Организация Объединенных Наций A/CN.9/630/Add.3

Генеральная Ассамблея

Distr.: General
16 April 2007

Russian
Original: English

Комиссия Организации Объединенных Наций по праву международной торговли
Сороковая сессия
Вена, 25 июня – 12 июля 2007 года

Возможная будущая работа в области электронной торговли

Комплексный справочный документ о необходимых элементах правовой базы, благоприятствующей развитию электронной торговли: выборочный раздел, касающийся электронных методов подписания и удостоверения подлинности

Записка Секретариата

Добавление

В приложении к настоящей записке содержится часть (часть вторая, глава I, разделы A и B) выборочного раздела комплексного справочного документа по правовым вопросам, связанным с международным использованием электронных методов подписания и удостоверения подлинности.

V.07-82261 (R) 070507 150507

Приложение

Содержание

Часть вторая

Трансграничное использование электронных методов подписания и удостоверения подлинности

I. Юридическое признание иностранных электронных методов подписания и удостоверения подлинности

1. Двумя основными факторами, затрудняющими трансграничное использование электронных методов подписания и удостоверения подлинности, особенно в случаях, когда они должны выполнять функции юридически действительной подписи, являются юридическая и техническая несовместимость. Техническая несовместимость препятствует взаимодействию систем удостоверения подлинности. Юридическая несовместимость может иметь место в случаях, когда законы, действующие в разных правовых системах, предусматривают различные требования в отношении использования и признания действительными электронных методов подписания и удостоверения подлинности.

A. Международные последствия внутреннего законодательства

2. Там, где внутреннее законодательство допускает использование электронных эквивалентов вместо тех методов удостоверения подлинности, которые основаны на бумажной документации, критерии действительности таких электронных эквивалентов не всегда согласуются между собой. Например, если законом признаются лишь цифровые подписи, то другие формы электронных подписей не будут считаться приемлемыми. Другие противоречия между критериями признания электронных методов подписания и удостоверения подлинности могут в принципе не исключать их трансграничного использования, однако затраты и неудобства, связанные с выполнением требований различных правовых систем, могут частично сводить на нет такие преимущества использования электронных сообщений, как быстрота и эффективность.

3. В нижеследующих разделах говорится о последствиях различных юридических подходов к соответствующим технологиям с точки зрения более широкого трансграничного признания этих технологий. В них также кратко изложен намечающийся международный консенсус в отношении мер, которые потенциально могли бы облегчить использование электронных методов подписания и удостоверения подлинности на международном уровне.

1. Препятствия на международном уровне, возникающие из-за противоречий между национальными подходами

4. Подходы, нейтральные с точки зрения технологии, – особенно те, которые включают "критерий надежности", – обычно позволяют преодолеть юридическую несовместимость. К числу международно-правовых документов, использующих такой подход, относятся Типовой закон ЮНСИТРАЛ об

электронной торговле (пункт 1 (b) статьи 7)[1] и Конвенция Организации Объединенных Наций об использовании электронных сообщений в международных договорах (пункт 3 статьи 9)[2]. Согласно этому подходу электронная подпись или метод удостоверения подлинности, дающие возможность как идентифицировать подписавшую сторону, так и указать намерение этой стороны в отношении информации, содержащейся в электронном сообщении, отвечают требованиям, предъявляемым к подписи, при условии соблюдения нескольких критериев. С учетом всех обстоятельств, включая возможную договоренность между составителем и адресатом сообщения данных, должно быть продемонстрировано, что подпись или метод удостоверения подлинности являются настолько надежными, насколько это соответствует цели, для которой сообщение данных было подготовлено или передано. В качестве альтернативы может быть показано, что они сами по себе или в сочетании с другими подтверждениями обеспечили достижение этих целей.

5. Имеются основания считать, что "минималистский" подход облегчает трансграничное использование электронных методов удостоверения подлинности и электронных подписей, так как согласно этому подходу любой метод электронного подписания или удостоверения подлинности может быть на законных основаниях использован для подписания или заверения договора или сообщения, если он соответствует изложенным выше общим условиям. Однако этот подход ведет к тому, что такие условия, как правило, подтверждаются лишь a posteriori, и нельзя быть уверенным в том, что суд признает правомерным применение того или иного конкретного метода.

