идентификации пользователя для использования конкретной удостоверяетелной услуги оператору удостоверяетелных услуг требуется, чтобы пользователь, уже имеющий свою запись идентификации пользователя в соответствии с подпунктом (а) настоящего определения, идентифицировал себя с использованием своего вторичного сертификата удостоверения личности (на основе знания, владения (в том числе по биометрическим данным));

25) «система идентификации» означает (онлайновое) пространство для операций по идентификации, регулируемых набором системных правил, в котором физические или юридические лица могут доверять друг другу, поскольку их идентификацию и удостоверение подлинности идентификационных данных обеспечивают авторитетные источники. Система идентификации включает а) набор правил, методов, процедур и подпрограмм, технологий, стандартов, принципов и процессов, б) применимых к группе участвующих субъектов, с) регулирующих сбор, проверку, хранение, обмен, аутентификацию и использование идентификационной атрибутивной информации о физическом или юридическом лице, д) с целью облегчения операций по идентификации;

26) «операция по идентификации» означает любую операцию с участием двух или более участников, которая предполагает создание, проверку, выдачу, подтверждение, отзыв, передачу или использование идентификационной информации;

27) «поставщик идентификационных услуг» означает субъекта, ответственного за идентификацию физических или юридических лиц, выдачу соответствующих средств идентификации, а также поддержание такой идентификационной информацией и управление ею;

28) «нотифицированная система идентификации» означает систему идентификации, которая а) соответствует требованиям Координационного совета, и б) была доведена поставщиком идентификационных услуг, эксплуатирующим эту систему идентификации, до сведения Координационного совета, как это предусмотрено в пункте 2 статьи 5 настоящего [проекта документа];

29) «уровень обеспечения доверия нотифицированной системы идентификации» означает атрибут (характеристику) нотифицированной системы идентификации, определяемый поставщиком идентификационных услуг, эксплуатирующим эту систему идентификации, в соответствии с требованиями Координационного совета, как это предусмотрено в пункте 2 статьи 5 настоящего [проекта документа];

30) «член» (Координационного совета) означает юридическое лицо, которое i) обладает юридическими полномочиями в рамках соответствующего национального законодательства для осуществления юридического признания услуг по управлению идентификационными данными и удостоверяетелных услуг, и ii) официально признало все положения настоящего [проекта документа].

Статья 3. Толкование

1. При толковании настоящего [проекта документа] надлежит учитывать его международный характер и необходимость содействовать достижению единообразия в его применении, а также соблюдению добросовестности при трансграничном электронном взаимодействии и иных принципов, установленных статьей 5 настоящего [проекта документа].

2. Вопросы, относящиеся к предмету регулирования настоящего [проекта документа], которые прямо в нем не разрешены, подлежат разрешению в соответствии с общими принципами, на которых он основан, а при отсутствии таких принципов — в соответствии с правом, применимым в силу норм международного частного права.

Статья 4. Принципы

Трансграничное электронное взаимодействие в рамках трансграничного пространства доверия осуществляется на основе следующих принципов, которые применяются к обоим сегментам трансграничного пространства доверия:

- 1) технологическая нейтральность;
- 2) функциональная эквивалентность в отношении обеспечения управления идентификационными данными и удостоверительных услуг;
- 3) защита информации ограниченного доступа, т.е. информации, охраняемой на основании норм международного права и национального законодательства государств-участников, включая коммерческую тайну и персональные данные, при осуществлении трансграничного электронного взаимодействия;
- 4) использование любой информации, документов и сообщений, в том числе блоков данных в распределенных базах данных, исключительно в целях, не противоречащих нормам международного права и нормам национального законодательства государств-участников;
- 5) экономическая нейтральность, способствующая экономической эффективности и сбалансированности в отношении обеспечения управления идентификационными данными и удостоверительных услуг;
- 6) пропорциональность, т.е. содержание и форма действий должны соответствовать преследуемой цели;
- 7) автономия сторон: свобода выбора участниками информационных носителей, технологии, идентификационных и удостоверительных услуг, соответствующих их конкретным коммерческим потребностям;
- 8) недопущение дискриминации.

Раздел III. Координационный совет

Статья 5. Функции Координационного совета

1. Координационный совет является органом, выполняющим функции руководящего органа в централизованном сегменте трансграничного пространства доверия и функции координатора в саморегулируемом сегменте трансграничного пространства доверия.

