Организация Объединенных Наций A/CN.9/WG.IV/WP.88

Генеральная Ассамблея

Distr.: Limited
30 January 2001

Russian
Original: English

**Комиссия Организации Объединенных Наций
по праву международной торговли
Рабочая группа
по электронной торговле**
Тридцать восьмая сессия
Нью-Йорк, 12–23 марта 2001 года

Электронные подписи

Проект руководства по принятию Типового закона ЮНСИТРАЛ об электронных подписях

Записка Секретариата

1. В соответствии с решениями, принятыми Комиссией на ее двадцать девятой (1996 год)[1] и тридцатой (1997 год)[2] сессиях, Рабочая группа по электронной торговле посвятила свои тридцать первую – тридцать седьмую сессии подготовке проекта типового закона ЮНСИТРАЛ об электронных подписях (далее в тексте – "Типовой закон", "проект типового закона" или "новый Типовой закон"). Доклады о работе этих сессий содержатся в документах A/CN.9/437, 446, 454, 457, 465, 467 и 483. При подготовке Типового закона Рабочая группа отметила, что было бы полезно представить в комментарии дополнительную информацию относительно Типового закона. С учетом подхода, использованного при разработке Типового закона ЮНСИТРАЛ об электронной торговле, была выражена общая поддержка предложению о подготовке сопровождающего новый Типовой закон руководства с целью предоставления государствам помощи в принятии и применении Типового закона. Это руководство, которое в значительной степени может основываться на *подготовительных материалах*, использованных в ходе работы над Типовым законом, было бы также полезным и для других пользователей Типового закона.

2. На своей тридцать седьмой сессии Рабочая группа завершила разработку проектов статей Типового закона и обсудила проект руководства по принятию Типового закона на основе записки Секретариата (A/CN.9/WG.IV/WP.86 и Add.1). Секретариату было предложено подготовить пересмотренный вариант проекта руководства, отражающий решения, которые были приняты Рабочей группой, на основе различных мнений, предложений и замечаний, высказанных на ее тридцать седьмой сессии. Из-за нехватки времени Рабочая группа не завершила рассмотрение проекта руководства по принятию (см. документ A/CN.9/483, пункты 23 и 145–152). Было решено выделить определенное время для завершения рассмотрения этого пункта повестки дня на тридцать восьмой сессии Рабочей группы. Отмечалось, что проект типового закона, наряду с проектом руководства по принятию, будет представлен Комиссии для рассмотрения и принятия на ее тридцать четвертой сессии, которая будет проходить в Вене 25 июня – 31 июля 2001 года.

3. В приложении к настоящей записке содержится пересмотренный вариант проекта руководства, подготовленный Секретариатом.

Приложение

ТИПОВОЙ ЗАКОН ЮНСИТРАЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

И

РУКОВОДСТВО ПО ПРИНЯТИЮ
2001 ГОД

СОДЕРЖАНИЕ

Часть первая

ТИПОВОЙ ЗАКОН ЮНСИТРАЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ (2001 год)

(принятый Рабочей группой ЮНСИТРАЛ по электронной торговле на ее тридцать седьмой сессии, проходившей в Вене 18–29 сентября 2000 года)

Статья 1. Сфера применения

Настоящий Закон применяется в тех случаях, когда электронные подписи используются в контексте* торговой** деятельности. Он не имеет преимущественной силы по отношению к любой правовой норме, предназначенной для защиты потребителей.

* Для государств, которые, возможно, пожелают расширить сферу применения настоящего Закона, Комиссия предлагает следующий текст:

"Настоящий Закон применяется в тех случаях, когда используются электронные подписи, за исключением следующих ситуаций: […]".

** Термин "торговая" следует толковать широко, с тем чтобы он охватывал вопросы, вытекающие из всех отношений торгового характера, как договорных, так и недоговорных. Отношения торгового характера включают следующие сделки, не ограничиваясь ими: любые торговые сделки на поставку товаров или услуг или обмен товарами или услугами; дистрибьюторские соглашения; коммерческое представительство и агентские отношения; факторинг; лизинг; строительство промышленных объектов; предоставление консультативных услуг; инжиниринг; купля/продажа лицензий; инвестирование; финансирование; банковские услуги; страхование; соглашения об эксплуатации или концессии; совместные предприятия и другие формы промышленного или предпринимательского сотрудничества; перевозка товаров и пассажиров воздушным, морским, железнодорожным и автомобильным транспортом.

Статья 2. Определения

Для целей настоящего Закона:

a) "электронная подпись" означает данные в электронной форме, которые содержатся в сообщении данных, приложены к нему или логически ассоциируются с ним и которые могут быть использованы для идентификации подписавшего в связи с сообщением данных и указания на то, что подписавший согласен с информацией, содержащейся в сообщении данных;

b) "сертификат" означает сообщение данных или иную запись, подтверждающую наличие связи между подписавшим и данными для создания подписи;

c) "сообщение данных" означает информацию, подготовленную, отправленную, полученную или хранимую с помощью электронных, оптических или аналогичных средств, включая электронный обмен данными (ЭДИ), электронную почту, телеграмму, телекс или телефакс, но не ограничиваясь ими;

d) "подписавший" означает лицо, которое обладает данными для создания подписи и действует от своего собственного имени или от имени лица, которое оно представляет;

e) "поставщик сертификационных услуг" означает лицо, которое выдает сертификаты и может предоставлять другие услуги, связанные с электронными подписями;

f) "полагающаяся сторона" означает лицо, которое может действовать на основании сертификата или электронной подписи.

Статья 3. Равный режим для технологий создания электронных подписей

Ничто в настоящем Законе, за исключением статьи 5, не применяется таким образом, чтобы исключать, ограничивать или лишать юридической силы любой метод создания электронной подписи, который удовлетворяет требованиям, указанным в статье 6(1), или иным образом отвечает требованиям применимого права.

Статья 4. Толкование

1) При толковании настоящего Закона следует учитывать его международное происхождение и необходимость содействовать достижению единообразия в его применении и соблюдению добросовестности.

2) Вопросы, которые относятся к предмету регулирования настоящего Закона и которые прямо в нем не разрешены, подлежат разрешению в соответствии с общими принципами, на которых основан настоящий Закон.

Статья 5. Изменение по договоренности

Допускается отход от положений настоящего Закона или изменение их действия по договоренности, за исключением случаев, когда такая договоренность не будет действительной или не будет иметь правовых последствий согласно применимому праву.

Статья 6. Соблюдение требования в отношении наличия подписи

1) В тех случаях, когда законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если использована электронная подпись, которая является настолько надежной, насколько это соответствует цели, для которой сообщение данных было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности.

2) Пункт 1 применяется как в тех случаях, когда упомянутое в нем требование имеет форму обязательства, так и в тех случаях, когда законодательство просто предусматривает наступление определенных последствий, если подпись отсутствует.

3) Электронная подпись считается надежной для цели удовлетворения требования, упомянутого в пункте 1, если:

a) данные для создания электронной подписи в том контексте, в котором они используются, связаны с подписавшим и ни с каким другим лицом;

b) данные для создания электронной подписи в момент подписания находились под контролем подписавшего и никакого другого лица;

c) любое изменение, внесенное в электронную подпись после момента подписания, поддается обнаружению; и

d) в тех случаях, когда одна из целей правового требования в отношении наличия подписи заключается в гарантировании целостности информации, к которой она относится, любое изменение, внесенное в эту информацию после момента подписания, поддается обнаружению.

4) Пункт 3 не ограничивает возможности любого лица в отношении:

a) установления любым другим способом для цели удовлетворения требования, упомянутого в пункте 1, надежности электронной подписи; или

b) представления доказательств ненадежности электронной подписи.

5) Положения настоящей статьи не применяются в следующих случаях: […]

Статья 7. Удовлетворение требований статьи 6

1) [*Любое лицо, орган или ведомство, будь то публичное или частное, назначенное принимающим государством в качестве компетентного лица, органа или ведомства*] может определять, какие электронные подписи удовлетворяют требованиям статьи 6.

2) Любое определение, вынесенное в соответствии с пунктом 1, должно соответствовать признанным международным стандартам.

3) Ничто в настоящей статье не затрагивает действия норм международного частного права.

Статья 8. Поведение подписавшего

1) В тех случаях, когда данные для создания подписи могут быть использованы для создания подписи, имеющей юридическую силу, каждый подписавший обязан:

a) проявлять разумную осмотрительность для недопущения несанкционированного использования его данных для создания подписи;

b) без неоправданных задержек уведомлять любое лицо, которое, как подписавший может разумно предполагать, полагается на электронную подпись или предоставляет услуги в связи с ней, если:

i) подписавшему известно, что данные для создания подписи были скомпрометированы; или

ii) обстоятельства, известные подписавшему, обусловливают существенный риск того, что данные для создания подписи могли быть скомпрометированы;

c) в тех случаях, когда для подтверждения электронной подписи используется сертификат, проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от подписавшего существенных заверений, которые относятся к жизненному циклу сертификата или которые должны быть включены в сертификат.

2) Подписавший несет ответственность за невыполнение требований пункта 1.

Статья 9. Поведение поставщика сертификационных услуг

1) В тех случаях, когда поставщик сертификационных услуг предоставляет услуги для подкрепления электронной подписи, которая может быть использована в качестве подписи, имеющей юридическую силу, такой поставщик сертификационных услуг:

a) действует в соответствии с заверениями, которые он делает в отношении своей политики и практики;

b) проявляет разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений, которые относятся к жизненному циклу сертификата или которые включены в сертификат;

c) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить по сертификату:

i) личность поставщика сертификационных услуг;
ii) что подписавший, который идентифицирован в сертификате, имел контроль над данными для создания подписи в момент выдачи сертификата;
iii) что данные для создания подписи были действительными в момент или до момента выдачи сертификата;

d) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить, соответственно, по сертификату или иным образом:

i) метод, использованный для идентификации подписавшего;
ii) любые ограничения в отношении целей или стоимостного объема, в связи с которыми могут использоваться данные для создания подписи или сертификат;
iii) что данные для создания подписи являются действительными и не были скомпрометированы;
iv) любые ограничения в отношении масштаба или объема ответственности, оговоренные поставщиком сертификационных услуг;
v) существуют ли средства для направления подписавшим уведомления в соответствии со статьей 8(1)(b);
vi) предлагается ли услуга по своевременному аннулированию;

e) в тех случаях, когда предлагаются услуги, предусмотренные в подпункте (d)(v), обеспечивает подписавшего средствами для направления уведомления в соответствии со статьей 8(1)(b), и, в тех случаях, когда предлагаются

услуги, предусмотренные в подпункте (d)(vi), обеспечивает наличие услуг по своевременному аннулированию;

f) использует надежные системы, процедуры и людские ресурсы при предоставлении своих услуг.

2) Поставщик сертификационных услуг несет ответственность за невыполнение требований пункта 1.

Статья 10. Надежность

Для целей статьи 9(1)(f) при определении того, являются ли – или в какой мере являются – любые системы, процедуры и людские ресурсы, используемые поставщиком сертификационных услуг, надежными, могут учитываться следующие факторы:

a) финансовые и людские ресурсы, в том числе наличие активов;

b) качество систем аппаратного и программного обеспечения;

c) процедуры для обработки сертификатов и заявок на сертификаты и хранения записей;

d) наличие информации для подписавших, идентифицированных в сертификатах и для потенциальных полагающихся сторон;

e) регулярность и объем аудита, проводимого независимым органом;

f) наличие заявления, сделанного государством, аккредитующим органом или поставщиком сертификационных услуг в отношении соблюдения или наличия вышеуказанного; или

g) любые другие соответствующие факторы.

Статья 11. Поведение полагающейся стороны

Полагающая сторона несет правовые последствия в случае:

a) непринятия ею разумных мер для проверки надежности электронной подписи; или

b) когда электронная подпись подкрепляется сертификатом, непринятия ею разумных мер:

i) для проверки действительности, приостановления действия или аннулирования сертификата; и
ii) для соблюдения любых ограничений в отношении сертификата.

Статья 12. Признание иностранных сертификатов и электронных подписей

1) При определении того, обладает ли – или в какой мере обладает – сертификат или электронная подпись юридической силой, не учитываются:

a) место выдачи сертификата или создания или использования электронной подписи, или

b) местонахождение коммерческого предприятия эмитента или подписавшего.

2) Сертификат, выданный за пределами [*принимающее государство*], обладает такой же юридической силой в [*принимающее государство*], как и сертификат, выданный в [*принимающее государство*], если он обеспечивает по существу эквивалентный уровень надежности.

3) Электронная подпись, созданная или используемая за пределами [*принимающее государство*], обладает такой же юридической силой в [*принимающее государство*], как и электронная подпись, созданная или используемая в [*принимающее государство*], если она обеспечивает по существу эквивалентный уровень надежности.

4) При определении того, обеспечивает ли сертификат или электронная подпись по существу эквивалентный уровень надежности для целей пункта 2 или 3, следует учитывать признанные международные стандарты и любые другие соответствующие факторы.

5) В тех случаях, когда, независимо от положений пунктов 2, 3 и 4, стороны договариваются между собой в отношении использования определенных видов электронных подписей или сертификатов, такая договоренность признается достаточной для цели трансграничного признания, за исключением случаев, когда такая договоренность не будет действительной или не будет иметь правовых последствий согласно применимому праву.

Часть вторая

РУКОВОДСТВО ПО ПРИНЯТИЮ ТИПОВОГО ЗАКОНА ЮНСИТРАЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ (2001 ГОД)

Цель настоящего Руководства

1. При подготовке и принятии Типового закона ЮНСИТРАЛ об электронных подписях (также именуемого в этой публикации "Типовым законом" или "новым Типовым законом") Комиссия Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ) учитывала, что Типовой закон даст в распоряжение государств более эффективное средство для модернизации их законодательства, если исполнительным правительственным органам и законодателям будут предоставлены справочная информация и пояснения, которые могут оказать им помощь в применении Типового закона. Комиссия также учитывала вероятность того, что Типовой закон будет применяться в ряде государств, в которых недостаточно известны методы передачи сообщений, рассматриваемые в Типовом законе. Настоящее Руководство, которое в значительной мере основывается на подготовительных материалах, использованных в ходе работы над Типовым законом, также предназначено для оказания помощи другим пользователям текста, таким как судьи, арбитражные судьи, практические работники и лица, занимающиеся научной работой в этой области. Такая информация может быть также полезной для государств при рассмотрении вопроса о том, какие положения – если в этом вообще возникнет необходимость – следует изменить, с тем чтобы учесть какие-либо особые национальные обстоятельства, обусловливающие необходимость в таких изменениях. Исходная посылка, используемая при подготовке Типового закона, состояла в том, что Типовой закон будет сопровождаться таким руководством. Например, в отношении ряда вопросов было принято решение отказаться от их урегулирования в самом Типовом законе, однако рассмотреть их в Руководстве, с тем чтобы государства могли воспользоваться соответствующими рекомендациями при принятии Типового закона. Цель представленной в настоящем Руководстве информации состоит в том, чтобы пояснить, почему в Типовой закон были включены положения, являющиеся важнейшими базовыми нормами законодательного инструмента, предназначенного для достижения целей Типового закона.

2. Настоящее Руководство по принятию было подготовлено Секретариатом в ответ на просьбу, высказанную ЮНСИТРАЛ при завершении ее тридцать четвертой сессии в 2001 году. Оно основывается на обсуждениях и решениях Комиссии на этой сессии, на которой был принят Типовой закон, а также на обсуждениях, проведенных в Рабочей группе по электронной торговле, которая осуществляла подготовительную работу.

Глава I. Введение к Типовому закону

I. ЦЕЛЬ И ПРОИСХОЖДЕНИЕ ТИПОВОГО ЗАКОНА

A. Цель

3. Расширение использования электронных методов удостоверения подлинности в качестве замены собственноручных подписей и других традиционных процедур удостоверения подлинности обусловило необходимость в специальной законодательной базе для сокращения неопределенности в отношении правовых последствий, которые могут быть созданы в результате использования таких современных методов (которые в целом можно назвать "электронными подписями"). Опасность того, что в различных странах будут использованы различающиеся законодательные подходы к урегулированию вопросов об электронных подписях, требует подготовки унифицированных законодательных положений, которые легли бы в основу базовых норм регулирования этой по сути международной концепции, для которой важнейшее значение имеет юридическая (а также техническая) взаимосопоставимость.

4. Новый Типовой закон, который разрабатывался с учетом фундаментальных принципов, лежащих в основе статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле (неизменно именуемого в этой публикации его полным названием во избежание путаницы), применительно к выполнению функции подписи в электронной среде, направлен на то, чтобы оказать государствам помощь в создании современной, унифицированной и взвешенной законодательной базы для более эффективного регулирования вопросов электронных подписей. В новом Типовом законе, который является скромным, однако важным дополнением к Типовому закону ЮНСИТРАЛ об электронной торговле, предлагаются практические стандарты, на основании которых может быть оценена техническая надежность электронных подписей. Кроме того, Типовой закон устанавливает связь между такой технической надежностью и правовой действенностью, возникновения которых можно ожидать в случае использования какой-либо конкретной электронной подписи. Типовой закон является существенным дополнением к Типовому закону ЮНСИТРАЛ об электронной торговле, поскольку в них применяется подход, согласно которому правовая действенность какого-либо конкретного способа электронного подписания может быть определена заранее (или оценена до фактического использования). Таким образом, Типовой закон преследует цель содействия лучшему пониманию концепции электронных подписей и укреплению уверенности в том, что определенные способы электронного подписания могут с надежностью использоваться в операциях, создающих важные правовые последствия. Кроме того, за счет обеспечения надлежащей гибкости при установлении свода базовых норм поведения для различных сторон, которые могут участвовать в использовании электронных подписей (т. е. подписавшие, полагающиеся стороны и третьи стороны – поставщики сертификационных услуг), Типовой закон может оказать помощь в развитии более согласованной коммерческой практики в "киберпространстве".