6. Трансграничное использование электронных методов удостоверения подлинности и электронных подписей становится реальной проблемой в системах, предписывающих или поощряющих применение той или иной конкретной технологии. Сложность этой проблемы возрастает прямо пропорционально степени государственного регулирования вопросов использования электронных подписей и электронных методов удостоверения подлинности, а также того уровня юридической определенности, которую с точки зрения закона обеспечивает тот или иной метод или технология. Причины этого просты: там, где закон не вкладывает какого-либо специального юридического смысла в конкретные виды электронных подписей или методы удостоверения подлинности и не устанавливает в связи с ними каких-либо презумпций, но просто признает их общую эквивалентность собственноручным подписям или "бумажным" средствам удостоверения подлинности, доверие к электронной подписи чревато таким же риском, как и доверие к собственноручной подписи в рамках действующего законодательства. Там же, где закон устанавливает больше юридических презумпций в связи с определенными видами электронных подписей (обычно теми, которые считаются "защищенными" или "современными"), дополнительный риск перекладывается с одной из сторон на другую. Одна из главных исходных посылок законодательства, привязанного к конкретным технологиям, заключается в том, что степень надежности, обеспечиваемая ими при соблюдении определенных стандартов и процедур, оправдывает такой общий

---

[1] См. сноску [...][издание Организации Объединенных Наций, в продаже под No. R.99.V.4].

[2] См. сноску [...][резолюция 60/21 Генеральной Ассамблеи, приложение].

априорный перенос юридического риска. Недостатком этого подхода является то, что, если надежность изначально предполагает (наряду с другими условиями) использование той или иной конкретной технологии, все другие технологии – и даже эта конкретная технология, применяемая при несколько иных условиях, – становятся априорно ненадежными или во всяком случае подпадают под изначальное подозрение в ненадежности.

7. Таким образом, коллизии национальных законов, привязанных к конкретным технологиям, могут препятствовать, а не способствовать использованию электронных подписей в международной торговле. Это может происходить двумя различными, но тесно взаимосвязанными путями.

8. Во-первых, если в отношении электронных подписей и удостоверяющих их подлинность поставщиков сертификационных услуг в разных правовых системах действуют идущие вразрез друг с другом юридические и технические требования, это может затруднять или исключать использование электронных подписей во многих трансграничных сделках, поскольку эти электронные подписи не способны одновременно удовлетворять требованиям разных правовых систем.

9. Во-вторых, привязанное к конкретным технологиям законодательство, особенно отдающее предпочтение цифровым подписям, – что относится и к "двухуровневому" подходу – имеет тенденцию приводить к появлению множества противоречащих друг другу технических стандартов и лицензионных требований, крайне осложняющих трансграничное использование электронных подписей. Система, при которой каждая страна устанавливает собственные стандарты, может также препятствовать заключению сторонами соглашений о взаимном признании и перекрестной сертификации[3]. Так, одной из главных нерешенных проблем, касающихся, в частности, цифровых подписей, является проблема трансграничного признания. Как отмечает Рабочая группа по безопасности и конфиденциальности информации (РГБКИ) Организации экономического сотрудничества и развития (ОЭСР) (далее именуется "РГБКИ ОЭСР"), хотя подход, принятый в большинстве правовых систем, производит впечатление недискриминационного, расхождения в местных требованиях будут и впредь создавать проблемы, затрудняющие взаимодействие[4]. Применительно к данному исследованию заслуживают внимания следующие из недостатков, на которые указывает РГБКИ ОЭСР:

a) **возможность взаимодействия.** Трудности и препятствия в этом отношении отмечаются повсеместно. На техническом уровне, несмотря на обилие различных стандартов, проблема усматривается в отсутствии единых "базовых" стандартов для некоторых технологий. К факторам, препятствующим прогрессу на юридическом/директивном уровне, относят отсутствие у принципалов достаточной ясности по поводу их отношений с доверенными

---

[3] Stewart Baker and Matthew Yeo, in collaboration with the secretariat of the International Telecommunication Union, “Background and issues concerning authentication and the ITU”, briefing paper presented to the Experts Meeting on Electronic Signatures and Certification Authorities: Issues for Telecommunications, Geneva, 9 and 10 December 1999, Document No. 2.