2. В рамках централизованного сегмента трансграничного пространства доверия Координационный совет утверждает по меньшей мере следующий набор требований, процедур, принципов и условий, явное выполнение которых участниками позволяет обеспечить взаимное признание результатов идентификации и средств идентификации, а также результатов использования удостоверительных услуг:

А. Управление идентификационными данными

- 1) требования к свойствам и характеристикам систем идентификации, используемых для выполнения первичной идентификации и приемлемых для нотификации.

Такие требования должны учитывать, что системы идентификации создаются и действуют в национальном контексте государств-участников, и должны учитывать соответствующее национальное законодательство, включая положения национального законодательства о сертификации систем идентификации.

Такие требования должны учитывать возможность определения различных уровней обеспечения доверия нотифицированной системы идентификации;

2) объем ответственности поставщиков идентификационных услуг уведомленных систем идентификации за любые потери;

3) процедуры взаимного признания полученных результатов идентификации и средств идентификации, выданных поставщиками идентификационных услуг нотифицированных систем идентификации;

4) определение юридических последствий — для целей настоящего [проекта документа], — возникающих в ходе использования нотифицированных систем идентификации, включая взаимное признание полученных результатов идентификации и выданных средств идентификации поставщиками идентификационных услуг нотифицированных систем идентификации; при этом следует учитывать различные уровни обеспечения доверия нотифицированной системы идентификации;

5) базовые условия использования нотифицированных систем идентификации;

6) требования к свойствам и характеристикам систем идентификации, используемых операторами удостоверительных услуг для выполнения вторичной идентификации пользователей;

7) правила урегулирования споров.

В. Удостоверительные услуги

1) требования к порядку деятельности операторов удостоверительных услуг, в том числе к страхованию гражданской ответственности и аудиту операторов удостоверительных услуг;

2) требования к программно-аппаратным средствам, используемым в рамках трансграничного электронного взаимодействия;

3) процедуры подтверждения соответствия операторов удостоверительных услуг, включая подтверждение соответствия систем идентификации, используемых для выполнения вторичной идентификации пользователей, и программно-аппаратных средств (аудит);

4) объем ответственности операторов удостоверительных услуг за любые потери;

5) правила урегулирования споров;

6) требования к органам и (или) физическим лицам, осуществляющим подтверждение соответствия операторов удостоверительных услуг, включая подтверждение соответствия систем идентификации, используемых для вторичной идентификации пользователей, и программно-аппаратных средств (аудит);

7) базовые условия использования удостоверительных услуг, определяемые в статьях 15, 16, 17, 18, 19 и 20 настоящего [проекта документа].

С. Другие документы, предусмотренные в настоящем [проекте документа]

3. Участники соглашаются в соответствии с настоящим [проектом документа] исполнять или обеспечивать исполнение актов Координационного совета, принятых в соответствии с пунктом 2 настоящей статьи, находящимися под их юрисдикцией публичными органами и органами местного самоуправления, пользователями и операторами удостоверительных услуг.

4. В саморегулируемом сегменте трансграничного пространства доверия Координационный совет:

1) утверждает рекомендуемый порядок подтверждения присоединения операторов распределенных баз данных к соответствующим базам данных;

2) утверждает порядок уведомления Координационного совета об инцидентах с информацией в распределенных базах данных, т.е. об использовании электронных сообщений, записей операций, блоков данных в распределенных базах данных в целях, противоречащих нормам международного права и нормам национального законодательства членом;

3) организует подачу операторами распределенных баз данных уведомлений в Координационный совет о добровольном принятии ими на себя обязательств по выполнению требований настоящего [проекта документа] в части обеспечения использования любой информации, документов и сообщений, включая блоки данных в распределенных базах данных, только в целях, не противоречащих нормам международного права и нормам национального законодательства членом, и в части информирования Координационного совета об инцидентах с информацией в распределенных базах данных.

5. Решения и документы, принимаемые Координационным советом в отношении саморегулируемого сегмента трансграничного пространства доверия, носят рекомендательный характер.

Статья 6. Создание и порядок работы Координационного совета

1. Координационный совет состоит из своих членом, избираемых на четырехлетний срок. Каждый член может назначить одного уполномоченного представителя.

2. Координационный совет может создавать вспомогательные органы, которые он сочтет необходимыми для выполнения своих функций.

3. Каждый член Координационного совета имеет один голос.

4. Решения Координационного совета по вопросам регламента его работы считаются принятыми, когда за них поданы голоса не менее двух третей его членом.