5. Цели Типового закона, которые заключаются в создании возможностей для использования электронных подписей и в содействии их использованию, а также в обеспечении равного режима для пользователей бумажной документации и

пользователей компьютеризированной информации, имеют важнейшее значение для повышения экономичности и эффективности международной торговли. Включение процедур, предусмотренных в Типовом законе (а также положений Типового закона ЮНСИТРАЛ об электронной торговле), в свое национальное законодательство для урегулирования тех ситуаций, когда стороны решают использовать электронные средства передачи данных, позволит принимающему государству создать надлежащие условия, которые будут нейтральными с точки зрения носителей информации.

B. История вопроса

6. Типовой закон является новым дополнением к серии принятых ЮНСИТРАЛ международных документов, которые либо специально направлены на удовлетворение нужд электронной торговли, либо были подготовлены с учетом потребностей использования современных средств передачи данных. В первую категорию документов, специально предназначенных для электронной торговли, входят Правовое руководство по электронному переводу средств (1987 год), Типовой закон ЮНСИТРАЛ о международных кредитовых переводах (1992 год) и Типовой закон ЮНСИТРАЛ об электронной торговле (1996 и 1998 годы). Ко второй категории относятся все принятые ЮНСИТРАЛ после 1978 года международные конвенции и другие законодательные документы, поскольку все они способствуют сокращению формальных требований и содержат определения понятия "письменная форма", направленные на то, чтобы охватить сообщения в нематериальной форме.

7. Наиболее известным документом ЮНСИТРАЛ в области электронной торговли является Типовой закон ЮНСИТРАЛ об электронной торговле. Его подготовка в начале 90-х годов была обусловлена расширением использования современных средств связи, таких как электронная почта и электронный обмен данными (ЭДИ), для заключения международных торговых сделок. Был сделан вывод о быстром развитии новых технологий, которое получит дополнительный импульс в результате расширения доступности соответствующих технических вспомогательных средств, таких как информационные магистрали и Интернет. В то же время передача юридически значимой информации в форме безбумажных сообщений затрудняется правовыми препятствиями использованию таких сообщений или неопределенностью относительно их юридической силы или действительности. Для облегчения развития применения современных средств связи ЮНСИТРАЛ подготовила Типовой закон об электронной торговле. Цель Типового закона ЮНСИТРАЛ об электронной торговле заключается в том, чтобы предложить вниманию национальных законодателей свод международно приемлемых правил, предусматривающий возможный порядок устранения таких юридических препятствий и создание более надежной правовой базы для так называемой "электронной торговли".

8. Принимая решение о разработке типового законодательства об электронной торговле, ЮНСИТРАЛ исходила из того, что в ряде стран действующее законодательство, регулирующее вопросы передачи сообщений и хранения информации, является недостаточным или устаревшим, поскольку в нем не предусматривается использование электронной торговли. В некоторых случаях действующее законодательство по-прежнему прямо или косвенно ограничивает применение современных средств связи, например предписывая использование "письменных", "подписанных" или "подлинных" документов. В отношении концепции "письменных", "подписанных" и "подлинных" документов в Типовом

законе ЮНСИТРАЛ об электронной торговле используется подход функциональной эквивалентности.

9. В период подготовки Типового закона ЮНСИТРАЛ об электронной торговле некоторые страны приняли специальные положения для регулирования ряда аспектов электронной торговли. Однако законодательства, регулирующего электронную торговлю в целом, не существует. Это может привести к возникновению неопределенности относительно правового характера и действительности информации, представленной не в традиционном бумажном документе, а в какой-либо иной форме. Кроме того, хотя эффективное законодательство и практика необходимы во всех странах, в которых начинают широко использоваться ЭДИ и электронная почта, такая же потребность ощущается и во многих других странах в том, что касается использования таких методов передачи данных, как телефакс и телекс.

10. Типовой закон ЮНСИТРАЛ об электронной торговле может также способствовать устранению неблагоприятных факторов, возникающих в результате того, что несовершенное законодательство на национальном уровне создает препятствия для международной торговли, которая в значительной степени осуществляется с применением современных средств передачи сообщений. Существующие различия в национальных правовых режимах, регулирующих использование таких методов передачи сообщений, а также неопределенность в отношении таких режимов могут по-прежнему в значительной степени приводить к ограничению способности коммерческих предприятий выходить на международные рынки.

11. Кроме того, на международном уровне Типовой закон ЮНСИТРАЛ об электронной торговле в ряде случаев может быть полезным в качестве инструмента для толкования действующих международных конвенций и других международных документов, создающих правовые препятствия использованию электронной торговли, например в результате того, что в них устанавливаются требования об обязательном письменном оформлении некоторых документов или договорных положений. В отношениях между государствами – участниками таких международных документов принятие Типового закона ЮНСИТРАЛ об электронной торговле в качестве правила толкования может представлять собой средство признания использования электронной торговли без необходимости дополнения соответствующего международного документа специальным протоколом.

C. История подготовки Типового закона

12. После принятия Типового закона ЮНСИТРАЛ об электронной торговле Комиссия на своей двадцать девятой сессии (1996 год) постановила включить в свою повестку дня вопросы о подписях в цифровой форме и сертификационных органах. Рабочей группе по электронной торговле было предложено рассмотреть целесообразность и возможность подготовки единообразных правил по этим темам. Было достигнуто согласие в отношении того, что единообразные правила, которые следует подготовить, должны охватывать такие вопросы, как правовая основа, поддерживающая процессы сертификации, включая появляющуюся технологию удостоверения подлинности и сертификации в цифровой форме; применимость процесса сертификации; распределение риска и ответственности пользователей, поставщиков и третьих сторон в контексте использования методов сертификации; конкретные вопросы сертификации через применение регистров; и включение путем ссылки[3].

13. На ее тридцатой сессии (1997 год) Комиссии был представлен доклад Рабочей группы о работе ее тридцать первой сессии (A/CN.9/437). Рабочая группа сообщила Комиссии, что она достигла консенсуса в отношении важного значения и необходимости работы по согласованию норм права в этой области. Хотя она не приняла окончательного решения в отношении формы и содержания такой работы, Рабочая группа пришла к предварительному выводу о том, что подготовка проекта единообразных правил, по крайней мере, по вопросам подписей в цифровой форме и сертификационных органов и, возможно, по связанным с этими вопросам практически осуществима. Рабочая группа напомнила о том, что, наряду с подписями в цифровой форме и сертификационными органами, в рамках будущей работы в области электронной торговли, возможно, также потребуется рассмотреть следующие темы: вопросы технических альтернатив криптографии с использованием публичных ключей; общие вопросы о функциях, выполняемых поставщиками услуг, являющимися третьими сторонами; и заключение контрактов в электронной форме (A/CN.9/437, пункты 156–157). Комиссия одобрила заключения Рабочей группы и поручила ей подготовить единообразные правила по правовым вопросам подписей в цифровой форме и сертификационных органов.

14. В отношении конкретной сферы применения и формы единообразных правил Комиссия в целом согласилась с тем, что на данном начальном этапе процесса принятие решения невозможно. Было сочтено, что, хотя Рабочая группа может надлежащим образом сосредоточить свое внимание на вопросах подписей в цифровой форме с учетом очевидной ведущей роли криптографии с использованием публичных ключей в зарождающейся практике электронной торговли, единообразные правила должны соответствовать нейтральному с точки зрения носителей информации подходу, который взят за основу в Типовом законе ЮНСИТРАЛ об электронной торговле. Таким образом, единообразные правила не должны препятствовать использованию других методов удостоверения подлинности. Кроме того, при решении вопросов криптографии с использованием публичных ключей в единообразных правилах, возможно, необходимо будет учесть различия в уровнях защиты и признать различные правовые последствия и уровни ответственности, соответствующие различным видам услуг, оказываемых в контексте подписей в цифровой форме. Что касается сертификационных органов, то Комиссия, хотя она и признала ценность стандартов, определяемых рыночными отношениями, в целом согласилась с тем, что Рабочая группа может надлежащим образом предусмотреть разработку минимального свода стандартов, которые должны будут строго соблюдаться сертификационными органами, особенно в случае, когда испрашивается трансграничная сертификация[4].

15. Рабочая группа приступила к разработке единообразных правил (которые позднее будут приняты в качестве Типового закона) на основе записки Секретариата (A/CN.9/WG.IV/WP.73) на своей тридцать второй сессии.

16. На ее тридцать первой сессии (1998 год) Комиссии был представлен доклад Рабочей группы о работе ее тридцать второй сессии (A/CN.9/446). Было отмечено, что на своих тридцать первой и тридцать второй сессиях Рабочая группа столкнулась с очевидными трудностями в достижении общего понимания новых правовых вопросов, которые возникают в связи с расширением использования подписей в цифровой и другой электронной форме. Было также отмечено, что еще предстоит достичь консенсуса в отношении того, каким образом эти вопросы могут быть урегулированы в международно приемлемых правовых рамках. Вместе с тем Комиссия в целом сочла, что достигнутый к этому моменту прогресс

свидетельствует о том, что эти единообразные правила постепенно превращаются в документ, который можно будет применять на практике.

17. Комиссия вновь подтвердила принятое на ее тридцатой сессии решение относительно возможности разработки таких единообразных правил и выразила уверенность в том, что на своей тридцать третьей сессии Рабочая группа сможет добиться дальнейшего прогресса на основе пересмотренного проекта, подготовленного Секретариатом (A/CN.9/WG.IV/WP.76). В контексте этого обсуждения Комиссия с удовлетворением отметила, что, по общему признанию, Рабочая группа стала особо важным международным форумом для обмена мнениями по правовым вопросам электронной торговли и для выработки решений по этим вопросам[5].

18. Рабочая группа продолжила рассмотрение единообразных правил на своих тридцать третьей (1998 год) и тридцать четвертой (1999 год) сессиях на основе записок, подготовленных Секретариатом (A/CN.9/WG.IV/WP.76 и A/CN.9/WG.IV/WP.79 и 80). Доклады о работе этих сессий содержатся в документах A/CN.9/454 и 457.

19. На ее тридцать второй сессии (1999 год) Комиссии были представлены доклады Рабочей группы о работе этих двух сессий (A/CN.9/454 и 457). Комиссия выразила признательность Рабочей группе за ее усилия по подготовке этих единообразных правил. Хотя было выражено общее согласие с тем, что на этих сессиях был достигнут значительный прогресс в понимании правовых вопросов, связанных с использованием электронных подписей, было также сочтено, что Рабочая группа столкнулась с трудностями в достижении консенсуса в отношении законодательного принципа, на котором должны основываться эти единообразные правила.

20. Было высказано мнение о том, что подход, применяемый в настоящее время Рабочей группой, недостаточно полно отражает потребность деловых кругов в гибком использовании электронных подписей и других методов удостоверения подлинности. В единообразных правилах, как они рассматриваются в настоящее время Рабочей группой, уделяется чрезмерно большое внимание методам цифровых подписей и – в сфере применения таких подписей – специальной практике сертификации третьей стороной. Соответственно, было предложено либо ограничить работу по вопросам электронных подписей, осуществляемую Рабочей группой, правовыми вопросами трансграничной сертификации, либо отложить ее до тех пор, пока не упрочится соответствующая рыночная практика. В связи с этим было также высказано мнение о том, что применительно к целям международной торговли большая часть правовых вопросов, возникающих в связи с использованием электронных подписей, уже была решена в Типовом законе ЮНСИТРАЛ об электронной торговле (см. ниже, пункт 28). Хотя некоторые виды использования электронных подписей, возможно, требуют урегулирования за рамками торгового права, Рабочей группе не следует заниматься какими-либо вопросами, связанными с такого рода регулированием.

21. Преобладающее мнение заключалось в том, что Рабочей группе следует выполнять свою задачу, исходя из своего первоначального мандата. Что касается необходимости в единообразных правилах об электронных подписях, то, как было разъяснено, правительственные и законодательные органы многих стран, занимающиеся подготовкой законодательства по вопросам электронных подписей,

включая создание инфраструктур публичных ключей (ИПК), или другими проектами по тесно связанным с этой областью вопросам (см. A/CN.9/457, пункт 16), ожидают определенных рекомендаций от ЮНСИТРАЛ. Что касается принятого Рабочей группой решения сосредоточить свое внимание на вопросах использования ИПК и терминологии ИПК, то было вновь указано, что комплекс взаимоотношений между тремя отдельными категориями сторон (т. е. обладателями ключей, сертификационными органами и полагающимися сторонами) отвечает одной возможной модели ИПК, но что можно предположить и существование других моделей, например в тех случаях, когда независимый сертификационный орган не является участником таких отношений. Одно из основных преимуществ, которое можно извлечь из сосредоточения внимания на вопросах ИПК, состоит в том, что это позволит облегчить составление единообразных правил за счет ссылок на три функции (или роли) применительно к парам ключей, а именно на функцию выдачи ключа (или функцию абонирования), сертификационную функцию и полагающуюся функцию. Было достигнуто общее согласие с тем, что эти три функции являются общими для всех моделей ИПК. Было также принято решение о том, что вопросы, связанные с этими тремя функциями, должны регулироваться независимо от того, выполняют ли их на практике три отдельных субъекта или же одно и то же лицо выполняет две из этих функций (например, в случаях, когда сертификационный орган также является полагающейся стороной). Кроме того, согласно получившему широкую поддержку мнению, уделение первостепенного внимания функциям, типичным для ИПК, а не какой-либо конкретной модели, может на более позднем этапе облегчить разработку такой нормы, которая являлась бы полностью нейтральной с точки зрения носителя информации (там же, пункт 68).

22. После обсуждения Комиссия вновь подтвердила принятые ею ранее решения относительно возможности подготовки таких единообразных правил и выразила уверенность в том, что Рабочая группа сможет добиться дальнейшего прогресса на своих будущих сессиях[6].

23. Рабочая группа продолжила свою работу на своих тридцать пятой (сентябрь 1999 года) и тридцать шестой (февраль 2000 года) сессиях на основе записок, подготовленных Секретариатом (A/CN.9/WG.IV/WP.82 и 84). На ее тридцать третьей сессии (2000 год) Комиссии были представлены доклады рабочей группы о работе этих двух сессий (A/CN.9/465 и 467). Было отмечено, что Рабочая группа на ее тридцать шестой сессии приняла текст проектов статей 1 и 3–12 единообразных правил. Было указано, что некоторые вопросы по-прежнему нуждаются в разъяснении, поскольку Рабочая группа приняла решение исключить из проекта единообразных правил понятие электронной подписи с высокой степенью защиты. Было сделано замечание о том, что в зависимости от решений, которые Рабочая группа примет в отношении проектов статей 2 и 13, остальные проекты положений, возможно, придется еще раз рассмотреть во избежание возникновения ситуации, когда установленный в единообразных правилах стандарт будет одинаково применяться и к электронным подписям, обеспечивающим высокий уровень надежности, и к недорогостоящим сертификатам, которые могут использоваться в контексте электронных сообщений, не преследующих цели создания существенных правовых последствий.

24. После обсуждения Комиссия выразила признательность Рабочей группе за ее усилия и прогресс, достигнутый в разработке этих единообразных правил. К Рабочей группе был обращен настоятельный призыв завершить работу над

единообразными правилами на ее тридцать седьмой сессии и рассмотреть проект руководства по принятию, который подготовит Секретариат[7].

25. Рабочая группа завершила разработку этих единообразных правил на своей тридцать седьмой сессии (сентябрь 2000 года). Доклад о работе этой сессии содержится в документе A/CN.9/483. Рабочая группа также рассмотрела проект руководства по принятию. Секретариату было предложено подготовить пересмотренный вариант проекта руководства с учетом решений, принятых Рабочей группой, на основе различных мнений, предложений и замечаний, которые были высказаны в ходе текущей сессии. Из-за нехватки времени Рабочая группа не завершила рассмотрение проекта руководства по принятию. Было решено выделить определенное время для завершения рассмотрения этого пункта повестки дня на тридцать восьмой сессии Рабочей группы. Отмечалось, что единообразные правила (в настоящее время в форме проекта типового закона ЮНСИТРАЛ об электронных подписях), наряду с проектом руководства по принятию, будут представлены Комиссии для рассмотрения и принятия на ее тридцать четвертой сессии (2001 год). *[Примечание Секретариата: данный раздел, посвященный истории подготовки Типового закона, будет окончательно доработан и, возможно, изложен в более сжатом виде после завершения рассмотрения и принятия Типового закона Комиссией.]*

II. ТИПОВОЙ ЗАКОН В КАЧЕСТВЕ ИНСТРУМЕНТА УНИФИКАЦИИ ЗАКОНОДАТЕЛЬСТВА

26. Как и Типовой закон ЮНСИТРАЛ об электронной торговле, новый Типовой закон представляет собой законодательный текст, рекомендуемый государствам для включения в их национальное законодательство. В отличие от международной конвенции типовые законодательные положения не требуют, чтобы принимающее их государство уведомляло об этом Организацию Объединенных Наций или другие государства, которые также могли их принять. В то же время государства настоятельно поощряются к тому, чтобы проинформировать Секретариат ЮНСИТРАЛ о принятии нового Типового закона (или любого другого типового закона, являющегося результатом работы ЮНСИТРАЛ).