[4] Organization for Economic Cooperation and Development, Working Party on Information Security and Privacy, *The Use of Authentication across Borders in OECD Countries* (DSTI/ICCP/REG(2005)4/FINAL), http://www.oecd.org/dataoecd/1/10/35809749.pdf, дата посещения – 2 февраля 2007 года.

лицами, включая вопросы передачи ответственности и компенсации. По мнению РГБКИ ОЭСР, эти вопросы "очевидно, требуют более пристального изучения и анализа на предмет возможной разработки общего инструментария, облегчающего достижение между различными правовыми системами того уровня взаимодействия, который желателен для решения той или иной конкретной задачи или функционирования той или иной системы";

b) **признание иностранных услуг по удостоверению подлинности**. По данным РГБКИ ОЭСР, основные усилия до сих пор направлялись на создание для этой цели внутренних служб. Соответственно, механизмы признания иностранных услуг по удостоверению подлинности "в целом не столь хорошо развиты". Исходя из этого, РГБКИ ОЭСР отмечает, что в данной области "представляется полезной дальнейшая работа. Учитывая, что любая такая работа будет тесно связана с более общей темой способности к взаимодействию, эти две темы можно было бы объединить";

c) **признание свидетельств**[5]. В некоторых случаях в качестве препятствия для взаимодействия упоминалось непризнание свидетельств, выданных другими юридическими лицами. В связи с этим РГБКИ ОЭСР предлагает рассмотреть возможность разработки комплекса практических рекомендаций или руководящих принципов, касающихся выдачи свидетельств для целей удостоверения подлинности. В нескольких правовых системах, возможно, уже ведется работа в данном направлении, которая может стать полезным вкладом в любые потенциальные инициативы РГБКИ ОЭСР по этим вопросам;

d) **использование целого ряда методов удостоверения подлинности**. РГБКИ ОЭСР констатировала, что практически во всех государствах – членах ОЭСР применяется целый ряд технических решений для удостоверения подлинности. Они предусматривают различные методы, от использования паролей до аппаратных ключей, цифровых подписей и биометрических данных. В зависимости от конкретной задачи и связанных с ней требований эти методы могут применяться по отдельности или в комбинации друг с другом. Многие могли бы счесть это позитивным моментом, однако информация, собранная РГБКИ ОЭСР в ходе проведенного обследования, свидетельствует о том, что операторы и пользователи соответствующих систем, столкнувшись со столь широким спектром возможностей, рискуют оказаться полностью дезориентированными относительно того, какой из методов наиболее отвечает их потребностям. По мнению РГБКИ ОЭСР, это указывает на целесообразность

---

[5] Под свидетельством понимается опознавательное средство, подтверждающее, что данное лицо или устройство прошло процедуру удостоверения. Свидетельства, привязанные к их держателю, необходимы для целей идентификации. Для получения некоторых видов полномочий может быть достаточно свидетельства, оформленного на предъявителя. Примерами могут служить действительное водительское удостоверение, индивидуальный номер физического лица в системе социального страхования или иной идентификационный номер, а также пластиковые карты с микропроцессорами. Centre for Democracy and Technology, “Privacy principles for authentication systems”, http://tprc.org/papers/2003/183/CDTauthenticationTPRC.pdf, дата посещения – 12 апреля 2007 года); см. также Centre for Democracy and Technology, Authentication Privacy Principles Working Group, “Interim report on privacy principles for authentication systems”, http://www.cdt.org/privacy/authentication/030513interim.pdf, дата посещения – 12 апреля 2007 года).

подготовки справочного пособия, позволяющего оценивать различные методы удостоверения подлинности и определять, насколько их свойства отвечают требованиям операторов или пользователей систем.