5. Решения Координационного совета об утверждении актов, упомянутых в пункте 2 статьи 5, принимаются единогласно.

6. Координационный совет устанавливает свои правила процедуры, включая порядок избрания своего председателя, процедуру поддержания взаимного доверия между ответственными представителями участников трансграничного пространства доверия и процедуру принятия решений в отношении утверждения документов, указанных в статье 5 настоящего [проекта документа].

Раздел IV. Участники трансграничного пространства доверия

Статья 7. Публичные органы и органы местного самоуправления государств-участников

1. Публичные органы участвуют в трансграничном электронном взаимодействии при выполнении публичных функций, возложенных на них национальным законодательством государств-участников, в соответствии с правилами, установленными настоящим [проектом документа] и принятыми в соответствии с ним актами Координационного совета.

2. Публичные органы вправе самостоятельно принимать решение о порядке участия в саморегулируемом сегменте трансграничного пространства доверия.

3. Публичные органы вправе устанавливать дополнительные требования по сравнению с требованиями, установленными настоящим [проектом документа] и принятыми в соответствии с ним актами Координационного совета, но не противоречащие им, в целях осуществления электронного взаимодействия в случаях, установленных Координационным советом.

Статья 8. Операторы достоверительных услуг

1. Операторы достоверительных услуг являются участниками централизованного сегмента трансграничного пространства доверия.
2. Операторы достоверительных услуг могут оказывать достоверительные услуги на территории отдельных членов и/или на территории всех государств-участников.
3. Операторы достоверительных услуг обязаны соответствовать требованиям, установленным Координационным советом, в зависимости от территории (всей территории государств-участников или ее части), на которой операторы достоверительных услуг оказывают услуги, и подтверждать соответствие установленным требованиям в порядке, установленном Координационным советом.
4. Операторы достоверительных услуг обязаны размещать в Интернете любую информацию о получении или изменении статуса оператора достоверительных услуг. Операторы достоверительных услуг обязаны уведомлять компетентные органы соответствующего участника о любых изменениях в оказании достоверительных услуг и о статусе оператора достоверительных услуг. Операторы достоверительных услуг обязаны предоставлять любую информацию, связанную с инцидентами при осуществлении трансграничного электронного взаимодействия, компетентным органам государств-участников и Координационному совету. Порядок и сроки предоставления информации, связанной с инцидентами при осуществлении трансграничного электронного взаимодействия, устанавливает Координационный совет.
5. Операторы достоверительных услуг обязаны страховать гражданскую ответственность или обеспечивать достаточное финансовое покрытие в соответствии с требованиями, установленными Координационным советом.
6. Операторы достоверительных услуг обязаны проходить процедуру подтверждения (независимый аудит) соответствия операторов достоверительных услуг, предоставляемых ими услуг, включая оценку систем идентификации, используемых для вторичной идентификации пользователей, и программно-аппаратных средств требованиям Координационного совета в установленном им порядке.

Статья 9. Независимый аудит соответствия. Страхование

1. Право оказывать достоверительные услуги имеют только операторы достоверительных услуг, прошедшие независимый аудит соответствия.
2. Аудит соответствия могут проводить органы или учреждения, уполномоченные в порядке, установленном Координационным советом.
3. Операторы достоверительных услуг осуществляют страхование гражданской ответственности в соответствии с требованиями, установленными Координационным советом.

Статья 10. Операторы распределенных баз данных

1. Операторы распределенных баз данных являются участниками саморегулируемого сегмента трансграничного пространства доверия.
2. Операторы распределенных баз данных организуют трансграничное электронное взаимодействие друг с другом и с пользователями на основе принципов саморегулирования и обеспечивают выполнение требований настоящего

[проекта документа] об использовании любой информации, документов и сообщений, в том числе блоков данных в распределенных базах данных, только в целях, не противоречащих нормам международного права и нормам национального законодательства государств-участников, и об информировании Координационного совета об инцидентах в распределенных базах данных.

3. Операторы распределенных баз данных признаются выполняющими требования настоящего [проекта документа] об использовании любой информации, документов и сообщений, в том числе блоков данных в распределенных базах данных, только в целях, не противоречащих нормам международного права и нормам национального законодательства членом, и об информировании Координационного совета об инцидентах в распределенных базах данных в случае добровольной подачи в Координационный совет уведомлений о добровольном соблюдении указанных требований. Порядок подачи соответствующих уведомлений и порядок ведения перечня операторов распределенных баз данных членом трансграничного пространства доверия устанавливаются Координационным советом.