27. При включении текста типовых законодательных положений в свою правовую систему государство может изменить или исключить некоторые такие положения. В случае конвенции возможность внесения изменений в единообразный текст государствами-участниками (которые обычно называются "оговорками") является намного более ограниченной; в частности, в конвенциях в области торгового права оговорки, как правило, либо полностью запрещаются, либо допускается внесение только очень немногих, конкретно указанных оговорок. Гибкость, присущая типовым законодательным положениям, является особенно желательной в тех случаях, когда вероятность того, что государство пожелает внести различные изменения в единообразный текст, прежде чем оно будет готово принять такой текст в качестве своего национального закона, является высокой. Внесения некоторых изменений можно в особенности ожидать в тех случаях, когда единообразный текст непосредственным образом затрагивает национальную судебную или процессуальную систему. Это, однако, также означает, что степень унификации, достигнутая с помощью типового законодательства, и определенность относительно правового регулирования будут, по всей вероятности, ниже, чем в случае принятия конвенции. Однако этот относительный недостаток типового законодательства может быть уравновешен тем фактом, что число государств, принимающих типовые законодательные положения, будет, по всей вероятности,

выше, чем число государств, присоединяющихся к конвенции. В целях достижения удовлетворительной степени унификации и определенности рекомендуется, чтобы государства вносили как можно меньше изменений при включении нового Типового закона в свои правовые системы. В целом при принятии нового Типового закона (или Типового закона ЮНСИТРАЛ об электронной торговле) рекомендуется в максимально возможной степени придерживаться единообразного текста, с тем чтобы максимально повысить прозрачность и понятность национального законодательства для его иностранных пользователей.

28. Следует отметить, что, по мнению некоторых стран, правовые вопросы, касающиеся использования электронных подписей, уже решены в Типовом законе ЮНСИТРАЛ об электронной торговле, и они не планируют принимать дополнительные правила об электронных подписях до тех пор, пока рыночная практика в этой новой области не получит более широкого распространения. Однако государства, принимающие новый Типовой закон наряду с Типовым законом ЮНСИТРАЛ об электронной торговле, могут рассчитывать на получение дополнительных выгод. Тем странам, в которых правительственные и законодательные органы находятся в процессе подготовки законодательства по вопросам электронных подписей, включая создание инфраструктур публичных ключей (ИПК), Типовой закон предлагает ориентиры международного документа, который разрабатывался с учетом вопросов и терминологии ИПК. Для всех стран Типовой закон предлагает свод основных правил, которые могут применяться помимо модели ИПК, поскольку они предусматривают взаимодействие трех отдельных функций, которые могут быть сопряжены с любым типом электронной подписи (т. е. функции создания электронной подписи, сертификационной функции и полагающейся функции). Вопросы, связанные с этими тремя функциями, должны регулироваться независимо от того, выполняют ли их на практике три отдельных субъекта или же одно и то же лицо выполняет две из этих функций (например, в случаях, когда сертификационный орган также является полагающейся стороной). Таким образом, Типовой закон обеспечивает общие основы для систем ИПК, полагаясь на независимые сертификационные органы и системы электронных подписей, когда ни одна такая независимая третья сторона не участвует в процессе использования электронной подписи. Во всех случаях новый Типовой закон обеспечивает дополнительную определенность в отношении правовой действенности электронных подписей, не ограничивая при этом применение гибкого критерия, закрепленного в статье 7 Типового закона ЮНСИТРАЛ об электронной торговле (см. ниже, пункты 67 и 70–75).

III. ОБЩИЕ СООБРАЖЕНИЯ ОТНОСИТЕЛЬНО ЭЛЕКТРОННЫХ ПОДПИСЕЙ[8]

A. Функции подписей

29. Статья 7 Типового закона ЮНСИТРАЛ об электронной торговле основывается на признании функций подписи в условиях использования бумажных документов. В ходе подготовки Типового закона ЮНСИТРАЛ об электронной торговле Рабочая группа обсудила следующие функции, традиционно выполняемые собственноручными подписями: идентификация лица; обеспечение определенности в отношении личного участия данного лица в акте подписания и подтверждение согласия данного лица с содержанием документа. Было отмечено, что, помимо этого, подпись может выполнять целый ряд функций в зависимости от характера подписанного документа. Например, подпись может подтверждать намерение стороны быть связанной содержанием подписанного контракта; намерение лица

одобрить авторство какого-либо текста (проявляя тем самым осведомленность о том, что акт подписания может повлечь за собой правовые последствия); намерение лица согласиться с содержанием документа, написанного кем-то другим; тот факт, что какое-либо лицо находилось в данном месте, и время, когда оно там находилось. Взаимосвязь между новым Типовым законом и статьей 7 Типового закона ЮНСИТРАЛ об электронной торговле более подробно рассматривается ниже, в пунктах 67 и 70–75 настоящего Руководства.

30. В условиях электронного обмена данными подлинник сообщения неотличим от копии, не имеет собственноручной подписи и не является бумажным документом. Возможность мошенничества велика из-за легкости трудно поддающегося обнаружению перехвата и изменения информации в электронной форме и скорости обработки многочисленных операций. Цель различных методов, которыми в настоящее время можно воспользоваться на рынке или которые еще находятся в стадии разработки, заключается в том, чтобы предложить технические средства, с помощью которых часть или все функции, характерные для собственноручных подписей, могли бы выполняться в условиях электронного обмена данными. Такие методы можно в широком смысле назвать "электронными подписями".

B. Цифровые подписи и другие электронные подписи

31. Обсуждая вопросы о целесообразности и практической возможности подготовки нового Типового закона и об определении сферы применения единообразных правил об электронных подписях, ЮНСИТРАЛ изучила различные электронные методы подписания, которые используются или разрабатываются в настоящее время. Общая цель этих методов состоит в том, чтобы обеспечить функциональные эквиваленты: 1) собственноручных подписей и 2) других механизмов удостоверения подлинности, используемых в среде бумажных документов (например, печатей или штампов). Эти же методы могут выполнять дополнительные функции в сфере электронной торговли, которые проистекают из функций подписи, однако не имеют аналогов в сфере обращения бумажных документов.

32. Как это уже указывалось выше (см. пункты 21 и 28), правительственные и законодательные органы многих стран, занимающиеся подготовкой законодательства по вопросам электронных подписей, включая создание инфраструктур публичных ключей (ИПК), или другими проектами по тесно связанным с этой областью вопросам (см. документ A/CN.9/457, пункт 16), ожидают определенных рекомендаций от ЮНСИТРАЛ. Что касается принятого ЮНСИТРАЛ решения сосредоточить свое внимание на вопросах использования ИПК и терминологии ИПК, то было вновь указано, что комплекс взаимоотношений между тремя отдельными категориями сторон (т. е. подписавшими, поставщиками сертификационных услуг и полагающимися сторонами) отвечает одной возможной модели ИПК, но что уже широко используются на рынке и другие модели (например, в тех случаях, когда независимый сертификационный орган не является участником таких отношений). Одно из основных преимуществ, которое можно извлечь из сосредоточения внимания на вопросах ИПК, состоит в том, что это позволит облегчить составление Типового закона за счет ссылок на три функции (или роли) применительно к электронным подписям, а именно на функцию подписания (или функцию абонирования), сертификационную функцию и полагающуюся функцию. Эти три функции являются общими для всех моделей ИПК, и вопросы, связанные с этими тремя функциями, должны регулироваться

независимо от того, выполняют ли их на практике три отдельных субъекта или же одно и то же лицо выполняет две из этих функций (например, в случаях, когда поставщик сертификационных услуг также является полагающейся стороной). Уделение первостепенного внимания функциям, типичным для ИПК, а не какой-либо конкретной модели, может также облегчить разработку такой нормы, которая являлась бы полностью нейтральной с точки зрения носителя информации, в той мере, в которой аналогичные функции выполняются с помощью электронной технологии подписания, не связанной с ИПК.

1. Электронные подписи, проставляемые с помощью иных методов, чем криптография с использованием публичных ключей

33. Следует напомнить, что наряду с "цифровыми подписями", основанными на криптографии с использованием публичных ключей, существуют различные другие средства, также охватываемые широкой концепцией механизмов "электронной подписи", которые могут использоваться в настоящее время или рассматриваться для использования в будущем с целью выполнения одной или нескольких вышеупомянутых функций собственноручных подписей. Например, некоторые методы предполагают удостоверение подлинности с помощью биометрического устройства, основанного на собственноручных подписях. При использовании такого устройства подписывающее лицо проставляет свою подпись собственноручно с помощью специальной ручки либо на экране компьютера, либо на планшете. Такая собственноручная подпись затем анализируется компьютером и хранится в виде набора числовых величин, который может быть поставлен под сообщением данных и воспроизведен получателем в целях удостоверения подлинности. Такая система удостоверения подлинности предполагает, что образцы собственноручной подписи были ранее проанализированы биометрическим устройством и хранятся в нем. К числу других технологий относится использование персональных идентификационных номеров (ПИН), собственноручных подписей в цифровой форме и других методов, таких как нажатие на клавишу "ОК".

34. ЮНСИТРАЛ стремилась выработать такие единообразные законодательные положения, какие способствовали бы использованию как цифровых подписей, так и электронных подписей в других формах. С этой целью ЮНСИТРАЛ попыталась подойти к урегулированию правовых вопросов, связанных с электронными подписями, на таком уровне, который был бы промежуточным между высоким уровнем общей применимости Типового закона ЮНСИТРАЛ об электронной торговле и более специальными правилами, которые могут потребоваться для урегулирования вопросов, связанных с конкретными методами подписания. В любом случае, согласно принципу нейтральности Типового закона ЮНСИТРАЛ об электронной торговле по отношению к носителям данных, новый Типовой закон не должен толковаться как препятствующий применению любых других методов электронного подписания, которые уже существуют или могут появиться в будущем.

2. Цифровые подписи, проставляемые с помощью криптографии с использованием публичных ключей[9]

35. С учетом расширения использования цифровых методов подписания в ряде стран лицам, занимающимся подготовкой законодательства об электронных подписях, окажется, возможно, полезной нижеследующая вводная информация.

a) Технические понятия и терминология

i) Криптография

36. Цифровые подписи создаются и проверяются путем использования криптографии, являющейся отраслью прикладной математики, позволяющей преобразовывать сообщения в кажущуюся непонятной форму и обратно в подлинную форму. При проставлении цифровых подписей применяется метод, известный как "криптография с использованием публичного ключа", которая зачастую основывается на использовании алгоритмических функций для создания двух разных, но математически соотносящихся "ключей" (т. е. больших чисел, составленных с помощью ряда математических формул в применении к простым числам). Один такой ключ используется для создания цифровой подписи или преобразования данных в кажущуюся непонятной форму, а другой ключ – для удостоверения подлинности цифровой подписи или возвращения сообщения в его подлинную форму. Компьютерное оборудование и программное обеспечение, использующие два таких ключа, зачастую вместе называются "криптосистемами" или, более конкретно, "асимметричными криптосистемами" в том случае, если они полагаются на использование асимметричных алгоритмов.

37. Хотя применение криптографии является одной из основных особенностей цифровых подписей, тот простой факт, что цифровая подпись используется для удостоверения подлинности сообщения, содержащего информацию в цифровой форме, не следует путать с более широким применением криптографии в целях обеспечения конфиденциальности. Кодирование является методом, используемым для кодирования электронного сообщения, с тем чтобы только его составитель и адресат были в состоянии его прочесть. В ряде стран применение криптографии в целях обеспечения конфиденциальности ограничивается законом по соображениям публичного порядка, которые могут включать соображения национальной обороны. Однако применение криптографии в целях удостоверения подлинности путем создания цифровой подписи не обязательно подразумевает использование кодирования для обеспечения конфиденциальности в процессе передачи сообщений, поскольку закодированная цифровая подпись может быть всего лишь добавлена к незакодированному сообщению.

ii) Публичные и частные ключи

38. Взаимно дополняющие ключи, используемые для проставления цифровой подписи, называются "частным ключом", который используется подписывающим лицом для создания цифровой подписи, и "публичным ключом", который обычно более широко известен и используется полагающейся стороной для проверки подлинности цифровой подписи. Предполагается, что пользователь частного ключа держит его в секрете. Следует отметить, что отдельному пользователю не нужно знать частный ключ. Такой частный ключ может быть указан на интеллектуальной карточке или быть доступным через персональный идентификационный номер или же, в идеале, через биометрическое идентификационное устройство, например через определитель отпечатков пальцев. Если многим лицам необходимо проверить подлинность цифровых подписей конкретного лица, то публичный ключ должен быть сообщен всем этим людям или распространен среди них, например путем включения в базу данных, работающую в диалоговом режиме, или в любой другой каталог общего пользования, где этот ключ легко можно найти. Несмотря на то что ключи одной пары математически соотносятся, если разработка и реализация

асимметрической криптосистемы надежна, то практически невозможно определить частный ключ, зная публичный ключ. Наиболее общие алгоритмы для кодирования посредством использования публичных и частных ключей основываются на важной особенности больших простых чисел: после их перемножения для получения нового числа фактически невозможно определить, какие два простых числа создали новое, большее число[10]. Таким образом, хотя многие могут знать публичный ключ какого-либо подписавшегося лица и использовать этот ключ для проверки подлинности его подписей, они не могут установить его частный ключ и использовать этот ключ для подделки цифровых подписей.

39. Вместе с тем следует отметить, что понятие криптографии с использованием публичного ключа не обязательно подразумевает использование вышеупомянутых алгоритмов, основывающихся на простых числах. В настоящее время применяются или разрабатываются другие математические методы, такие как криптосистемы, использующие эллиптические кривые, которые часто считаются обеспечивающими высокую степень неприкосновенности данных путем использования ключей значительно меньшей длины.

iii) Функция хеширования

40. В дополнение к подготовке пар ключей как для создания, так и для проверки подлинности цифровой подписи используется еще один основополагающий процесс, обычно именуемый "функцией хеширования". Функция хеширования представляет собой математический процесс, основанный на использовании алгоритма, который создает цифровое обозначение или сжатую форму сообщения, которая часто называется "резюме сообщения" или "отпечаток" сообщения, в форме "величины хеширования" или "результата хеширования" стандартной длины, которая обычно намного меньше, чем само сообщение, но, тем не менее, по существу относится только к нему. Любое изменение в сообщении неизбежно дает иной результат хеширования, когда используется та же функция хеширования. В случае использования надежной функции хеширования, иногда именуемой "функцией одностороннего хеширования", фактически невозможно получить подлинное сообщение на основании осведомленности о его величине хеширования. Поэтому функции хеширования дают возможность того, чтобы программное обеспечение, используемое для создания цифровых подписей, было задействовано на основе меньшего и предсказуемого объема данных и все же предоставляло надежное доказательство его связи с содержанием подлинного сообщения, обеспечивая тем самым эффективную гарантию того, что в сообщение не вносились изменения после его подписания в цифровой форме.

iv) Цифровая подпись

41. Чтобы подписать какой-либо документ или любой другой элемент данных, подписывающее лицо сначала определяет точные границы того, что предстоит подписать. Затем путем использования функции хеширования подписывающее лицо с помощью программного обеспечения исчисляет результат хеширования, относящийся (для всех практических целей) только к подписываемой информации. Далее подписывающее лицо с помощью программного обеспечения преобразует результат хеширования в цифровую подпись, используя свой частный ключ. Таким образом, созданная цифровая подпись относится только к подписываемой информации и только к частному ключу, использовавшемуся для ее создания.

42. Как правило, цифровая подпись (результат хеширования сообщения, подписанный в цифровой форме) прилагается к сообщению и хранится или передается с этим сообщением. Однако она может также передаваться или храниться в качестве отдельного элемента данных до тех пор, пока она сохраняет надежную связь со своим сообщением. Поскольку цифровая подпись относится только к своему сообщению, она является бесполезной, если лишена постоянной связи со своим сообщением.

v) Проверка подлинности цифровой подписи

43. Проверка подлинности цифровой подписи представляет собой процесс проверки такой подписи путем обращения к подлинному сообщению и какому-либо публичному ключу и тем самым установления того, была ли эта цифровая подпись создана для того же сообщения с использованием частного ключа, соответствующего упоминаемому публичному ключу. Проверка цифровой подписи производится путем исчисления нового результата хеширования подлинного сообщения с помощью той же функции хеширования, которая использовалась для создания цифровой подписи. Затем, используя публичный ключ и новый результат хеширования, проверяющий устанавливает, была ли цифровая подпись создана с использованием соответствующего частного ключа и совпадает ли вновь исчисленный результат хеширования с первоначальным результатом хеширования, который был преобразован в цифровую подпись в процессе подписания.