10. Повышению доверия к электронным методов подписания и удостоверения подлинности при международных сделках могли бы способствовать широкое принятие Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах и применение предусмотренного ею подхода к электронным подписям и удостоверению подлинности, нейтрального с точки зрения технологии. Однако было бы нереалистичным ожидать, что это полностью устранит необходимость согласованного решения проблемы несовместимости юридических и технических стандартов. Во многих странах по-прежнему предписывается использование конкретных методов удостоверения подлинности при сделках определенных видов. Кроме того, некоторые страны могут ощущать потребность в более конкретных рекомендациях по оценке надежности методов подписания и удостоверения подлинности, особенно применяемых в других странах, и степени их эквивалентности методам, используемым или хотя бы известным в данной стране.

2. Формирующийся консенсус

11. Наметившиеся на международном уровне расхождения в политике, по всей вероятности, обусловлены различными комбинациями ряда факторов. Как показано выше (см. пункты [...]-[...] выше), некоторые страны придерживаются более строгих и детализированных требований в отношении формы подписей и документов, тогда как другие уделяют основное внимание намерениям подписавшей стороны и допускают подтверждение действительности подписи множеством различных способов. Эти общие расхождения обычно находят свое отражение в конкретных законодательных актах, касающихся электронных методов подписания и удостоверения подлинности (см. пункты [...]-[...] выше). Еще одной причиной расхождений являются различия в степени государственного вмешательства в технические аспекты электронного подписания и удостоверения подлинности. Правительства некоторых стран склонны непосредственно участвовать в определении стандартов для новых технологий, возможно, полагая, что это обеспечивает конкурентные преимущества отечественным компаниям[6].

12. Различные подходы в политике также могут быть следствием несовпадения взглядов на то, как будут развиваться технологии удостоверения подлинности в будущем. Согласно одному из сценариев, получившему название "универсальная парадигма удостоверения подлинности"[7], главной целью технологии удостоверения подлинности будет проверка личности и других сведений о лицах, не состоявших ранее в каких-либо отношениях друг с другом, для которых совместное использование технических средств не является предметом юридического договора. Соответственно, технология подписания или удостоверения подлинности должна позволять удостоверять личность или иные сведения о том или ином лице для потенциально неограниченного круга других

---

[6] См. сноску [...][Background and issues concerning authentication and the ITU].

[7] Там же.

лиц и для потенциально неограниченного числа целей. Данная модель ставит во главу угла технические стандарты и функциональные требования поставщиков сертификационных услуг, когда речь идет об участии доверенных третьих сторон. Другой сценарий – так называемая "ограниченная парадигма удостоверения подлинности" – исходит из того, что основным назначением технологий подписания и удостоверения подлинности будет проверка личности и других сведений о лицах, совместно использующих технические средства в рамках юридических договоров[8]. Соответственно, технология удостоверения подлинности должна позволять удостоверять личность или другие сведения о держателе сертификата лишь для ряда конкретных целей и для ограниченного круга потенциальных полагающихся сторон, связанных общими условиями использования данной технологии. В этой модели основное значение придается юридическому признанию договорных отношений.

13. Несмотря на эти расхождения, некоторые из которых сохраняются по сей день, выводы РГБКИ ОЭСР[9] указывают на расширяющийся международный консенсус в отношении основных принципов, которыми должна регулироваться электронная торговля и, в частности, использование электронных подписей. Для целей настоящего исследования наибольший интерес представляют следующие выводы:

a) **недискриминационный подход к "иностранным" подписям и услугам**. Законодательные положения не отрицают юридической силы подписей, созданных с помощью служб, базирующихся в других странах, если эти подписи были созданы при таких же условиях, как те, которые имеют юридическую силу в данной стране. С этой точки зрения данный подход представляется недискриминационным при условии выполнения местных или эквивалентных им требований. Это соответствует выводам предыдущих обследований по вопросам удостоверения подлинности, проводившихся РГБКИ ОЭСР;

b) **нейтральность с точки зрения технологий.** Хотя практически все респонденты указывали, что принятые у них нормативно-правовые рамки деятельности служб удостоверения подлинности и создания электронных подписей нейтральны с точки зрения технологии, большинство отмечало, что при использовании электронных средств для правительственных нужд и в случаях, когда в отношении электронной подписи требуется максимальная юридическая определенность, предписывается использование инфраструктуры публичных ключей (ИПК). Таким образом, даже при технологической нейтральности законодательных норм, на директивном уровне, по-видимому, требуется применение конкретных технологий;