Координационный совет вправе отказать во включении в перечень уведомления оператора распределенной базы данных, если он располагает информацией о нарушениях норм международного права и норм национального законодательства государств-участников, допущенных этим оператором.

4. Взаимодействие операторов распределенных баз данных и Координационного совета, а также операторов распределенных баз данных и пользователей может осуществляться без идентификации юридических и физических лиц, являющихся операторами распределенных баз данных и пользователями.

5. В случае получения Координационным советом информации о нарушении оператором распределенной базы данных требований настоящего [проекта документа], указанных в пункте 2 настоящей статьи, оператор распределенной базы данных может быть исключен из общедоступного перечня операторов распределенных баз данных, являющихся сторонами трансграничного пространства доверия.

Статья 11. Пользователи

1. Пользователи являются участниками обоих сегментов трансграничного пространства доверия.

2. В зависимости от сегмента трансграничного пространства доверия пользователи осуществляют обмен электронными сообщениями и электронными документами в соответствии с правилами, установленными Координационным советом и операторами удостоверяющих услуг, или в соответствии с правилами, установленными операторами распределенных баз данных, соответственно.

Раздел V. Инфраструктура трансграничного пространства доверия

Статья 12. Программно-аппаратные средства операторов удостоверяющих услуг

1. Операторы удостоверяющих услуг используют для оказания услуг только программно-аппаратные средства, успешно прошедшие процедуры оценки соответствия согласно пункту 6 статьи 8 и пункту 1 статьи 9.

2. Функциональные требования к программно-аппаратным средствам операторов удостоверяющих услуг и требования к процедуре подтверждения соответствия программно-аппаратных средств установленным функциональным требованиям в соответствии с принципом технологической нейтральности устанавливаются Координационным советом в соответствии с пунктом 6 статьи 8 и пунктами 1 и 2 статьи 9.

Статья 13. Программно-аппаратные средства операторов распределенных баз данных

Операторы распределенных баз данных самостоятельно определяют требования к программно-аппаратным средствам, необходимым для проверки подлинности и полноты записей операций, создания, хранения и проверки полноты блоков данных.

Статья 14. Программно-аппаратные средства пользователей

Пользователи обязаны самостоятельно обеспечивать соответствие программно-аппаратных средств, используемых при трансграничном электронном взаимодействии, требованиям операторов удостоверяющих услуг.

Раздел VI. Удостоверяющие услуги в рамках централизованного сегмента трансграничной среды доверия

Статья 15. Электронная подпись

1. Электронная подпись не может быть лишена юридической силы и приемлемости в качестве доказательства в судебном разбирательстве только на том основании, что она имеет электронную форму или не соответствует требованиям, предъявляемым к квалифицированной электронной подписи.

2. Усиленная электронная подпись должна отвечать следующим требованиям:

а) она должна быть уникальным образом связана с подписавшей стороной;

б) она должна давать возможность идентифицировать подписавшую сторону;

в) она должна быть создана с использованием данных создания электронной подписи, которые подписавшая сторона использует под единоличным контролем;

г) она должна быть связана с данными, в отношении которых она представляется, таким образом, чтобы любое последующее изменение таких данных можно было обнаружить.

3. Квалифицированная электронная подпись представляет собой усиленную электронную подпись, основанную на квалифицированном сертификате электронной подписи и созданную с помощью программно-аппаратных средств, сертифицированных в соответствии с пунктом 6 статьи 8. Квалифицированная электронная подпись имеет такую же юридическую силу, что и собственноручная подпись.

Усиленная электронная подпись, которая не является квалифицированной электронной подписью, имеет такую же юридическую силу, что и собственноручная подпись в случаях, определенных в соглашении сторон об использовании такой подписи или в нормативно-правовых актах государств-участников.

4. Квалифицированная электронная подпись, основанная на квалифицированном сертификате, выданном под юрисдикцией одного члена, признается квалифицированной электронной подписью всеми другими членами.

Статья 16. Электронная печать

1. Электронная печать не может быть лишена юридической силы и приемлемости в качестве доказательства в судебном разбирательстве только на том

основании, что она имеет электронную форму или не соответствует требованиям, предъявляемым к квалифицированной электронной печати.