44. Используемое для такой проверки программное обеспечение подтвердит цифровую подпись как "проверенную", если: 1) для подписания сообщения в цифровой форме использовался частный ключ подписавшего лица, что, как известно, будет иметь место в том случае, если для проверки этой подписи использовался публичный ключ подписавшего лица, поскольку публичный ключ подписавшего лица позволяет проверить только ту цифровую подпись, которая была создана с помощью его частного ключа; и 2) в сообщение не были внесены изменения, что, как известно, будет иметь место только в том случае, если результат хеширования, исчисленный проверяющим, является идентичным результату хеширования, полученному из цифровой подписи в процессе проверки.

b) Инфраструктура публичных ключей (ИПК) и поставщик сертификационных услуг

45. Чтобы проверить цифровую подпись, проверяющий должен иметь доступ к публичному ключу подписавшего лица и быть уверенным в том, что он соответствует частному ключу подписавшего лица. Однако пара публичного и частного ключей не имеет внутренне присущей ей связи с каким-либо лицом; это всего лишь пара чисел. Необходим дополнительный механизм для того, чтобы с достоверностью установить наличие связи какого-либо конкретного физического или юридического лица с данной парой ключей. Чтобы кодирование с помощью публичного ключа служило своим предполагаемым целям, должен быть предусмотрен способ направления ключей целому ряду лиц, многие из которых не известны отправителю и между которыми не установились доверительные отношения. Поэтому участвующие стороны должны испытывать большое доверие к выдаваемым публичным и частным ключам.

46. Требуемая степень доверия может наличествовать между сторонами, которые полностью доверяют друг другу, имели дело друг с другом в течение

определенного периода времени, общаются через закрытые системы, действуют в пределах замкнутой группы или которые могут регулировать свои сделки договорным путем, например на основе соглашения о торговом партнерстве. В случае сделки, затрагивающей только две стороны, каждая сторона может просто сообщить (через относительно надежный канал, такой как курьер или защищенная телефонная линия) публичный ключ из пары ключей, которую каждая сторона будет использовать. Однако той же степени доверия может и не возникнуть, если стороны редко ведут дела друг с другом, общаются через открытые системы (например, всемирную сеть системы Интернет), не входят в какую-либо замкнутую группу или не заключили соглашений о торговом партнерстве либо не располагают другими нормами права, регулирующими их взаимоотношения.

47. Кроме того, поскольку кодирование с помощью публичного ключа представляет собой сложный математический процесс, все пользователи должны быть уверены в профессионализме и познаниях сторон, выдающих публичные и частные ключи, и в принимаемых ими мерах по обеспечению неприкосновенности соответствующих данных[11].

48. Лицо, намеревающееся использовать цифровую подпись, может сделать публичное заявление о том, что подписи, проверяемые с помощью какого-либо конкретного публичного ключа, следует рассматривать как исходящие от этого лица. Однако другие стороны могут и не пожелать признать это заявление, особенно при отсутствии заранее достигнутой договоренности, устанавливающей правовую силу такого опубликованного заявления со всей определенностью. Сторона, полагающаяся на такое неподтвержденное опубликованное заявление в открытой системе, рискует по неосторожности довериться мошеннику или столкнется с необходимостью уличить в ложном отказе от цифровой подписи (вопрос, который часто упоминается в контексте "неотказа" от цифровых подписей), если сделка окажется неблагоприятной для подразумеваемого подписавшего лица.

49. Решение этих проблем заключается в том, чтобы заручиться готовностью одной или нескольких доверенных третьих сторон установить связь между идентифицированным подписавшим лицом или его именем и конкретным публичным ключом. Такую доверенную третью сторону обычно называют "сертификационным органом" или "поставщиком сертификационных услуг" в большинстве технических стандартов и руководящих принципов (в Типовом законе было решено использовать термин "поставщик сертификационных услуг"). В ряде стран создана иерархическая структура таких сертификационных органов, которую часто называют инфраструктурой публичных ключей (ИПК).

i) Инфраструктура публичных ключей (ИПК)

50. Создание инфраструктуры публичных ключей (ИПК) является способом обеспечить уверенность в том, что: 1) публичный ключ пользователя не был изменен и действительно соответствует частному ключу этого пользователя; 2) используемые методы кодирования являются надежными; 3) учреждениям, которые выдают криптографические ключи, можно доверить хранение или воссоздание публичных и частных ключей, которые могут использоваться для кодирования в целях обеспечения конфиденциальности, если применение такого метода санкционировано; 4) различные системы кодирования могут взаимодействовать. Для обеспечения вышеупомянутой уверенности ИПК может предлагать ряд услуг, включая следующие: 1) управление криптографическими

ключами, используемыми для цифровых подписей; 2) удостоверение того, что публичный ключ соответствует частному ключу; 3) предоставление ключей конечным пользователям; 4) решение вопроса о том, какие пользователи будут иметь привилегии в системе, и определение таких привилегий; 5) опубликование достоверного справочника публичных ключей или сертификатов; 6) управление личными опознавательными средствами (например, интеллектуальными карточками), которые могут идентифицировать пользователя с помощью уникальной личной идентификационной информации или могут подготавливать и хранить частные ключи какого-либо лица; 7) проверку правильности идентификации конечных пользователей и предоставление им услуг; 8) предоставление услуг в отношении неотказа; 9) предоставление услуг по фиксации времени передачи сообщения; 10) управление кодовыми ключами, используемыми для кодирования в целях обеспечения конфиденциальности, если применение такого метода санкционировано.

51. Инфраструктура публичных ключей (ИПК) зачастую основывается на иерархии органов различного уровня. Например, модели, рассматриваемые в некоторых странах с целью возможного создания ИПК, включают ссылки на следующие уровни: 1) единственный "базовый орган", который сертифицирует технологию и практику всех сторон, уполномоченных выдавать пары криптографических ключей или сертификаты в связи с использованием таких пар ключей, и осуществляет регистрацию подчиненных сертификационных органов[12]; 2) различные сертификационные органы, занимающие более низкую ступень по сравнению с "базовым" органом, которые удостоверяют, что публичный ключ пользователя действительно соответствует частному ключу этого пользователя (т. е. не был изменен); и 3) различные местные регистрационные органы, занимающие более низкую ступень по сравнению с сертификационными органами и получающие от пользователей просьбы о предоставлении пар криптографических ключей или сертификатов в связи с использованием таких пар ключей, требующие доказательства идентификации и проверяющие идентификационную информацию потенциальных пользователей. В некоторых странах предусматривается, что государственные нотариусы могут действовать в качестве местных регистрационных органов или оказывать им поддержку.

52. Вопросы ИПК, как представляется, нелегко согласовать на международном уровне. Создание ИПК может быть сопряжено с различными техническими вопросами, а также вопросами публичного порядка, которые на нынешнем этапе, возможно, лучше оставить на усмотрение каждого отдельного государства[13]. В связи с этим может потребоваться, чтобы каждое государство, рассматривающее возможность создания ИПК, принимало решения, например, в отношении: 1) формы и числа уровней органов, которые должны быть объединены в ИПК; 2) вопроса о том, следует ли разрешать только определенным органам, относящимся к ИПК, выдавать пары криптографических ключей или же такие пары ключей могут создаваться самими пользователями; 3) вопроса о том, должны ли сертификационные органы, удостоверяющие действительность пар криптографических ключей, быть публичными учреждениями или же частные учреждения также могут действовать в качестве сертификационных органов; 4) вопроса о том, должен ли процесс выдачи какому-либо учреждению разрешения действовать в качестве сертификационного органа принимать форму прямого разрешения или "лицензирования" со стороны государства или же следует использовать другие методы контроля за качеством работы сертификационных органов, если им будет разрешено функционировать в отсутствие специального разрешения; 5) степени, в

которой следует разрешить использование криптографии в целях обеспечения конфиденциальности; и 6) вопроса о том, должны ли правительственные органы сохранять доступ к закодированной информации через механизм "ключа на хранении у третьей стороны" или как-либо иначе. Эти вопросы в Типовом законе не рассматриваются.

ii) Поставщик сертификационных услуг

53. Чтобы установить связь между парой ключей и будущим подписывающим лицом, поставщик сертификационных услуг (или сертификационный орган) выдает сертификат, т. е. электронную запись, в которой указываются публичный ключ и имя абонента сертификата в качестве "субъекта" сертификата и может подтверждаться, что будущее подписывающее лицо, указанное в сертификате, является держателем соответствующего частного ключа. Основная функция сертификата заключается в увязывании публичного ключа с конкретным держателем. "Получатель" сертификата, желающий положиться на цифровую подпись, созданную держателем, который поименован в сертификате, может использовать указанный в сертификате публичный ключ для проверки подлинности того, что данная цифровая подпись была создана с помощью соответствующего частного ключа. Если такая проверка дает положительный результат, то обеспечивается гарантия того, что цифровая подпись была создана поименованным в сертификате держателем публичного ключа и что соответствующее сообщение не было изменено после его подписания в цифровой форме.

54. Чтобы удостоверить подлинность сертификата с точки зрения как его содержания, так и его источника, сертификационный орган подписывает его в цифровой форме. Подлинность цифровой подписи на сертификате выдавшего его сертификационного органа может быть проверена путем использования публичного ключа сертификационного органа, указанного в другом сертификате другим сертификационным органом (который может находиться на более высоком уровне в иерархии, но не обязательно), а подлинность этого другого сертификата может быть, в свою очередь, удостоверена публичным ключом, указанным в еще одном сертификате, и т. д. до тех пор, пока лицо, полагающееся на цифровую подпись, не получит должной гарантии ее истинности. В каждом случае выдающий сертификат сертификационный орган должен подписать в цифровой форме свой собственный сертификат в течение срока действия другого сертификата, использовавшегося для проверки подлинности цифровой подписи сертификационного органа.

55. Цифровая подпись, соответствующая сообщению, независимо от того, была ли она создана держателем пары ключей для удостоверения подлинности сообщения или же сертификационным органом для удостоверения подлинности своего сертификата, должна быть, как правило, надежно датирована, с тем чтобы проверяющий мог точно установить, была ли цифровая подпись создана в течение "срока действия", указанного в сертификате, что является условием проверки подлинности цифровой подписи.

56. Чтобы обеспечить доступность публичного ключа и данных о его соответствии конкретному держателю для использования при проверке подлинности, сертификат может быть опубликован в соответствующем реестре или предоставляться для ознакомления каким-либо иным образом. Обычно реестры представляют собой работающие в оперативном режиме базы данных по

сертификатам и другой информации, которая может быть получена и использована для проверки подлинности цифровых подписей.

57. Уже выданный сертификат может оказаться ненадежным, например в таких ситуациях, когда держатель представил неправильные идентификационные данные сертификационному органу. В других обстоятельствах сертификат может быть достаточно надежным при выдаче, но стать ненадежным впоследствии. Если частный ключ "скомпрометирован", например в результате потери контроля над ним его держателем, то сертификат может лишиться достоверности или стать ненадежным, и сертификационный орган (по просьбе держателя или даже без его согласия, в зависимости от обстоятельств) может приостановить действие (временно прервать срок действия) такого сертификата или аннулировать (навсегда признать недействительность) его. Сразу же после приостановления действия или аннулирования сертификата сертификационный орган, как правило, должен опубликовать уведомление об аннулировании или приостановлении действия сертификата или уведомить об этом лиц, которые делали соответствующий запрос или которые, как известно, получали цифровую подпись, подлинность которой может быть проверена путем ссылки на ненадежный сертификат.

58. Функционирование сертификационных органов может обеспечиваться правительственными учреждениями или поставщиками услуг из частного сектора. В ряде стран по соображениям публичного порядка предусматривается, что только правительственные учреждения могут быть уполномочены действовать в качестве сертификационных органов. В других странах считается, что услуги по сертификации должны быть открытыми для конкуренции со стороны частного сектора. Независимо от того, обеспечивается ли функционирование сертификационных органов правительственными учреждениями или поставщиками услуг из частного сектора и требуется ли, чтобы сертификационные органы получили лицензию для осуществления своей деятельности, обычно в рамках ИПК действуют не один, а несколько сертификационных органов. Особую сложность представляют собой взаимоотношения между различными сертификационными органами. Сертификационные органы в рамках ИПК могут создаваться в виде иерархической структуры, в которой некоторые сертификационные органы только сертифицируют другие сертификационные органы, которые предоставляют услуги непосредственно пользователям. В такой структуре одни сертификационные органы подчинены другим сертификационным органам. В других возможных структурах одни сертификационные органы могут действовать на равноправной основе с другими сертификационными органами. В любой крупной ИПК, по всей вероятности, будут и подчиненные, и вышестоящие сертификационные органы. В любом случае в отсутствие международной ИПК может возникнуть целый ряд вопросов в отношении признания сертификатов сертификационными органами в зарубежных странах. Признание иностранных сертификатов часто обеспечивается с помощью метода "перекрестной сертификации". В таком случае необходимо, чтобы по существу равнозначные сертификационные органы (или сертификационные органы, готовые взять на себя определенные риски в связи с сертификатами, выданными другими сертификационными органами) признавали предоставляемые ими услуги, с тем чтобы их соответствующие пользователи могли сноситься друг с другом более эффективно и с большей уверенностью в надежности выдаваемых сертификатов.

59. В связи с перекрестной сертификацией или "увязыванием" сертификатов, когда принимается целый ряд мер по обеспечению многоуровневой защиты неприкосновенности данных, могут возникать правовые проблемы. Примеры таких

проблем могут включать определение того, чье неправильное поведение привело к убыткам и на чьи заверения полагался пользователь. Следует отметить, что правовые нормы, рассматриваемые для принятия в некоторых странах, предусматривают, что если пользователи осведомлены об уровне обеспечения неприкосновенности данных и соответствующих мерах и если не имелось небрежности со стороны сертификационных органов, то ответственности не возникает.

60. На сертификационный орган или базовый орган может быть возложена обязанность обеспечивать, чтобы его требования в отношении надлежащих действий выполнялись на постоянной основе. Хотя выбор сертификационных органов может основываться на ряде факторов, включая надежность используемого публичного ключа и идентификационных данных пользователя, высокая репутация любого сертификационного органа может также зависеть от его способности обеспечить соблюдение стандартов, касающихся выдачи сертификатов, и надежности проводимой им оценки данных, получаемых от пользователей, которые запрашивают сертификаты. Особое значение имеет режим ответственности, применяемый к любому сертификационному органу в связи с выполнением им требований в отношении надлежащих действий и обеспечения неприкосновенности данных, установленных базовым органом или вышестоящим сертификационным органом, или же любого другого соответствующего требования, на постоянной основе.

61. При подготовке Типового закона в качестве возможных факторов, которые необходимо принимать во внимание при оценке надежности какого-либо сертификационного органа, были рассмотрены следующие элементы: 1) независимость (т. е. отсутствие финансового или иного интереса в затрагиваемых сделках); 2) финансовые ресурсы и наличие финансовых возможностей нести риск привлечения к ответственности за ущерб; 3) компетентность в области технологии использования публичных ключей и надлежащих процедур обеспечения неприкосновенности данных; 4) длительная перспектива работы (от сертификационных органов может потребоваться представление доказательств сертификации или декодирующих ключей через много лет после исполнения затрагивавшихся сделок в связи с судебным иском или имущественным требованием); 5) одобрение аппаратного и программного обеспечения; 6) сохранение документов аудита и проведение аудита независимым органом; 7) существование плана действий в непредвиденных случаях (например, программное обеспечение, позволяющее восстанавливать данные в чрезвычайных случаях, или ключ на хранении у третьей стороны; 8) подбор персонала и руководство им; 9) меры по защите частного ключа самого сертификационного органа; 10) внутренняя безопасность; 11) процедуры прекращения операций, включая направление уведомления пользователям; 12) гарантии и заверения (предоставленные или исключенные); 13) ограничение ответственности; 14) страхование; 15) способность взаимодействовать с другими сертификационными органами; 16) процедуры аннулирования (в случаях, когда криптографические ключи могут быть потеряны или "скомпрометированы").

c) Краткое изложение процесса проставления цифровой подписи

62. Использование цифровых подписей обычно сопряжено со следующими процессами, осуществляемыми либо подписывающим лицом, либо получателем сообщения, подписанного в цифровой форме:

1) пользователь подготавливает пару уникальных криптографических ключей или же такая пара ему предоставляется;

2) отправитель составляет сообщение (например, в форме сообщения по электронной почте) с помощью компьютера;

3) отправитель составляет "резюме сообщения", используя надежный алгоритм хеширования. В процессе создания цифровой подписи используется результат хеширования, полученный как из подписанного сообщения, так и из какого-либо частного ключа и относящийся только к ним. Чтобы результат хеширования был надежным, должна существовать лишь ничтожная вероятность того, что такая же цифровая подпись может быть создана с помощью комбинации любого другого сообщения или частного ключа;

4) отправитель кодирует резюме сообщения с помощью частного ключа. Частный ключ применяется к тексту этого резюме сообщения путем использования математического алгоритма. Цифровая подпись состоит из закодированного резюме сообщения;

5) отправитель обычно прилагает или добавляет свою подпись к сообщению;

6) отправитель направляет цифровую подпись и (незакодированное или закодированное) сообщение получателю электронным способом;

7) получатель использует публичный ключ отправителя для проверки подлинности цифровой подписи отправителя. Проверка подлинности с использованием публичного ключа отправителя служит доказательством того, что сообщение пришло именно от отправителя;

8) получатель также составляет "резюме сообщения", используя тот же надежный алгоритм хеширования;

9) получатель сравнивает два резюме сообщения. Если они одинаковы, то тогда получатель знает, что сообщение не было изменено после его подписания. Если хотя бы один бит в сообщении был изменен после подписания этого сообщения в цифровой форме, резюме сообщения, составленное получателем, будет отличаться от резюме сообщения, составленного отправителем;

10) получатель сообщения получает сертификат от сертификационного органа (или через составителя сообщения), который подтверждает цифровую подпись на сообщении отправителя. Сертификационный орган обычно является доверенной третьей стороной, которая осуществляет сертификацию в системе цифровых подписей. Сертификат, подписанный в цифровой форме сертификационным органом, содержит публичный ключ и имя отправителя (и, возможно, дополнительную информацию).