c) **преобладание ИПК**. Согласно данным РГБКИ ОЭСР, в случаях, когда требуется надежное удостоверение личности и высокая юридическая определенность электронной подписи, предпочтение при выборе метода удостоверения отдается ИПК. Она используется в конкретных "сообществах по интересам", где все пользователи, по-видимому, уже состоят друг с другом в тех или иных деловых отношениях. Внедрение поддерживающих ИПК микропроцессорных карт и оснащение прикладных программ встроенными функциями выдачи и проверки цифровых сертификатов упростили для

---

[8] Там же.

[9] См. сноску [...][*The Use of Authentication across Borders in OECD Countries*].

пользователей применение этого метода. Вместе с тем обычно признается, что ИПК необходима не во всех случаях и что выбор метода удостоверения подлинности должен определяться его соответствием тем задачам, для которых он будет использоваться.

14. Кроме того, РГБКИ ОЭСР констатировала, что во всех охваченных обследованием странах имеется тот или иной комплекс законодательных или нормативных положений, обеспечивающих юридическую силу электронных подписей в пределах данной страны. РГБКИ ОЭСР пришла к выводу о том, что хотя законы разных правовых систем могут различаться в деталях, в них просматривается и общий подход, заключающийся в том, что большинство этих законов опираются на существующие международные или транснациональные правовые режимы (в частности, Типовой закон ЮНСИТРАЛ об электронных подписях и Директиву 1999/93/ЕС Европейского парламента и Совета об основах законодательства Сообщества в отношении электронных подписей)[10].

B. Критерии признания иностранных электронных методов подписания и удостоверения подлинности

15. Как уже отмечалось, одним из основных препятствий для трансграничного использования электронных подписей и методов удостоверения подлинности является отсутствие возможности взаимодействия, обусловленное противоречиями и расхождениями в стандартах либо их непоследовательным применением. Для содействия применению ИПК, опирающейся на соответствующие стандарты, обеспечивающей такое взаимодействие и способной лечь в основу обеспечения надежности электронных коммерческих сделок, учрежден целый ряд форумов. В их число входят как межправительственные[11], так и смешанные государственно-частные организации[12] глобального[13] и регионального уровня.

---

[10] *Official Journal of the European Communities*, L 13/12, 19 January 2000.

[11] В Азиатско-тихоокеанском регионе имеются разработанные Азиатско-тихоокеанским форумом по экономическому сотрудничеству (АТЭС) "Руководящие принципы для систем выдачи сертификатов, пригодных к использованию в электронной торговле между субъектами, относящимися к различным правовым системам" (eSecurity Task Group, APEC Telecommunications and Information Working Group, December 2004; http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf; дата посещения – 12 апреля 2007 года). Эти руководящие принципы предназначены в помощь при разработке потенциально способных к взаимодействию систем и оценке возможности взаимодействия систем, которые уже существуют. Руководящие принципы охватывают категории или типы сертификатов, используемые только в транснациональной электронной торговле. Они не рассчитаны на сертификаты других типов и не претендуют на то, чтобы ограничить круг выдаваемых сертификатов лишь теми, которые подпадают под эти руководящие принципы.

[12] В Европейском союзе в 1999 году Совет по стандартам в области информационных и коммуникационных технологий (ИКТ) учредил Европейскую инициативу по стандартам для электронных подписей (ЕИСЭП), призванную координировать деятельность по стандартизации во исполнение Директивы Европейского союза 1999/93/ЕС об электронных подписях. Совет по стандартам в области ИКТ сам представляет собой инициативу Европейского комитета по стандартизации (ЕКС), созданного национальными организациями по стандартизации при участии двух некоммерческих организаций –

16. Часть этой работы направлена на определение технических стандартов представления информации, необходимой для выполнения определенных юридических требований[14]. Однако в значительной мере эта важная работа посвящена именно техническим, а не юридическим аспектам и выходит за рамки настоящего исследования. Поэтому в последующих разделах основное внимание уделяется формальным и материально-правовым требованиям, касающимся трансграничного признания электронных подписей.