2. Усиленная электронная печать должна отвечать следующим требованиям:
 - a) она должна быть уникальным образом связана с создателем печати;
 - b) она должна давать возможность идентифицировать создателя печати;
 - c) она должна быть создана с использованием данных создания электронной печати, которые создатель печати использует под единоличным контролем;
 - d) она должна быть связана с данными, к которым она относится, таким образом, чтобы любое последующее изменение таких данных можно было обнаружить.

3. Квалифицированная электронная печать представляет собой усиленную электронную печать, основанную на квалифицированном сертификате электронной печати и созданную с помощью программно-аппаратных средств, сертифицированных в соответствии с пунктом 6 статьи 8. Квалифицированная электронная печать создает презумпцию целостности данных и правильности происхождения этих данных, которые заверяет такая квалифицированная электронная печать.

Усиленная электронная печать, которая не является квалифицированной электронной печатью, создает презумпцию целостности данных и правильности происхождения этих данных, которые заверяет такая квалифицированная электронная печать, в случаях, определенных в соглашении сторон об использовании такой печати или в нормативно-правовых актах государств-участников.

4. Квалифицированная электронная печать, основанная на квалифицированном сертификате, выданном под юрисдикцией одного члена, признается квалифицированной электронной печатью всеми другими членами.

Статья 17. Электронная отметка времени

1. Электронная отметка не может быть лишена юридической силы и приемлемости в качестве доказательств в судебном разбирательстве только на том основании, что она имеет электронную форму или не соответствует требованиям, предъявляемым к квалифицированной электронной отметке времени.
2. Квалифицированная электронная отметка времени создает презумпцию точности указанных даты и времени и целостности данных, которые удостоверяются/заверяются такой квалифицированной электронной отметкой времени.
3. Квалифицированная электронная отметка времени должна отвечать следующим требованиям:
 - a) она должна привязывать дату и время к данным таким образом, чтобы разумно исключалась возможность незаметного изменения данных;
 - b) она должна быть основана на источнике, указывающем точное время и соотносимом с универсальным глобальным временем;
 - c) она должна быть заверена усиленной электронной подписью или усиленной электронной печатью оператора удостоверяющих услуг, прошедшего процедуру подтверждения соответствия согласно пункту 6 статьи 8.
4. Квалифицированная электронная временная отметка, выдаваемая под юрисдикцией одного члена, признается квалифицированной электронной отметкой времени всеми другими членами.

Статья 18. Электронный сервис доставки с подтверждением получения

1. Данные, отправленные и полученные с помощью электронного сервиса доставки с подтверждением получения, не могут быть лишены юридической силы

и приемлемости в качестве доказательства в судебном разбирательстве только на том основании, что они имеют электронную форму или не соответствует требованиям, предъявляемым к квалифицированным электронным сервисам доставки с подтверждением получения.

2. Данные, отправленные и полученные с помощью квалифицированного электронного сервиса доставки с подтверждением получения, создают презумпцию целостности данных, отправления таких данных идентифицированным отправителем, получения таких данных идентифицированным получателем, точности даты и времени отправления и получения, указанных квалифицированным электронным сервисом доставки с подтверждением получения.

3. Квалифицированные электронные сервисы доставки с подтверждением получения должны соответствовать следующим требованиям:

a) они предоставляются одним или несколькими операторами удостоверительных услуг, прошедшими процедуру подтверждения соответствия согласно пункту 6 статьи 8 настоящего [проекта документа];

b) они обеспечивают с высокой степенью надежности идентификацию отправителя;

c) они обеспечивают идентификацию получателя до предоставления данных;

d) отправление и получение данных заверяются усиленной электронной подписью или усиленной электронной печатью оператора удостоверительных услуг таким образом, чтобы исключить возможность незаметного внесения изменений в данные;

e) любые изменения данных, осуществляемые с целью отправления или получения данных, явным образом доводятся до сведения отправителя и получателя;

f) дата и время отправления, получения и любого изменения данных указаны с помощью квалифицированной электронной отметки времени.

4. Результаты использования квалифицированного электронного сервиса доставки с подтверждением получения, полученные под юрисдикцией одного члена, признаются в качестве результатов использования квалифицированного электронного сервиса доставки с подтверждением получения всеми другими членами.