IV. ОСНОВНЫЕ ЧЕРТЫ ТИПОВОГО ЗАКОНА

A. Законодательная природа Типового закона

63. Новый Типовой закон был подготовлен исходя из той предпосылки, что он будет непосредственно вытекать из статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле и будет рассматриваться в качестве средства, позволяющего представить более подробную информацию относительно концепции "способа, использованного для идентификации" какого-либо лица и "указания на то, что это лицо согласно" с информацией, содержащейся в сообщении данных (см. A/CN.9/WG.IV/WP.71, пункт 49).

64. При разработке этого документа обсуждался вопрос о том, в какой форме он должен быть подготовлен, и, кроме того, была отмечена важность рассмотрения взаимосвязи между формой и содержанием. В отношении возможной формы было предложено использовать различные подходы, в том числе предлагалось подготовить договорные правила, законодательные положения или руководящие принципы для государств, рассматривающих вопрос о принятии законодательства об электронных подписях. В качестве рабочей предпосылки было принято решение о том, что текст следует подготовить в форме законодательных норм, сопровождаемых комментарием, а не просто в форме руководящих принципов (см. A/CN.9/437, пункт 27; A/CN.9/446, пункт 25; и A/CN.9/457, пункты 51 и 72). В конечном итоге этот текст был принят в качестве Типового закона (A/CN.9/483, пункты 137–138).

B. Взаимосвязь с Типовым законом ЮНСИТРАЛ об электронной торговле

1. Новый Типовой закон в качестве отдельного юридического документа

65. Существовала возможность включения новых положений в расширенный вариант Типового закона ЮНСИТРАЛ об электронной торговле, например в качестве новой части III Типового закона ЮНСИТРАЛ об электронной торговле. С тем чтобы ясно указать, что новый Типовой закон может быть принят либо самостоятельно, либо в сочетании с Типовым законом ЮНСИТРАЛ об электронной торговле, в конечном счете было принято решение о том, что новый Типовой закон следует подготовить в качестве отдельного юридического документа (см. документ A/CN.9/465, пункт 37). Это решение основывалось в основном на том факте, что во время окончательной доработки нового Типового закона Типовой закон ЮНСИТРАЛ об электронной торговле уже успешно применялся в ряде стран, а многие другие страны рассматривали вопрос о его принятии. Подготовка расширенного варианта Типового закона ЮНСИТРАЛ об электронной торговле могла бы нанести ущерб первоначальному тексту, поскольку это могло обусловить предположение о необходимости совершенствования этого текста путем обновления. Кроме того, подготовка нового варианта Типового закона ЮНСИТРАЛ об электронной торговле могла бы вызвать трудности для тех стран, которые недавно приняли этот документ.

2. Полное соответствие нового Типового закона Типовому закону ЮНСИТРАЛ об электронной торговле

66. При разработке нового Типового закона предпринимались все возможные усилия для обеспечения его соответствия Типовому закону ЮНСИТРАЛ об электронной торговле как по существу, так и с точки зрения терминологии (A/CN.9/465, пункт 37). В этом новом документе воспроизводятся общие положения Типового закона ЮНСИТРАЛ об электронной торговле. Речь идет о статьях 1

(Сфера применения), 2(a), (c) и (e) (Определения терминов "сообщение данных", "составитель" и "адресат"), 3 (Толкование), 4 (Изменение по договоренности) и 7 (Подпись) Типового закона ЮНСИТРАЛ об электронной торговле.

67. Новый Типовой закон, который основывается на Типовом законе ЮНСИТРАЛ об электронной торговле, направлен, в частности, на то, чтобы отразить следующее: принцип нейтральности с точки зрения носителя информации; подход, согласно которому не допускается дискриминации в отношении функциональных эквивалентов традиционных концепций и практики в сфере использования бумажных документов; и широкое признание автономии сторон (A/CN.9/WG.IV/WP.84, пункт 16). Он предназначен для использования как в качестве минимальных стандартов в "открытой" среде (т. е. в условиях, когда стороны обмениваются электронными сообщениями без предварительного соглашения), так и в качестве типовых договорных положений или субсидиарных правил в "закрытой" среде (т. е. в условиях, когда стороны связаны уже существующими договорными нормами и процедурами, которые подлежат соблюдению при обмене сообщениями с помощью электронных средств).

3. Взаимосвязь со статьей 7 Типового закона ЮНСИТРАЛ об электронной торговле

68. В ходе подготовки нового Типового закона было выражено мнение о том, что ссылка на статью 7 Типового закона ЮНСИТРАЛ об электронной торговле в тексте статьи 6 нового Типового закона должна толковаться в качестве ограничивающей сферу действия нового Типового закона теми ситуациями, когда электронная подпись используется для удовлетворения императивного требования законодательства о том, что для обеспечения *действительности* некоторых документов они должны быть подписаны. Согласно этой точке зрения, в силу того, что в законодательстве большинства стран содержатся лишь весьма немногочисленные подобные требования в отношении документов, используемых для целей коммерческих сделок, сфера действия нового Типового закона является весьма узкой. В ответ на это мнение была высказана получившая общую поддержку точка зрения о том, что подобное толкование статьи 6 (и статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле) не соответствует толкованию слова "законодательство", которое было принято Комиссией в пункте 68 Руководства по принятию Типового закона ЮНСИТРАЛ об электронной торговле и согласно которому «слово "законодательство" ("the law") следует понимать как включающее не только статутное право или подзаконные акты, но также нормы, создаваемые судами, и другие процессуальные нормы». Так, сфера действия и статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле, и статьи 6 нового Типового закона является особенно широкой, поскольку в связи с большинством документов, используемых в контексте коммерческих сделок, на практике, по всей вероятности, возникнет необходимость в соблюдении требований законодательства по вопросам доказывания в том, что касается представления доказательств в письменной форме (A/CN.9/465, пункт 67).

C. "Рамочные правила", дополняемые техническими и договорными нормами

69. Новый Типовой закон, являющийся дополнением к Типовому закону ЮНСИТРАЛ об электронной торговле, преследует цель установления важнейших принципов, направленных на содействие применению электронных подписей. Однако в качестве "рамочного" Типовой закон сам по себе не устанавливает всех

норм и правил, которые могут потребоваться (в дополнение к договорным механизмам, согласованным пользователями) для применения этих методов в принимающем его государстве. Кроме того, как это указывается в настоящем Руководстве, Типовой закон не преследует цели охватить все аспекты применения электронных подписей. Соответственно, принимающее государство, возможно, пожелает принять подзаконные акты, с тем чтобы подробно регламентировать процедуры, вводимые Типовым законом, и учесть конкретные обстоятельства и их возможные изменения в этом государстве без ущерба для целей Типового закона. Если решение о необходимости таких подзаконных актов будет принято, то принимающему Типовой закон государству рекомендуется уделить особое внимание необходимости сохранения гибкости в использовании систем электронных подписей их пользователями.

70. Следует отметить, что методы электронного подписания, рассматриваемые в Типовом законе, могут – в дополнение к вопросам процедурного характера, которые, возможно, потребуется учесть в технических подзаконных актах, принимаемых в целях осуществления Типового закона, – поставить определенные правовые вопросы, ответы на которые могут содержаться не в Типовом законе, а в других правовых нормах. К числу таких правовых норм могут относиться, например, положения применимого административного, договорного, уголовного и судебно-процессуального права, которые не предполагалось охватить в Типовом законе.

D. Дополнительная определенность в отношении правовых последствий электронных подписей

71. Одна из основных черт нового Типового закона состоит в создании дополнительной определенности в отношении применения гибкого критерия, установленного в статье 7 Типового закона ЮНСИТРАЛ об электронной торговле в связи с признанием электронной подписи в качестве функционального эквивалента собственноручной подписи. В статье 7 Типового закона ЮНСИТРАЛ об электронной торговле говорится следующее:

> "1) Если законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если:
>
> *a)* использован какой-либо способ для идентификации этого лица и указания на то, что это лицо согласно с информацией, содержащейся в сообщении данных;
>
> *b)* этот способ является как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано с учетом всех обстоятельств, включая любые соответствующие договоренности.
>
> 2) Пункт 1 применяется как в тех случаях, когда содержащееся в нем требование выражено в форме обязательства, так и в тех случаях, когда законодательство просто предусматривает наступление определенных последствий, если подпись отсутствует.
>
> 3) Положения настоящей статьи не применяются в следующих случаях: […]".

72. Статья 7 основывается на признании функций подписи в сфере бумажных документов. При подготовке Типового закона ЮНСИТРАЛ об электронной торговле были рассмотрены следующие функции подписи: идентификация лица; обеспечение определенности в том, что это лицо лично участвовало в акте подписания; отождествление этого лица с содержанием документа. Было отмечено, что, помимо этого, подпись может выполнять целый ряд других функций в зависимости от характера подписанного документа. Например, подпись может удостоверять намерение стороны принять на себя обязательства в соответствии с содержанием подписанного контракта; намерение лица подтвердить авторство в отношении соответствующего текста; намерение лица одобрить содержание документа, написанного другим лицом; факт того, что определенное лицо в определенное время находилось в определенном месте.

73. В целях обеспечения того, чтобы сообщение, подлинность которого должна быть удостоверена, не лишалось юридической силы на том лишь основании, что его подлинность не была удостоверена тем же способом, что и подлинность бумажных документов, в статье 7 использован комплексный подход. В ней устанавливаются общие условия, при соблюдении которых подлинность сообщений данных будет считаться достаточно надежно удостоверенной и их исковая сила будет признаваться при наличии требований о подписи, которые в настоящее время создают препятствия для электронной торговли. Основное внимание в статье 7 уделяется двум основополагающим функциям подписи, а именно идентификации автора документа и подтверждению согласия автора с содержанием этого документа. В пункте 1(a) устанавливается принцип, в соответствии с которым в условиях использования электронных средств основополагающие правовые функции подписи выполняются с помощью способа, который позволяет идентифицировать составителя сообщения данных и подтвердить, что составитель согласен с содержанием этого сообщения данных.

74. В пункте 1(b) устанавливается гибкий подход к уровню надежности, обеспечиваемому способом идентификации, использованным в соответствии с пунктом 1(a). Способ, использованный согласно пункту 1(a), должен являться как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано с учетом всех обстоятельств, включая любую договоренность между составителем и адресатом сообщения данных.

75. При определении того, является ли способ, использованный согласно пункту 1, соответствующим, могут учитываться, среди прочего, следующие правовые, технические и коммерческие факторы: 1) сложность оборудования, используемого каждой из сторон; 2) характер их коммерческой деятельности; 3) частотность коммерческих сделок между сторонами; 4) вид и объем сделки; 5) функция требований о подписи в конкретной нормативно-правовой среде; 6) возможности систем связи; 7) выполнение процедур удостоверения подлинности, установленных посредниками; 8) набор процедур удостоверения подлинности, предлагаемых каким-либо посредником; 9) соблюдение торговых обычаев и практики; 10) наличие механизмов страхового покрытия для случаев передачи несанкционированных сообщений; 11) важность и ценность информации, содержащейся в сообщении данных; 12) наличие альтернативных способов идентификации и затраты на их использование; 13) степень принятия или непринятия данного способа идентификации в соответствующей отрасли или области как во время достижения договоренности в отношении этого способа, так и во время передачи сообщения данных; и 14) любые другие соответствующие

факторы (Руководство по принятию Типового закона ЮНСИТРАЛ об электронной торговле, пункты 53 и 56–58).

76. На основе гибкого критерия, изложенного в статье 7(1)(b) Типового закона ЮНСИТРАЛ об электронной торговле, в статьях 6 и 7 нового Типового закона устанавливается механизм, с помощью которого может быть предусмотрен порядок для оперативного определения правовой действенности электронных подписей, удовлетворяющих объективному критерию технической надежности. В Типовом законе признаются две категории электронных подписей. Первой и наиболее широкой из них является категория, описанная в статье 7 Типового закона ЮНСИТРАЛ об электронной торговле. Она состоит из любого "способа", который может быть использован для выполнения правового требования о собственноручной подписи. Правовая действенность использования такого "способа" в качестве эквивалента собственноручной подписи зависит от демонстрации его "надежности" лицу или органу, производящему соответствующую оценку. Вторая, более узкая категория подписей создается Типовым законом. В нее входят способы электронного подписания, которые могут быть признаны государственным органом, частным аккредитованным учреждением или самими сторонами в качестве удовлетворяющих критериям технической надежности, установленным в Типовом законе. Преимущество такого признания состоит в том, что оно создает определенность для пользователей подобных методов электронного подписания (которые иногда называются "усиленными", "защищенными" или "отвечающими установленным условиям" электронными подписями) до фактического использования ими соответствующего способа электронного подписания.

Е. Базовые правила поведения заинтересованных сторон

77. Вопросы ответственности, которые могут затронуть различные стороны, участвующие в применении систем электронного подписания, сколь-либо подробно в Типовом законе не рассматриваются. Они оставлены на урегулирование на основании применимого права за пределами Типового закона. В то же время в Типовом законе устанавливаются критерии, на основании которых оценивается поведение таких сторон, т. е. подписавшего, полагающейся стороны и поставщика сертификационных услуг.

78. Что касается подписавшего, то Типовой закон исходит из базового принципа, заключающегося в том, что подписавший обязан проявлять разумную осмотрительность в отношении своего электронного подписывающего устройства. Ожидается, что подписавший будет проявлять разумную осмотрительность для недопущения несанкционированного использования такого подписывающего устройства. В тех случаях, когда подписавшему известно или должно было быть известно о том, что подписывающее устройство было "скомпрометировано", он должен без неоправданных задержек уведомить любое лицо, которое, как он может разумно предполагать, полагается на электронную подпись или предоставляет услуги в связи с ней. В тех случаях, когда для подтверждения электронной подписи используется сертификат, ожидается, что подписавший будет проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений в отношении сертификата.

79. Ожидается, что полагающаяся сторона примет разумные меры для проверки надежности электронной подписи. В тех случаях, когда электронная подпись подкрепляется сертификатом, полагающейся стороне следует принять разумные меры для проверки действительности, приостановления действия или

аннулирования сертификата и соблюдения любых ограничений в отношении сертификата.

80. Общая обязанность поставщика сертификационных услуг заключается в использовании надежных систем, процедур и людских ресурсов и в осуществлении операций в соответствии с заверениями, которые он делает в отношении своей политики и практики. Кроме того, ожидается, что поставщик сертификационных услуг будет проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений в связи с сертификатом. В сертификат поставщик должен включать важнейшую информацию, которая позволит полагающейся стороне установить личность поставщика. Он должен также заверять, что: 1) лицо, которое идентифицировано в сертификате, имело контроль над подписывающим устройством в момент подписания; и 2) подписывающее устройство функционировало на дату или до даты выдачи сертификата. В рамках своих отношений с полагающейся стороной поставщик сертификационных услуг должен предоставлять дополнительную информацию относительно: 1) метода, использованного для идентификации подписавшего; 2) любого ограничения в отношении целей или стоимостного объема, в связи с которыми может использоваться подписывающее устройство или сертификат; 3) функционального состояния подписывающего устройства; 4) любого ограничения в отношении масштаба или объема финансовой ответственности поставщика сертификационных услуг; 5) существования средств для направления подписавшим уведомления о том, что подписывающее устройство было "скомпрометировано"; и 6) наличия услуги по своевременному аннулированию.

81. В Типовом законе также приводится открытый перечень примерных факторов для оценки надежности систем, процедур и людских ресурсов поставщика сертификационных услуг.

F. Рамки, являющиеся нейтральными с точки зрения технологии

82. С учетом темпов технического прогресса Типовой закон обеспечивает правовое признание электронных подписей независимо от вида используемой технологии [например, цифровых подписей, основывающихся на использовании асимметричной криптографии; биометрических характеристик; персональных идентификационных номеров (ПИН); собственноручных подписей в цифровой форме и других методов, таких как нажатие на клавишу "ОК"].

V. ПОМОЩЬ СО СТОРОНЫ СЕКРЕТАРИАТА ЮНСИТРАЛ

A. Помощь в подготовке законопроектов

83. В рамках своей деятельности по подготовке кадров и оказанию помощи Секретариат ЮНСИТРАЛ предоставляет государствам помощь в виде технических консультаций при подготовке законодательства на основе Типового закона ЮНСИТРАЛ об электронных подписях. Такая же помощь предоставляется правительствам, рассматривающим законодательство, основанное на других типовых законах ЮНСИТРАЛ [т. е. на Типовом законе ЮНСИТРАЛ о международном торговом арбитраже, Типовом законе ЮНСИТРАЛ о международных кредитовых переводах, Типовом законе ЮНСИТРАЛ о закупках товаров (работ) и услуг, Типовом законе ЮНСИТРАЛ об электронной торговле и Типовом законе ЮНСИТРАЛ о трансграничной несостоятельности], или рассматривающим вопрос о присоединении к одной из конвенций по праву международной торговли, подготовленных ЮНСИТРАЛ.