Европейского комитета по электротехническим стандартам (СЕНЕЛЕК) и Европейского института по стандартизации в области электросвязи (ЕТСИ). В рамках ЕИСЭП разработан ряд стандартов, рассчитанных на облегчение взаимодействия, которые, однако, внедряются медленными темпами, якобы из-за их сложности (Paolo Balboni, "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication," *Information and Communications Technology Law*, vol. 13, No. 3, 2004), pp. 211-242, 214.

[13] Например, Организация по развитию стандартов структурированной информации (ОРССИ) – некоммерческий международный консорциум, основанный в 1993 году в целях содействия разработке, сближению и принятию стандартов для электронных сделок. ОРССИ учредила Технический комитет по ИПК, в состав которого входят пользователи ИПК, ее поставщики и эксперты в этой области и в котором рассматриваются вопросы внедрения технологии цифровых сертификатов. Техническим комитетом ОРССИ по ИПК составлен план действий, который предусматривает, в частности, выработку конкретных моделей или руководящих принципов практического применения стандартов, обеспечивающих возможность взаимодействия систем ИПК; установление новых стандартов по мере необходимости; а также разработку тестов на способность к взаимодействию и проведение мероприятий по тестированию (OASIS, PKI Technical Committee, "PKI action plan" (February 2004), http://www.oasis-open.org/committees/pki/pkiactionplan.pdf; дата посещения – 12 апреля 2007 года.

[14] Например, ЕТСИ разработал стандарт (TS 102 231) для реализации неиерархической структуры, обеспечивающей, среди прочего, возможность взаимного признания между доменами ИПК и, соответственно, подтверждения действительности сертификатов. Смысл технического стандарта ЕТСИ TS 102 231 сводится к определению параметров представления информации о статусе поставщика сертификационных услуг (trust service provider). Он имеет форму скрепленного подписью списка, именуемого "Trust-service Status List", на основе которого представляется соответствующая информация. Такой "статусный список", составляемый согласно спецификациям ЕТСИ, отвечает требованию относительно подтверждения того, была ли деятельность поставщика сертификационных услуг санкционирована той или иной общепризнанной системой – будь то на момент оказания услуг или на момент совершения сделки сторонами, полагающимися на эти услуги. Чтобы соответствовать этому требованию, "статусный список" должен содержать информацию, позволяющую установить, был ли оператор упомянутой системы на момент сделки осведомлен о сертификационных услугах, оказываемых данным поставщиком, и если да, то каким был статус выданного этому поставщику разрешения (т.е. было ли оно действительно, приостановлено, аннулировано или отозвано). Таким образом, "статусный список", предусмотренный техническим стандартом ЕТСИ TS 102 231, должен содержать информацию не только о текущем, но и о прошлом статусе поставщика услуг. Иными словами, он сочетает в себе перечень поставщиков, имеющих действительные разрешения ("белый" список), и поставщиков, чьи разрешения аннулированы или отозваны ("черный" список) (см. http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc, дата посещения – 4 марта 2007 года).

1. Место происхождения, взаимность и подтверждение в другой стране

17. Место происхождения является одним из традиционных факторов, определяющих юридическое признание иностранных документов или действий. Как правило, такое признание имеет место на основе взаимности, т.е. подписи и сертификаты из соответствующей страны наделяются внутри государства такой же юридической силой, какая признается за подписями и сертификатами этого государства в стране их происхождения. Еще одним фактором в этой связи является требование о том, чтобы иностранные подписи и сертификаты так или иначе заверялись или подтверждались отечественным поставщиком сертификационных услуг, сертификационным или регулирующим органом. Иногда имеет место сочетание всех этих факторов[15].