Статья 19. Аутентификация веб-сайтов

1. Квалифицированный сертификат аутентификации веб-сайтов должен содержать:

a) указание — по крайней мере, в форме, пригодной для автоматической обработки, — на то, что сертификат был выдан в качестве квалифицированного сертификата аутентификации веб-сайтов;

b) набор данных, однозначно представляющих оператора удостоверительных услуг, который выдал квалифицированный сертификат;

c) для физических лиц — по меньшей мере имя или псевдоним лица, которому выдан сертификат; для юридических лиц — по меньшей мере наименование юридического лица, которому выдан сертификат, и, если применимо, регистрационный номер, указанный в официальном реестре;

d) частичные данные адреса, включая по меньшей мере город и государство физического или юридического лица, которому выдан сертификат, и, если это применимо, в соответствии с официальными документами;

e) доменное имя (имена), принадлежащее физическому или юридическому лицу, которому выдан сертификат;

- f) данные о начале и окончании срока действия сертификата;
 - g) идентификационный код сертификата, который должен быть уникальным для конкретного оператора удостоверяющих услуг;
 - h) усиленную электронную подпись или усиленную электронную печать выдающего сертификат оператора удостоверяющих услуг, прошедшего процедуру подтверждения соответствия согласно пункту 6 статьи 8 настоящего [проект документа];
 - i) место нахождения сервисов статуса действительности сертификата, которые могут использоваться для запроса статуса квалифицированного сертификата.
2. Результаты использования удостоверяющих услуг аутентификации веб-сайтов, основанного на квалифицированном сертификате аутентификации веб-сайтов, выданном под юрисдикцией одного члена, признаются в качестве результатов использования удостоверяющих услуг аутентификации веб-сайтов, основанного на квалифицированном сертификате аутентификации веб-сайтов, всеми другими членами.

Статья 20. Другие удостоверяющие услуги

1. Координационный совет может дополнительно включать в сферу своего регулирования другие удостоверяющие услуги, не указанные в статьях 15–19 [проекта документа].
2. Регулирование других удостоверяющих услуг должно осуществляться аналогично регулированию удостоверяющих услуг, упомянутых в статьях 15–19 [проекта документа].
3. В целях содействия общему использованию удостоверяющих услуг в трансграничных отношениях следует обеспечить возможность использования удостоверяющих услуг в качестве доказательств в рамках судебного разбирательства во всех государствах-участниках. Юридические последствия удостоверяющих услуг определяются национальным законодательством, за исключением случаев, когда в настоящем [проекте документа] предусмотрено иное.

Статья 21. Признание удостоверяющих услуг третьих стран и международных организаций

1. Удостоверяющие услуги, оказываемые операторами, уполномоченными в соответствии с законодательством третьих стран или международных организаций, могут признаваться юридически эквивалентными удостоверяющим услугам, оказываемым операторами, прошедшими процедуру подтверждения соответствия согласно пункту 6 статьи 8 настоящего [проект документа], если это согласовано между Координационным советом и уполномоченным органом третьей страны или международной организации в соответствии с пунктом 2 настоящей статьи.
2. Соглашения, упомянутые в пункте 1 настоящей статьи, предусматривают, в частности, что:
 - 1) требования, предъявляемые к операторам удостоверяющих услуг третьей страны или международной организации, не ниже требований, предъявляемых к операторам удостоверяющих услуг, оказывающих удостоверяющие услуги в соответствии с настоящим [проектом документа];
 - 2) третья страна или международная организация, являющаяся участником такого соглашения, признает на своей территории (под своей юрисдикцией) юридическую эквивалентность услуг, оказываемых операторами удостоверяющих услуг, прошедшими процедуру подтверждения соответствия согласно пункту 6 статьи 8 настоящего [проекта документа], и услуг, оказываемых операторами удостоверяющих услуг, уполномоченными в соответствии с

законодательством третьей страны или международной организации, подписавшей это соглашение.

Раздел VII. Защита прав и интересов участников трансграничного электронного взаимодействия

Статья 22. Судебная защита

1. Электронные документы и электронные сообщения, включая результаты использования удостоверительных услуг, описанных в статьях 15–20 [проекта документа], принимаются в качестве доказательств во всех судах и арбитражных судах членов.
2. Субъективное право, удостоверенное электронным документом, имеет такую же правовую силу, как и право, удостоверенное документом в бумажной форме.

Статья 23. Урегулирование споров

1. Координационный совет принимает правила административного урегулирования споров, возникающих в ходе трансграничного электронного взаимодействия в рамках централизованного сегмента трансграничной среды доверия.
 2. Участники трансграничного электронного взаимодействия имеют право заключать двусторонние и многосторонние соглашения о процедуре урегулирования споров, касающихся трансграничного электронного взаимодействия.
-