84. Более подробную информацию, касающуюся Типового закона, а также других типовых законов и конвенций, подготовленных ЮНСИТРАЛ, можно получить в Секретариате по нижеследующему адресу:

International Trade Law Branch, Office of Legal Affairs
United Nations
Vienna International Centre
P.O. Box 500
A-1400, Vienna, Austria
Telephone: (+43-1) 26060-4060 or 4061
Telecopy: (+43-1) 26060-5813
Electronic mail: uncitral@uncitral.org
Internet Home Page: http://www.uncitral/org

B. Информация о толковании законодательных актов, основывающихся на Типовом законе

85. Секретариат будет рад получить замечания, касающиеся Типового закона и Руководства, а также информацию, касающуюся принятия законодательства, основанного на Типовом законе. Типовой закон, после его принятия, будет включен в информационную систему ППТЮ, которая используется для сбора и распространения информации о судебных и арбитражных решениях, касающихся конвенций и типовых законов, явившихся результатом работы ЮНСИТРАЛ. Цель этой системы состоит в привлечении международного внимания к законодательным текстам, разработанным ЮНСИТРАЛ, и в содействии их единообразному толкованию и применению. Секретариат публикует на шести официальных языках Организации Объединенных Наций выдержки из решений и предоставляет для ознакомления – за плату, покрывающую расходы на изготовление копий, – сами решения, на основе которых были подготовлены выдержки. Функционирование этой системы разъясняется в руководстве для пользователей, которое может быть получено в Секретариате в виде изданного документа (A/CN.9/SER.C/GUIDE/1) и ознакомиться с которым можно на вышеупомянутой собственной странице ЮНСИТРАЛ в сети Интернет.

Глава II. Постатейные комментарии

Название

"*Типовой закон*"

86. В ходе всей работы по подготовке этого документа он задумывался как дополнение к Типовому закону ЮНСИТРАЛ об электронной торговле, которое должно рассматриваться на тех же основаниях и которое должно обладать той же юридической природой, что и Типовой закон ЮНСИТРАЛ об электронной торговле.

Статья 1. Сфера применения

Настоящий Закон применяется в тех случаях, когда электронные подписи используются в контексте[*] торговой[**] деятельности. Он не имеет преимущественной силы по отношению к любой правовой норме, предназначенной для защиты потребителей.

[*] Для государств, которые, возможно, пожелают расширить сферу применения настоящего Закона, Комиссия предлагает следующий текст:

"Настоящий Закон применяется в тех случаях, когда используются электронные подписи, за исключением следующих ситуаций: […]".

[**] Термин "торговая" следует толковать широко, с тем чтобы он охватывал вопросы, вытекающие из всех отношений торгового характера, как договорных, так и недоговорных. Отношения торгового характера включают следующие сделки, не ограничиваясь ими: любые торговые сделки на поставку товаров или услуг или обмен товарами или услугами; дистрибьюторские соглашения; коммерческое представительство и агентские отношения; факторинг; лизинг; строительство промышленных объектов; предоставление консультативных услуг; инжиниринг; купля/продажа лицензий; инвестирование; финансирование; банковские услуги; страхование; соглашения об эксплуатации или концессии; совместные предприятия и другие формы промышленного или предпринимательского сотрудничества; перевозка товаров и пассажиров воздушным, морским, железнодорожным и автомобильным транспортом.

Общие замечания

87. Цель статьи 1 заключается в том, чтобы обозначить сферу применения Типового закона. Используемый в Типовом законе подход состоит в том, чтобы обеспечить, как принцип, охват всех фактических ситуаций использования электронных подписей, независимо от применения какой-либо конкретной электронной подписи или метода удостоверения подлинности. В ходе подготовки Типового закона было сочтено, что исключение любой формы или любого носителя путем ограничения сферы действия Типового закона может привести к практическим трудностям и будет противоречить цели подготовки правил, являющихся действительно "нейтральными с точки зрения носителя информации". В то же время в ходе подготовки Типового закона особое внимание уделялось "цифровым подписям", т. е. тем электронным подписям, для проставления которых

используется криптография двойных ключей, которая, по мнению Рабочей группы ЮНСИТРАЛ по электронной торговле, представляет собой особенно распространенную технологию. В центре внимания Типового закона стоят вопросы использования современной технологии, и, если в нем прямо не предусмотрено иное, Типовой закон не преследует цели изменить традиционные нормы, касающиеся собственноручных подписей.

Сноска[**]

88. Было сочтено, что в Типовой закон должно быть включено указание на то, что основное внимание в нем уделяется тем видам ситуаций, которые встречаются в коммерческой области, и что они разрабатывались в контексте торгово-финансовых отношений. По этой причине в статью 1 была включена ссылка на "торговую деятельность", а в сноску[**] включены указания на то, что под этим понимается. Эти указания, которые могут быть особенно полезными для тех стран, где не имеется отдельного свода норм торгового права, соответствуют, по соображениям необходимости обеспечения последовательности, сноске к статье 1 Типового закона ЮНСИТРАЛ о международном торговом арбитраже (которая также воспроизводится в качестве сноски[****] к статье 1 Типового закона ЮНСИТРАЛ об электронной торговле). В некоторых странах использование сносок в тексте законодательного акта может не рассматриваться в качестве приемлемой законодательной практики. Поэтому национальные власти, принимающие Типовой закон, могли бы рассмотреть возможность включения текста ссылок непосредственно в текст Типового закона.

Сноска[*]

89. Типовой закон применяется ко всем видам сообщений данных, к которым может прикладываться электронная подпись, создающая правовые последствия, и ничто в Типовом законе не должно препятствовать намерению принимающих его государств расширить сферу действия Типового закона, с тем чтобы охватить виды использования электронных подписей за пределами коммерческой сферы. Например, хотя основное внимание в Типовом законе уделяется не отношениям между лицами, использующими электронные подписи, и публичными органами, не предполагается, что Типовой закон не может применяться к таким отношениям. В сноске[*] содержится альтернативная формулировка для возможного использования принимающими государствами, которые могут счесть целесообразным расширить сферу действия Типового закона за пределы коммерческой сферы.

Защита потребителей

90. В некоторых странах действуют специальные законы о защите потребителей, которые могут регулировать определенные аспекты использования информационных систем. Что касается такого законодательства о защите потребителей, то, как и в случае предыдущих документов ЮНСИТРАЛ (например, Типового закона ЮНСИТРАЛ о международных кредитовых переводах и Типового закона ЮНСИТРАЛ об электронной торговле), было сочтено, что следует включить указание на то, что при подготовке Типового закона особого внимания вопросам, которые могут возникнуть в контексте защиты потребителей, не уделялось. В то же время было сочтено, что нет никаких причин для исключения ситуаций, затрагивающих потребителей, из сферы действия Типового закона посредством принятия какого-либо общего положения, особенно в силу того, что положения

Типового закона могут быть сочтены вполне благоприятными для защиты потребителей, в зависимости от законодательства конкретного государства, принимающего этот закон. В силу этого в статье 1 признается, что любое такое законодательство о защите потребителей может иметь преимущественную силу по отношению к положениям Типового закона. Если законодатели придут к иным выводам в вопросе о благоприятном воздействии Типового закона на потребительские сделки в той или иной стране, они могут рассмотреть возможность исключения вопросов, связанных с потребителями, из сферы применения законодательного акта, вводящего в действие Типовой закон. Вопрос о том, какие физические или юридические лица будут рассматриваться в качестве "потребителей", оставлен на урегулирование на основании применимого права за пределами Типового закона.

Использование электронных подписей в международных и внутренних сделках

91. Рекомендуется обеспечить применение Типового закона, по возможности, на максимально широкой основе. Особую осторожность следует проявлять при исключении применения Типового закона путем ограничения сферы его действия международными видами использования электронных подписей, поскольку подобное ограничение может быть рассмотрено как препятствующее полному достижению целей Типового закона. Кроме того, разнообразие процедур, которые могут быть использованы в соответствии с Типовым законом для ограничения использования электронных подписей в случаях, когда это требуется (например, по соображениям публичного порядка), может уменьшить необходимость в ограничении сферы действия Типового закона. Правовая определенность, которую будет обеспечивать Типовой закон, является необходимой как для внутренней, так и международной торговли, а двойственность режимов, регулирующих использование электронных подписей, может создать серьезное препятствие для использования таких средств.

Справочные документы ЮНСИТРАЛ

A/CN.9/467, пункты 22–24;
A/CN.9/WG.IV/WP.84, пункт 22;
A/CN.9/465, пункты 36–42;
A/CN.9/WG.IV/WP.82, пункт 21;
A/CN.9/457, пункты 53–64.

Статья 2. Определения

Для целей настоящего Закона:

a) "электронная подпись" означает данные в электронной форме, которые содержатся в сообщении данных, приложены к нему или логически ассоциируются с ним и которые могут быть использованы для идентификации подписавшего в связи с сообщением данных и указания на то, что подписавший согласен с информацией, содержащейся в сообщении данных;

b) "сертификат" означает сообщение данных или иную запись, подтверждающую наличие связи между подписавшим и данными для создания подписи;

c) "сообщение данных" означает информацию, подготовленную, отправленную, полученную или хранимую с помощью электронных, оптических или аналогичных средств, включая электронный обмен данными (ЭДИ), электронную почту, телеграмму, телекс или телефакс, но не ограничиваясь ими;

d) "подписавший" означает лицо, которое обладает данными для создания подписи и действует от своего собственного имени или от имени лица, которое оно представляет;

e) "поставщик сертификационных услуг" означает лицо, которое выдает сертификаты и может предоставлять другие услуги, связанные с электронными подписями;

f) "полагающаяся сторона" означает лицо, которое может действовать на основании сертификата или электронной подписи.

Определение понятия "электронная подпись"

Электронная подпись как функциональный эквивалент собственноручной подписи

92. Понятие "электронная подпись" призвано охватить все традиционные виды использования собственноручной подписи для обеспечения ее юридической силы, идентификации подписавшего и определения намерения подписать, которое является не чем иным, как наименьшим общим знаменателем различных подходов к "подписи", принятых в различных правовых системах. Эти функции собственноручной подписи уже рассматривались в контексте подготовки текста статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле. Таким образом, определение электронной подписи как способной указывать на согласие с информацией равнозначно в первую очередь установлению технического предварительного условия признания какой-либо данной технологии, способной создавать эквивалент собственноручной подписи. Это определение не игнорирует тот факт, что технологии, называемые обычно "электронными подписями", могут использоваться в иных целях, чем создание юридически значимой подписи. Это определение всего лишь показывает, что Типовой закон направлен на использование электронных подписей в качестве функциональных эквивалентов собственноручных подписей (см. документ A/CN.9/483, пункт 62).

Возможные другие виды использования электронной подписи

93. Следует провести различие между правовым понятием "подписи" и техническим понятием "электронной подписи", т. е. термином, охватывающим те виды практики, которые необязательно связаны с созданием юридически значимых подписей. В ходе подготовки Типового закона считалось, что внимание пользователей следует обратить на риск возникновения путаницы в результате использования одного и того же технического средства для создания юридически значимой подписи и для других функций удостоверения подлинности и идентификации (там же).

Определение понятия "сертификат"

Необходимость в определении

94. Термин "сертификат" используется в контексте определенных видов электронных подписей и, как определено в Типовом законе, мало чем отличается от его общего значения документа, которым какое-либо лицо подтверждает некоторые факты. Однако, поскольку общего понятия "сертификат" не существует во всех правовых системах или, фактически, во всех языках, было сочтено полезным включить его определение в контекст Типового закона (там же, пункт 65).

Цель сертификата

95. Цель сертификата заключается в том, чтобы признать, показать или подтвердить связь между данными для создания подписи и подписавшим. Эта связь устанавливается в момент получения данных для создания подписи (там же, пункт 67).

"данные для создания подписи"

96. Слова "данные для создания подписи" призваны обозначить те секретные ключи, коды или другие элементы, которые в процессе создания электронной подписи используются для обеспечения надежной связи между создаваемой электронной подписью и личностью подписавшего. Например, в контексте цифровых подписей, основанных на асимметричной криптографии, функциональным ключевым элементом, в отношении которого можно утверждать, что он "связан с подписавшим и ни с каким другим лицом", является пара криптографических ключей. В контексте электронных подписей, основанных на применении биометрических устройств, важнейшим элементом является биометрический индикатор, например отпечаток пальца или данные сканирования сетчатки глаза. Это определение охватывает только те ключевые элементы, конфиденциальность которых следует обеспечивать для гарантирования качества процесса подписания, и не охватывает любые другие элементы, которые, хотя они и могут способствовать процессу подписания, можно раскрывать, не подвергая опасности надежность создаваемой электронной подписи. Например, в случае цифровых подписей, хотя и публичный, и частный ключи связаны с личностью подписавшего, только частный ключ должен охватываться таким определением, поскольку необходимо обеспечивать конфиденциальность только частного ключа, а публичный ключ неизбежно должен быть общеизвестен (A/CN.9/483, пункт 71). В число элементов, которые не должны охватываться этим определением, входит текст, подписываемый электронным способом, который, хотя он также играет важную роль в процессе создания подписи (посредством функции хеширования или как-либо иначе), явно не должен быть предметом такой же конфиденциальности, что и информация, идентифицирующая подписавшего (там же, пункты 72 и 76). Статья 6 выражает идею о том, что данные для создания подписи должны быть связаны с подписавшим и ни с каким другим лицом (там же, пункт 75).

Определение понятия "сообщение данных"

97. Определение "сообщения данных" взято из статьи 2 Типового закона ЮНСИТРАЛ об электронной торговле как широкое понятие, охватывающее все сообщения, создаваемые в контексте электронной торговли, включая "web-торговлю" (там же, пункт 69). Понятие "сообщение данных" не ограничивается переданным сообщением, но также призвано охватить компьютерные записи,

которые не предназначаются для передачи. Таким образом, понятие "сообщение" включает понятие "запись".

98. Ссылка на "аналогичные средства" призвана отразить то обстоятельство, что Типовой закон не предназначается только для применения в контексте существующих методов передачи сообщений, но стремится учесть предвидимые технические достижения. Цель определения "сообщения данных" заключается в охвате всех видов сообщений, которые подготовлены, хранятся или отправлены по существу в безбумажной форме. Для этой цели все средства передачи сообщений и хранения информации, которые могут использоваться для выполнения функций, параллельных функциям, выполняемым с помощью средств, перечисленных в этом определении, охватываются ссылкой на "аналогичные средства", хотя, например, "электронные" и "оптические" средства передачи сообщений могут и не быть, строго говоря, аналогичными. Для целей Типового закона слово "аналогичный" означает "функционально-эквивалентный".

99. Определение "сообщения данных" также призвано применяться в случае отзыва или изменения сообщения данных. Считается, что сообщение данных имеет фиксированное информационное содержание, однако оно может быть отозвано или изменено с помощью другого сообщения данных (Руководство по принятию Типового закона ЮНСИТРАЛ об электронной торговле, пункты 30–32).

Определение понятия "подписавший"

"лицо"

100. В соответствии с подходом, принятым в Типовом законе ЮНСИТРАЛ об электронной торговле, любая ссылка в новом Типовом законе на какое-либо "лицо" должна пониматься как охватывающая все категории лиц или организаций, будь то физические, корпоративные или другие юридические лица (A/CN.9/483, пункт 86).

"от имени лица, которое оно представляет"

101. Аналогия с собственноручными подписями может и не быть всегда приемлемой с точки зрения использования возможностей, предлагаемых современной технологией. Например, в среде бумажных документов юридические лица, строго говоря, не могут являться стороной, подписавшей документы, составленные от их имени, поскольку действительные собственноручные подписи могут проставлять только физические лица. Однако электронные подписи могут быть разработаны таким образом, чтобы позволять осуществлять их атрибуцию компаниям или другим юридическим лицам (включая правительственные или другие государственные органы), и могут существовать ситуации, когда личность какого-либо лица, фактически подготовившего подпись – в случаях, когда для этого требуются действия человека, – может не иметь какого-либо значения с точки зрения целей, в которых была создана подпись (там же, пункт 85).

102. Тем не менее в соответствии с Типовым законом понятие "подписавший" не может быть отделено от физического или юридического лица, которые фактически создали электронную подпись, поскольку ряд устанавливаемых согласно Типовому закону конкретных обязательств подписавшего логически связан с фактическим контролем над данными для создания подписи. Однако чтобы охватить ситуации, когда подписавший будет действовать как представитель другого лица, в определении понятия "подписавший" были сохранены слова "или от имени лица,

которое оно представляет". Вопрос о степени, в которой какое-либо лицо будет связано электронной подписью, созданной "от его имени", должен решаться в соответствии с правом, регулирующим, на надлежащих основаниях, правовые отношения между подписавшим и лицом, от имени которого была создана подпись, с одной стороны, и полагающейся стороной – с другой. Этот вопрос, а также другие вопросы, затрагивающие основную сделку, включая вопросы агентских отношений и другие вопросы, например о том, кто несет конечную ответственность за неспособность подписавшего выполнить свои обязательства по статье 8 (будь то подписавший или лицо, которое представлял подписавший), выходят за пределы сферы действия Типового закона (там же, пункты 86–87).

Определение понятия "поставщик сертификационных услуг"

103. Как минимум, поставщик сертификационных услуг, определяемый для целей Типового закона, должен будет предоставлять сертификационные услуги, возможно наряду с другими услугами (там же, пункт 100).