18. Национальные законы обычно не содержат положений, прямо исключающих юридическое признание подписей или сертификатов иностранного происхождения, что может восприниматься как свидетельство их недискриминационного характера. На практике, однако, положения о признании, предусмотренные во многих правовых режимах, часто ведут, пусть и непреднамеренно, к тем или иным дискриминационным последствиям. Так, Директива Европейского союза об электронных подписях в целом запрещает дискриминацию иностранных сертификатов, соответствующих установленным требованиям (т.е. цифровых подписей на основе ИПК). Однако на практике это касается главным образом сертификатов, выданных поставщиками сертификационных услуг, учрежденными на территории государств – членов Европейского союза. Поставщик сертификационных услуг, базирующийся в стране, которая не входит в Европейский союз, может обеспечить признание своих сертификатов в Европейском союзе тремя способами: выполнить требования Директивы Европейского союза об электронных подписях и получить аккредитацию в системе, учрежденной в одном из государств-членов; заключить соглашение о перекрестной сертификации с поставщиком сертификационных услуг, учрежденным в одном из государств – членов Европейского союза; либо действовать в рамках общих положений о признании, предусмотренных на уровне международного соглашения[16]. То, как в Директиве Европейского союза регулируются соответствующие международные аспекты, позволяет предположить, что одной из ее целей было создание условий для

---

[15] В Аргентине, например, иностранные сертификаты и электронные подписи признаются при наличии соглашения о взаимности между Аргентиной и страной происхождения иностранного сертификационного органа либо в случае их "признания сертификационным органом, лицензированным в Аргентине и имеющим удостоверение, выданное правоприменительной инстанцией" (см. Ley de firma digital (2001), статья 16).

[16] Так, в соответствии со статьей 7 упомянутой Директивы, государства – члены Европейского союза обязаны обеспечить признание сертификатов, выданных поставщиком сертификационных услуг в третьей стране, юридически эквивалентными сертификатам, выданным поставщиком сертификационных услуг, учрежденным на территории Сообщества, только в следующих случаях: a) если данный поставщик сертификационных услуг "отвечает требованиям, изложенным в данной Директиве, и аккредитован в системе добровольной аккредитации, учрежденной в одном из государств-членов"; b) если сертификат "гарантирован" поставщиком сертификационных услуг, учрежденным на территории Сообщества и отвечающим требованиям, изложенным в данной Директиве; или c) если сертификат или поставщик сертификационных услуг "признан в рамках двустороннего или многостороннего соглашения между Сообществом и третьими странами или международными организациями".

доступа поставщиков сертификационных услуг из стран Европейского союза на внешние рынки[17]. Присовокупляя к требованию относительно эквивалентности существу норм Европейского союза дополнительное требование "аккредитации в системе, учрежденной в одном из государств-членов", Директива Европейского союза об электронных подписях фактически требует от иностранных поставщиков сертификационных услуг соблюдения как своего национального режима, так и режима Европейского союза, т.е. устанавливает для них более высокий стандарт, чем тот, который применяется к поставщикам сертификационных услуг, аккредитованных в государствах – членах Европейского союза[18].

19. В части практического выполнения статьи 7 Директивы Европейского союза об электронных подписях имеют место определенные вариации[19]. Например, в Ирландии и на Мальте иностранные цифровые подписи (или, согласно терминологии Европейского союза, отвечающие установленным требованиям сертификаты) признаются эквивалентными отечественным подписям, при условии соблюдения других юридических требований. В других случаях такое признание обусловлено подтверждением в принимающей стране (Австрия, Люксембург) или решением внутренней инстанции (Чешская Республика, Эстония, Польша). Такая тенденция к обязательному сохранению национального контроля в той или иной форме, которое, как правило, обосновывают законными сомнениями в надежности иностранных сертификатов, на практике приводит к возникновению системы дискриминации таких сертификатов по признаку их географического происхождения.

2. Эквивалентность по существу

20. Следуя давней традиции, ЮНСИТРАЛ не дала согласия на включение географических соображений в число факторов, определяющих признание иностранных сертификатов и электронных подписей. Так, в пункте 1 статьи 12 Типового закона ЮНСИТРАЛ об электронных подписях прямо говорится, что при определении того, обладает ли – или в какой мере обладает – сертификат или электронная подпись юридической силой, "не учитываются" ни "место выдачи сертификата или создания или использования электронной подписи", ни "местонахождение коммерческого предприятия эмитента или подписавшего".

21. В пункте 1 статьи 12 Типового закона ЮНСИТРАЛ об электронных подписях имелось в виду отразить тот основополагающий принцип, что место происхождения само по себе ни в коей мере не следует считать фактором, определяющим то, должны ли сертификаты или электронные подписи

---

[17] О стремлении обеспечить европейским поставщикам сертификационных услуг доступ на иностранные рынки наглядно свидетельствует формулировка пункта 3 статьи 7 Директивы, согласно которому "[е]сли Комиссии становится известно о каких-либо трудностях, испытываемых предприятиями Сообщества при получении доступа на рынки третьих стран, она может, в случае необходимости, представить Совету предложения относительно соответствующего мандата на проведение переговоров о предоставлении предприятиям Сообщества сопоставимых прав в таких третьих странах".

[18] Jos Dumortier and others, “The legal and market aspects of electronic signatures- Study for the European Commission Directorate General Information Society” (Katholieke Universiteit Leuven, 2003), p. 58.

[19] Там же., pp. 92-94.

иностранного происхождения признаваться способными обладать юридической силой, и если должны, то в какой степени. Вопрос о том, может ли электронная подпись обладать юридической силой, и если да, то в какой степени, должен решаться в зависимости от ее технической надежности, а не от места, где был выдан сертификат или создана электронная подпись. Положения о недискриминации, аналогичные статье 12 Типового закона об электронных подписях, можно найти и в некоторых национальных режимах, таких как Закон Соединенных Штатов Америки от 2000 года об электронных подписях в глобальной и национальной торговле[20]. Согласно этим положениям, место происхождения само по себе не следует считать фактором, определяющим то, должны ли сертификаты или электронные подписи иностранного происхождения признаваться в принимающем Закон государстве способными обладать юридической силой, и если должны, то в какой степени. В них устанавливается, что юридическая сила сертификата или электронной подписи должна зависеть от их технической надежности[21].

22. Вместо географических факторов Типовой закон предусматривает критерий эквивалентной надежности, по существу обеспечиваемой соответствующими сертификатами и подписями. Так, если сертификат иностранного происхождения обеспечивает уровень надежности, "по существу эквивалентный" уровню надежности сертификата, выданного в принимающем Типовой закон государстве, то он обладает "такой же юридической силой". Аналогичным образом, электронная подпись, созданная или использованная за пределами страны, "обладает такой же юридической силой", как и электронная подпись, созданная или использованная в данной стране, "если она обеспечивает по существу эквивалентный уровень надежности". Эквивалентность уровней надежности, обеспечиваемых сертификатами и подписями иностранного и внутреннего происхождения, должна определяться исходя из признанных международных стандартов и любых других соответствующих факторов, включая наличие между сторонами договоренности об использовании определенных видов электронных подписей или сертификатов, за исключением случаев, когда такая договоренность не будет действительной или не будет иметь правовых последствий согласно применимому праву.

23. Типовой закон не содержит положений о взаимности и не побуждает к их принятию. В нем не предусмотрено "никаких конкретных предложений" относительно "правовых методов, с помощью которых принимающее Типовой закон государство может обеспечить заблаговременное признание надежности сертификатов и подписей, отвечающих требованиям законодательства зарубежной страны (например, посредством односторонней декларации или договора)"[22]. К возможным методам достижения этого результата, упоминавшимся в ходе подготовки Типового закона, относится, например, автоматическое признание подписи, соответствующей законам другого государства, если законы иностранного государства предусматривают уровень надежности, по меньшей мере эквивалентный тому, который требуется от

---

[20] См. сноску […][United States Code, title 15, chapter 96, section 7031 (Principles governing the use of electronic signatures in international transactions)].

[21] См. *Типовой закон ЮНСИТРАЛ об электронных подписях и Руководство по принятию,* Часть вторая, пункт 83.

[22] Там же, пункт 157.

эквивалентных подписей внутреннего происхождения. В число других правовых методов, с помощью которых принимающее Типовой закон государство может обеспечить заблаговременное признание надежности иностранных сертификатов и подписей, могут входить односторонние декларации или договоры[23].

---

[23] См. Доклад Рабочей группы по электронной торговле о работе ее тридцать седьмой сессии (A/CN.9/483), пункты 39 и 42.