104. В Типовом законе не проводится различие между ситуациями, когда поставщик сертификационных услуг занимается предоставлением сертификационных услуг в качестве своей основной деятельности или же вспомогательной деятельности, на регулярной или на нерегулярной основе, непосредственно или же через субподрядчика. Это определение охватывает всех субъектов, которые предоставляют сертификационные услуги в пределах сферы действия Типового закона, т. е. "в контексте торговой деятельности". Однако с учетом этого ограничения сферы применения Типового закона субъекты, которые выдают сертификаты для внутренних целей, а не в торговых целях, не будут входить в категорию "поставщиков сертификационных услуг", как они определены в статье 2 (там же, пункты 94–99).

Определение понятия "полагающаяся сторона"

105. Определение "полагающейся стороны" призвано обеспечить симметрию в определении различных сторон, участвующих в процессе функционирования систем электронных подписей согласно Типовому закону (там же, пункт 107). Для целей этого определения слово "действовать" следует толковать широко – как охватывающее не только фактическое действие, но и бездействие (там же, пункт 108).

Справочные документы ЮНСИТРАЛ

A/CN.9/483, пункты 59–109;
A/CN.9/WG.IV/WP.84, пункты 23–36;
A/CN.9/465, пункт 42;
A/CN.9/WG.IV/WP.82, пункты 22–23;
A/CN.9/457, пункты 22–47; 66–67; 89; 109;
A/CN.9/WG.IV/WP.80, пункты 7–10;
A/CN.9/WG.IV/WP.79, пункт 21;
A/CN.9/454, пункт 20;
A/CN.9/WG.IV/WP.76, пункты 16–20;
A/CN.9/446, пункты 27–46 (проект статьи 1), 62–70 (проект статьи 4), 113–131 (проект статьи 8), 132–133 (проект статьи 9);
A/CN.9/WG.IV/WP.73, пункты 16–27; 37–38; 50–57 и 58–60;
A/CN.9/437, пункты 29–50 и 90–113 (проекты статей A, B и C);
A/CN.9/WG.IV/WP.71, пункты 52–60.

Статья 3. Равный режим для технологий создания электронных подписей

Ничто в настоящем Законе, за исключением статьи 5, не применяется таким образом, чтобы исключать, ограничивать или лишать юридической силы любой метод создания электронной подписи, который удовлетворяет требованиям, указанным в статье 6(1) настоящего Закона, или иным образом отвечает требованиям применимого права.

Нейтральность с точки зрения технологии

106. В статье 3 закрепляется основополагающий принцип, заключающийся в том, что не допускается дискриминация в отношении ни одного из способов электронного подписания, т. е. что для всех технологий будут предусматриваться одни и те же возможности удовлетворения требований статьи 6. В результате этого не должно быть никаких расхождений в режимах сообщений, подписанных электронным образом, и бумажных документов, подписанных собственноручно, или в режимах различных видов сообщений, подписанных электронным образом, при условии, что они удовлетворяют основополагающим требованиям, установленным в статье 6(1) Типового закона или любым другим требованиям, установленным в применимом праве. Такие требования могут, например, предписывать использование конкретно указанных способов подписания в определенных конкретных ситуациях или могут иным образом устанавливать стандарты, которые могут быть выше или ниже, чем те, которые установлены в статье 7 Типового закона ЮНСИТРАЛ об электронной торговле (и в статье 6 Типового закона). Предполагается обеспечить общую применимость основополагающего принципа недискриминации. Следует отметить, однако, что закрепление этого принципа не преследует цели оказать воздействие на свободу договора, признаваемую согласно статье 5. В отношениях между собой и в той мере, в которой это допускается законодательством, стороны должны сохранять свободу исключать, на основании соглашения, использование некоторых способов электронного подписания. С помощью формулировки "ничто в настоящем Законе не применяется таким образом, чтобы исключать, ограничивать или лишать юридической силы любой метод создания электронной подписи" в статье 3 просто устанавливается, что форма приложения определенных электронных подписей не может использоваться в качестве единственного основания, по которому такой подписи может быть отказано в правовой действенности. В то же время статью 3 не следует ошибочно толковать как устанавливающую правовую действительность любого конкретного способа подписания или любой информации, подписанной в электронной форме.

Справочные документы ЮНСИТРАЛ

A/CN.9/467, пункты 25–32;
A/CN.9/WG.IV/WP.84, пункт 37;
A/CN.9/465, пункты 43–48;
A/CN.9/WG.IV/WP.82, пункт 34;
A/CN.9/457, пункты 53–64.

Статья 4. Толкование

1) При толковании настоящего Закона следует учитывать его международное происхождение и необходимость содействовать достижению единообразия в его применении и соблюдению добросовестности.

2) Вопросы, которые относятся к предмету регулирования настоящего Закона и которые прямо в нем не разрешены, подлежат разрешению в соответствии с общими принципами, на которых основан настоящий Закон.

Источник

107. Статья 4 сформулирована на основе статьи 7 Конвенции Организации Объединенных Наций о договорах международной купли-продажи товаров и аналогична статье 3 Типового закона ЮНСИТРАЛ об электронной торговле. Ее цель состоит в том, чтобы установить руководящие положения для толкования Типового закона третейскими судами, судами и другими национальными или местными административными органами. Применение статьи 4, как ожидается, будет способствовать ограничению той степени, в которой унифицированный текст после его включения в местное законодательство будет толковаться только с помощью ссылок на концепции местного права.

Пункт 1

108. Цель пункта 1 состоит в том, чтобы обратить внимание любого лица, которое может столкнуться с необходимостью применения Типового закона, на тот факт, что положения Типового закона (или положения документа, вводящего в действие Типовой закон), хотя они и приняты как часть национального законодательства и, таким образом, носят внутренне-правовой характер, должны толковаться с учетом их международного происхождения для обеспечения единообразия в толковании Типового закона во всех принимающих его странах.

Пункт 2

109. Что касается общих принципов, на которых основывается Типовой закон, то может быть рассмотрен следующий неисчерпывающий перечень: 1) содействие международной и внутренней электронной торговле; 2) признание юридической силы сделок, заключенных с помощью новых информационных технологий; 3) содействие развитию и поощрение применения новых информационных технологий в целом и электронных подписей в частности таким образом, который был бы нейтральным с технологической точки зрения; 4) содействие унификации права; и 5) поддержка коммерческой практики. Хотя общая цель Типового закона заключается в содействии использованию электронных подписей, его никоим образом не следует толковать как навязывающий их использование.

Справочные документы ЮНСИТРАЛ

A/CN.9/467, пункты 33–35;
A/CN.9/WG.IV/WP.84, пункт 38;
A/CN.9/465, пункты 49–50;
A/CN.9/WG.IV/WP.82, пункт 35.

Статья 5. Изменение по договоренности

Допускается отход от положений настоящего Закона или изменение их действия по договоренности, за исключением случаев, когда такая договоренность не будет действительной или не будет иметь правовых последствий согласно применимому праву.

Отсылка к применимому праву

110. Решение провести работу по подготовке Типового закона основывалось на признании того, что правовые проблемы, связанные с использованием современных средств передачи данных, на практике пытаются урегулировать в первую очередь в тексте контрактов. Цель Типового закона состоит, таким образом, в том, чтобы подтвердить принцип автономии сторон. В то же время применимое право может устанавливать ограничения в отношении этого принципа. Статью 5 не следует ошибочно толковать как разрешающую сторонам отходить от императивных норм, например норм, принятых в силу соображений публичного порядка. Ничто в статье 5 не следует ошибочно толковать как поощряющее государства к установлению императивных законодательных ограничений на автономию сторон применительно к использованию электронных подписей или иным образом предлагающее государствам ограничить свободу сторон согласовывать в отношениях между собой вопросы о формальных требованиях применительно к обмену сообщениями между ними.

111. Принцип автономии сторон широко применяется в отношении положений Типового закона, поскольку Типовой закон не содержит какого-либо императивного положения. Этот принцип также применяется в контексте статьи 13(1). В силу этого, хотя суды принимающего государства или органы, ответственные за применение Типового закона, не должны отказывать в юридической силе иностранным сертификатам или аннулировать их правовые последствия только на основании места выдачи сертификата, статья 13(1) не ограничивает свободу сторон коммерческих сделок договариваться об использовании сертификатов, выданных в каком-либо конкретном месте (A/CN.9/483, пункт 112).

Прямая или подразумеваемая договоренность

112. Что касается формы изложения принципа автономии сторон в статье 5, то в ходе подготовки Типового закона в целом признавалось, что изменения могут вноситься по прямой или подразумеваемой договоренности. Была сохранена согласованность формулировки статьи 5 со статьей 6 Конвенции Организации Объединенных Наций о договорах международной купли-продажи товаров (A/CN.9/467, пункт 38).

Двусторонняя или многосторонняя договоренность

113. Статья 5 предназначена для применения не только в контексте отношений между составителями и адресатами сообщений данных, но и в контексте отношений с участием посредников. Таким образом, положения Типового закона могут быть изменены либо на основе двусторонних или многосторонних договоренностей между сторонами, либо на основе согласованных сторонами системных правил. Как правило, применимое право будет ограничивать сферу действия принципа автономии сторон правами и обязательствами, создаваемыми в отношениях между этими сторонами, с тем чтобы исключить какие-либо последствия для прав и обязательств третьих сторон.

Справочные документы ЮНСИТРАЛ

A/CN.9/467, пункты 36–43;
A/CN.9/WG.IV/WP.84, пункты 39–40;
A/CN.9/465, пункты 51–61;
A/CN.9/WG.IV/WP.82, пункты 36–40;
A/CN.9/457, пункты 53–64.

Статья 6. Соблюдение требования в отношении наличия подписи

1) В тех случаях, когда законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если использована электронная подпись, которая является настолько надежной, насколько это соответствует цели, для которой сообщение данных было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности.

2) Пункт 1 применяется как в тех случаях, когда упомянутое в нем требование имеет форму обязательства, так и в тех случаях, когда законодательство просто предусматривает наступление определенных последствий, если подпись отсутствует.

3) Электронная подпись считается надежной для цели удовлетворения требования, упомянутого в пункте 1, если:

a) данные для создания электронной подписи в том контексте, в котором они используются, связаны с подписавшим и ни с каким другим лицом;

b) данные для создания электронной подписи в момент подписания находились под контролем подписавшего и никакого другого лица;

c) любое изменение, внесенное в электронную подпись после момента подписания, поддается обнаружению; и

d) в тех случаях, когда одна из целей правового требования в отношении наличия подписи заключается в гарантировании целостности информации, к которой она относится, любое изменение, внесенное в эту информацию после момента подписания, поддается обнаружению.

4) Пункт 3 не ограничивает возможности любого лица в отношении:

a) установления любым другим способом для цели удовлетворения требования, упомянутого в пункте 1, надежности электронной подписи; или

b) представления доказательств ненадежности электронной подписи.

5) Положения настоящей статьи не применяются в следующих случаях: […].

Важность статьи 6

114. Статья 6 является одним из ключевых положений Типового закона. Цель статьи 6 состоит в развитии положений статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле и в установлении руководящих указаний относительно того порядка, в котором может удовлетворяться критерий надежности, предусмотренный в статье 7(1)(b). При толковании статьи 6 следует учитывать, что цель этого положения заключается в обеспечении того, чтобы во всех случаях, когда из использования собственноручной подписи вытекают какие-либо правовые последствия, точно такие же последствия вытекали бы из использования надежной электронной подписи.

Пункты 1, 2 и 5

115. В пунктах 1, 2 и 5 статьи 6 воспроизводятся положения, взятые, соответственно, из статьи 7 (1)(b), (2) и (3) Типового закона ЮНСИТРАЛ об электронной торговле. Формулировка, основывающаяся на статье 7(1) Типового закона ЮНСИТРАЛ об электронной торговле, уже включена в определение "электронной подписи" согласно статье 2(a).

Понятия "личности" и "идентификации"

116. Рабочая группа согласилась с тем, что для целей определения "электронной подписи" в соответствии с Типовым законом термин "идентификация" может толковаться более широко, чем простая идентификация подписавшего по его имени. Понятия "личности" или "идентификации" включают выделение соответствующего лица по его имени или иным образом из числа любых других лиц и могут относиться к другим существенным характеристикам, таким как занимаемая должность или имеющиеся полномочия, будь то в сочетании с именем соответствующего лица или без ссылки на него. По этой причине не имеется необходимости в проведении разграничения между "личностью" и другими существенными характеристиками или же ограничивать действие Типового закона теми ситуациями, когда используются только сертификаты личности, в которых указывается имя обладателя подписывающего устройства (A/CN.9/467, пункты 56–58).

Типовой закон предусматривает различные последствия в зависимости от уровня технической надежности

117. В ходе подготовки Типового закона было высказано мнение о том, что (либо с помощью ссылки на понятие "электронной подписи с высокой степенью защиты", либо с помощью прямого упоминания критериев для установления технической надежности того или иного метода подписания) двойная цель статьи 6 должна состоять в установлении следующего: 1) из применения тех методов электронного подписания, которые признаны надежными, будут вытекать правовые последствия и 2) наоборот, никаких таких правовых последствий не будет вытекать из применения методов, являющихся менее надежными. В то же время в целом было сочтено, что между различными возможными методами электронного подписания потребуется, по всей вероятности, провести более тонкое различие, поскольку Типовой закон не должен устанавливать дискриминацию в отношении какой-либо формы электронной подписи, какой бы упрощенной и ненадежной она ни могла показаться в конкретных обстоятельствах. В силу этого любой метод электронного подписания, примененный для подписания сообщения данных согласно статье 7(1)(a) Типового закона ЮНСИТРАЛ об электронной торговле будет, по всей вероятности, создавать правовые последствия при условии, что он является достаточно надежным с учетом всех обстоятельств, включая любую договоренность между сторонами. В то же время согласно статье 7 Типового закона ЮНСИТРАЛ об электронной торговле любое определение в отношении того, что представляет собой надежный способ подписания с учетом обстоятельств, может быть вынесено только судом или другим лицом или органом, оценивающим факты и действующим согласно возложенным на него функциям, возможно уже по истечении длительного срока после проставления электронной подписи. В отличие от этого новый Типовой закон направлен на то, чтобы создать презумпцию, благоприятствующую некоторым методам, которые признаны в качестве особенно надежных, независимо от обстоятельств их использования. Именно эту цель преследует пункт 3, который направлен на создание – уже в момент или еще до начала использования любого такого метода электронного подписания (*ex ante*) – определенности (либо с помощью презумпции,

либо с помощью материально-правовой нормы) относительно того, что использование признанного метода приведет к правовым последствиям, эквивалентным последствиям собственноручной подписи. Таким образом, пункт 3 является важнейшим положением для достижения цели Типового закона, заключающейся в обеспечении более значительной определенности, чем та, которая уже создается Типовым законом ЮНСИТРАЛ об электронной торговле, в отношении правовых последствий, наступления которых можно ожидать в случае использования особенно надежных видов электронных подписей (см. документ A/CN.9/465, пункт 64).

Презумпция или материально-правовая норма

118. В целях обеспечения определенности относительно правовых последствий, вытекающих из использования подписи, которая может или не может считаться "электронной подписью с высокой степенью защиты" согласно статье 2, в пункте 3 прямо устанавливаются правовые последствия, которые будут вытекать из наличия определенных технических характеристик электронной подписи. Что касается порядка установления таких последствий, то государства, принимающие Типовой закон, должны иметь возможность, по своему выбору и в зависимости от своего гражданско-процессуального и торгового законодательства, установить соответствующую презумпцию или определить такие последствия путем прямого закрепления связи между определенными техническими характеристиками и правовыми последствиями подписи (см. документ A/CN.9/467, пункты 61–62).

Намерение подписавшего

119. Остается неурегулированным вопрос о том, должны ли вытекать какие-либо правовые последствия из использования методов электронного подписания, которые могут быть применены без явного намерения подписавшего выразить согласие на юридическую силу одобрения информации, подписываемой в электронной форме. В любых подобных обстоятельствах вторая функция, описанная в статье 7(1)(a) Типового закона ЮНСИТРАЛ об электронной торговле, не выполняется, поскольку отсутствует "намерение указать какое-либо согласие с информацией, содержащейся в сообщении данных". Подход, использованный в Типовом законе, состоит в том, что правовые последствия использования собственноручной подписи должны воспроизводиться в электронной среде. Таким образом, в результате подписания (будь то собственноручного или электронного) определенной информации должна возникать презумпция того, что подписавший выразил согласие с установлением связи между его личностью и этой информацией. Ответ на вопрос о том, создает ли такая связь какие-либо правовые последствия (договорные или иные), будет зависеть от характера подписываемой информации и от любых других обстоятельств, которые должны быть оценены в соответствии с правом, применимым за пределами сферы действия Типового закона. В этом контексте Типовой закон отнюдь не преследует цели создания коллизии с общим договорным или обязательственным правом (см. документ A/CN.9/465, пункт 65).

Критерий технической надежности

120. Цель подпунктов (a)–(d) пункта 3 состоит в том, чтобы оговорить объективный критерий технической надежности электронных подписей. В центре внимания подпункта (a) стоят объективные характеристики данных для создания подписи, которые должны быть связаны с "подписавшим и ни с каким другим лицом". С технической точки зрения данные для создания подписи могут устанавливать уникальную "связь" с подписавшим, не являясь сами по себе

"уникальными". Важнейшим элементом является связь между данными, использованными для создания подписи, и подписавшим (A/CN.9/467, пункт 63). Хотя определенные данные для создания электронной подписи могут совместно использоваться самыми различными пользователями, например в тех случаях, когда несколько сотрудников будут совместно использовать корпоративные данные для создания подписей, такие данные должны давать возможность несомненной идентификации каждого пользователя в контексте каждой электронной подписи.

Исключительный контроль подписавшего над данными для создания подписи

121. Подпункт (b) касается обстоятельств, при которых используются данные для создания подписи. В момент использования данных для создания подписи они должны находиться под исключительным контролем подписавшего. В связи с концепцией исключительного контроля подписавшего возникает вопрос о том, сохраняет ли подписавший способность уполномочивать другое лицо использовать данные для создания подписи от его имени. Такая ситуация может возникнуть в случае использования данных для создания подписи в корпоративном контексте, когда подписавшим будет являться корпорация, однако при этом целый ряд лиц будет иметь право ставить подпись от ее имени (A/CN.9/467, пункт 66). Еще одним примером в этой связи могут быть коммерческие прикладные программы, когда данные для создания подписи существуют в сети и могут использоваться целым рядом лиц. В подобной ситуации сеть будет предположительно связана с конкретным субъектом, который будет являться подписавшим и будет осуществлять контроль над данными для создания подписи. Если дело будет обстоять иным образом и данные для создания подписи будут находиться в широком доступе, то подобные ситуации не должны охватываться Типовым законом (A/CN.9/467, пункт 67). Если один ключ используется несколькими лицами в рамках схемы "разъемного ключа" или другой схемы "ограниченного доступа для нескольких пользователей", ссылка на "подписавшего" означает ссылку на всю группу таких лиц (A/CN.9/483, пункт 152).

Агентские услуги

122. В результате совместного применения подпунктов (a) и (b) обеспечивается такой порядок, при котором данные для создания подписи могут использоваться в какой-либо конкретный момент только одним лицом, в первую очередь в момент, когда создается подпись, и не могут быть использованы каким-либо иным лицом. Вопрос об агентских услугах или санкционированном использовании данных для создания подписи должен быть урегулирован в определении термина "подписавший" (A/CN.9/467, пункт 68).

Целостность

123. Подпункты (c) и (d) касаются вопросов целостности электронной подписи и целостности информации, подписываемой в электронной форме. По всей вероятности, существовала возможность объединить эти два положения, с тем чтобы подчеркнуть, что, когда подпись прикладывается к документу, целостность документа и целостность подписи настолько тесно взаимосвязаны, что отделить одно из этих понятий от другого весьма сложно. В тех случаях, когда подпись используется для подписания документа, идея целостности документа непреложно вытекает из использования подписи. В то же время было принято решение о том, что в Типовом законе необходимо следовать разграничению, проводимому между статьями 7 и 8 Типового закона ЮНСИТРАЛ об электронной торговле. Хотя некоторые технологии предусматривают как удостоверение подлинности (статья 7

Типового закона ЮНСИТРАЛ об электронной торговле), так и обеспечение целостности (статья 8 Типового закона ЮНСИТРАЛ об электронной торговлей), эти понятия можно рассматривать в качестве отдельных правовых понятий и предусмотреть их регулирование в качестве таковых. Поскольку собственноручная подпись не обеспечивает ни гарантии целостности документа, к которому она прилагается, ни гарантии того, что любое внесенное в этот документ изменение можно будет обнаружить, то согласно функционально-эквивалентному подходу требуется, чтобы эти понятия рассматривались не в одном, а в разных положениях. Цель пункта 3(c) состоит в том, чтобы установить критерий, который должен быть выполнен, с тем чтобы продемонстрировать, что тот или иной конкретный метод электронного подписания является достаточно надежным для удовлетворения законодательного требования о подписи. Это законодательное требование может быть удовлетворено без необходимости доказывания целостности всего документа (см. документ A/CN.9/467, пункты 72–80).

Функциональный эквивалент подлинного документа

124. Подпункт (d) предназначен для использования в первую очередь в тех странах, где действуют регулирующие использование собственноручных подписей правовые нормы, которые не могут учитывать различия между целостностью подписи и целостностью подписываемой информации. В других странах в силу подпункта (d) может быть создана подпись, которая будет более надежной, чем собственноручная подпись, и, таким образом, будет иметь место выход за рамки понятия функционального эквивалента подписи. При любых обстоятельствах в силу подпункта (d) будет создаваться функциональный эквивалент подлинного документа.

Электронное подписание части сообщения

125. В подпункте (d) оговаривается необходимая связь между подписью и подписываемой информацией, с тем чтобы избежать создания впечатления о том, что электронная подпись может прилагаться только к полному содержанию сообщения данных. На практике подписываемая информация будет во многих случаях являться лишь частью информации, содержащейся в сообщении данных. Например, электронная подпись может относиться только к информации, прилагаемой к сообщению для целей передачи.

Изменение по договоренности

126. Пункт 3 не преследует цели ограничить применение статьи 5 или любых норм применимого права, признающих свободу сторон оговаривать в любом соответствующем соглашении, что тот или иной конкретный метод подписания будет рассматриваться в отношениях между ними в качестве надежного эквивалента собственноручной подписи.

Справочные документы ЮНСИТРАЛ

A/CN.9/467, пункты 44–87;
A/CN.9/WG.IV/WP.84, пункты 41–47;
A/CN.9/465, пункты 62–82;
A/CN.9/WG.IV/WP.82, пункты 42–44;
A/CN.9/457, пункты 48–52;
A/CN.9/WG.IV/WP.80, пункты 11–12.

Статья 7. Удовлетворение требований статьи 6

1) [*Любое лицо, орган или ведомство, будь то публичное или частное, назначенное принимающим государством в качестве компетентного лица, органа или ведомства*] может определять, какие электронные подписи удовлетворяют требованиям статьи 6.

2) Любое определение, вынесенное в соответствии с пунктом 1, должно соответствовать признанным международным стандартам.

3) Ничто в настоящей статье не затрагивает действия норм международного частного права.

Предварительное определение статуса электронной подписи

127. В статье 7 оговаривается роль, которую играет государство, принимающее Типовой закон, в создании или признании какого-либо субъекта, который может придавать силу использованию электронных подписей или иным образом сертифицировать их качество. Как и статья 6, статья 7 основывается на идее о том, что для содействия развитию электронной торговли необходимы определенность и предсказуемость в момент, когда коммерческие стороны используют методы электронного подписания, а не в момент рассмотрения споров в суде. В тех случаях, когда тот или иной конкретный метод подписания может удовлетворять требованиям о высокой степени надежности и безопасности, должно существовать средство для оценки технических аспектов надежности и безопасности и предоставления методам подписания той или иной формы признания.

Цель статьи 7

128. Цель статьи 7 состоит в том, чтобы четко установить, что принимающее государство может назначить орган или ведомство, которые будут иметь полномочия определять, на какие конкретные технологии могут распространяться презумпции или материально-правовые нормы, устанавливаемые согласно статье 6. Статья 7 не является положением, создающим какие-либо конкретные права, и она необязательно должна приниматься государствами в ее нынешнем виде. В то же время ее цель состоит в том, чтобы четко передать мысль о том, что определенность и предсказуемость могут быть достигнуты с помощью определения того, какие методы электронного подписания удовлетворяют критериям надежности статьи 6, при условии, что такое определение выносится в соответствии с международными стандартами. Статью 7 не следует толковать таким образом, который будет либо предписывать императивные правовые последствия использования определенных методов подписания, либо будет ограничивать использование технических средств теми методами, которые определены в качестве удовлетворяющих требованиям надежности статьи 6. Например, стороны должны сохранять свободу использовать те методы, которые не были определены в качестве удовлетворяющих статье 6, если они договорились об этом. Они должны также сохранять свободу доказывать в суде или в третейском суде, что метод подписания, избранный ими для использования, удовлетворяет требованиям статьи 6, даже несмотря на то, что соответствующего определения в отношении этого метода заранее вынесено не было.

Пункт 1

129. В пункте 1 четко устанавливается, что любой субъект, который может придать силу использованию электронных подписей или иным образом сертифицировать их качество, необязательно должен быть создан в качестве государственного ведомства. Пункт 1 не следует толковать в качестве рекомендации государствам в отношении единственного пути обеспечения признания технологии подписания, а скорее в качестве указания на те ограничения, которые должны применяться в случае, если государства пожелают использовать такой подход.

Пункт 2

130. Что касается пункта 2, то понятие "стандарт" не должно ограничиваться официальными стандартами, разработанными, например, Международной организацией по стандартизации (МОС) и Целевой инженерной группой по Интернет (ЦИГИ) или другими техническими стандартами. Слово "стандарты" следует толковать в широком смысле, который будет охватывать отраслевую практику и торговые обычаи, тексты, подготовленные такими международными организациями, как Международная торговая палата, а также работу самой ЮНСИТРАЛ (включая настоящий Типовой закон и Типовой закон ЮНСИТРАЛ об электронной торговле). Возможное отсутствие соответствующих стандартов не должно препятствовать компетентным лицам или властям выносить определение, о котором говорится в пункте 1. Что касается ссылки на "признанные" стандарты, то может возникнуть вопрос о том, что подразумевается под понятием "признание" и от кого будет требоваться такое признание (см. документ A/CN.9/465, пункт 94). Этот вопрос также рассматривается в связи со статьей 12 (см. ниже, пункт 154).

Пункт 3

131. Пункт 3 направлен на то, чтобы самым четким образом указать, что статья 7 не преследует цели затронуть обычное действие норм международного частного права (см. документ A/CN.9/467, пункт 94). В отсутствие такого положения статья 7 может неверно истолковаться как побуждающая государства, принимающие Типовой закон, к установлению дискриминационного режима в отношении иностранных электронных подписей на основании несоблюдения правил, утвержденных соответствующим лицом или органом согласно пункту 1.

Справочные документы ЮНСИТРАЛ

A/CN.9/467, пункты 90–95;
A/CN.9/WG.IV/WP.84, пункты 49–51;
A/CN.9/465, пункты 90–98;
A/CN.9/WG.IV/WP.82, пункт 46;
A/CN.9/457, пункты 48–52;
A/CN.9/WG.IV/WP.80, пункт 15.

Статья 8. Поведение подписавшего

1) В тех случаях, когда данные для создания подписи могут быть использованы для создания подписи, имеющей юридическую силу, каждый подписавший обязан:

a) проявлять разумную осмотрительность для недопущения несанкционированного использования его данных для создания подписи;

b) без неоправданных задержек уведомлять любое лицо, которое, как подписавший может разумно предполагать, полагается на электронную подпись или предоставляет услуги в связи с ней, если:

i) подписавшему известно, что данные для создания подписи были скомпрометированы; или
ii) обстоятельства, известные подписавшему, обусловливают существенный риск того, что данные для создания подписи могли быть скомпрометированы;

c) в тех случаях, когда для подтверждения электронной подписи используется сертификат, проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от подписавшего существенных заверений, которые относятся к жизненному циклу сертификата или которые должны быть включены в сертификат.

2) Подписавший несет ответственность за невыполнение требований пункта 1.

Название

132. Первоначально планировалось включить в статью 8 (и в статьи 9 и 11) нормы, касающиеся обязательств и ответственности различных заинтересованных сторон (подписавшего, полагающейся стороны и поставщика сертификационных услуг). Однако быстрый прогресс, затрагивающий технические и коммерческие аспекты электронной торговли, а также та роль, которую в ряде стран в настоящее время играет саморегулирование в области электронной торговли, затруднили достижение консенсуса относительно содержания подобных норм. Эти статьи были подготовлены в качестве положений, устанавливающих минимальный "кодекс поведения" различных сторон. Последствия несоблюдения этого кодекса поведения оставлены на урегулирование на основании применимого права за пределами Типового закона.

Пункт 1

133. Подпункты (a) и (b) в целом применимы ко всем электронным подписям, а подпункт (c) применяется только в отношении тех электронных подписей, которые подтверждены сертификатом. В частности, устанавливаемое в пункте 1(a) обязательство проявлять разумную осмотрительность для недопущения несанкционированного использования данных для создания подписи представляет собой базовое обязательство, которое, например, как правило, включается в соглашения относительно использования кредитных карт. В соответствии с принципом, закрепляемым в пункте 1, такое обязательство должно также распространяться на любые данные для создания электронной подписи, которые могут использоваться для цели выражения юридически значимого намерения. В то же время положение об изменении по договоренности, содержащееся в статье 5, позволяет изменять устанавливаемые в статье 8 стандарты в тех областях, в которых они будут сочтены неуместными или приведут к незапланированным последствиям.

134. В пункте 1(b) используется понятие "лица, которое, как подписавший может разумно предполагать, полагается на электронную подпись или предоставляет услуги в связи с ней". В зависимости от используемой технологии такой "полагающейся стороной" может быть не только лицо, которое может намереваться положиться на подпись, но и такие лица, как поставщик сертификационных услуг, поставщик услуг по аннулированию сертификатов и другая заинтересованная сторона.

135. Пункт 1(c) применяется в тех случаях, когда для подтверждения данных для создания подписи используется сертификат. Предполагается, что понятие "жизненный цикл сертификата" будет толковаться широко – как охватывающее период, начинающийся с подачи заявки на получение сертификата или создания сертификата и заканчивающийся в момент истечения срока действия сертификата или его аннулирования.

Пункт 2

136. В пункте 2 не оговариваются ни последствия, ни пределы ответственности: эти вопросы оставлены на урегулирование на основании национального права. В то же время, несмотря на то что последствия наступления ответственности оставлены на урегулирование на основании национального права, пункт 2 дает ясное указание государствам, принимающим Типовой закон, на то, что невыполнение обязательств, установленных в пункте 1, должно влечь за собой наступление ответственности. Пункт 2 основывается на сделанном Рабочей группой на ее тридцать пятой сессии выводе о том, что достижение консенсуса относительно конкретных последствий, которые могут вытекать из ответственности обладателя данных для создания подписи, может вызвать трудности. В зависимости от контекста использования электронной подписи такие последствия, согласно действующим правовым нормам, могут простираться от установления такого порядка, при котором обладатель данных для создания подписи будет связан содержанием сообщения, до установления ответственности за возмещение убытков. Соответственно, в пункте 2 просто закрепляется принцип, согласно которому обладатель данных для создания подписи должен нести ответственность за несоблюдение требований пункта 1, а вопрос урегулирования правовых последствий, которые будут вытекать из наступления такой ответственности, оставлен для урегулирования на основании права каждого принимающего государства, применимого за пределами Типового закона (A/CN.9/465, пункт 108).

Справочные документы ЮНСИТРАЛ

A/CN.9/467, пункты 96–104;
A/CN.9/WG.IV/WP.84, пункты 52–53;
A/CN.9/465, пункты 99–108;
A/CN.9/WG.IV/WP.82, пункты 50–55;
A/CN.9/457, пункты 65–98;
A/CN.9/WG.IV/WP.80, пункты 18–19.

Статья 9. Поведение поставщика сертификационных услуг

1) В тех случаях, когда поставщик сертификационных услуг предоставляет услуги для подкрепления электронной подписи, которая может быть использована в качестве подписи, имеющей юридическую силу, такой поставщик сертификационных услуг:

a) действует в соответствии с заверениями, которые он делает в отношении своей политики и практики;

b) проявляет разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений, которые относятся к жизненному циклу сертификата или которые включены в сертификат;

c) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить по сертификату:

i) личность поставщика сертификационных услуг;
ii) что подписавший, который идентифицирован в сертификате, имел контроль над данными для создания подписи в момент выдачи сертификата;
iii) что данные для создания подписи были действительными в момент или до момента выдачи сертификата;

d) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить, соответственно, по сертификату или иным образом:

i) метод, использованный для идентификации подписавшего;
ii) любые ограничения в отношении целей или стоимостного объема, в связи с которыми могут использоваться данные для создания подписи или сертификат;
iii) что данные для создания подписи являются действительными и не были скомпрометированы;
iv) любые ограничения в отношении масштаба или объема ответственности, оговоренные поставщиком сертификационных услуг;
v) существуют ли средства для направления подписавшим уведомления в соответствии со статьей 8(1)(b);
vi) предлагается ли услуга по своевременному аннулированию;

e) в тех случаях, когда предлагаются услуги, предусмотренные в подпункте (d) (v), обеспечивает подписавшего средствами для направления уведомления в соответствии со статьей 8(1)(b), и в тех случаях, когда предлагаются услуги, предусмотренные в подпункте (d) (vi), обеспечивает наличие услуг по своевременному аннулированию;

f) использует надежные системы, процедуры и людские ресурсы при предоставлении своих услуг.

2) Поставщик сертификационных услуг несет ответственность за невыполнение требований пункта 1.

Пункт 1

137. В подпункте (a) закрепляется базовая норма, состоящая в том, что поставщик сертификационных услуг должен соблюдать заверения и обязательства,

которые он сделал или принял на себя, например в заявлении о практике сертификации или в любом другом заявлении о принципах функционирования. В подпункте (b) воспроизводится стандарт проведения, установленный в статье 8(1)(c) в отношении подписавшего, применительно к контексту функционирования поставщика сертификационных услуг.

138. В подпункте (c) определяются основное содержание и ключевые последствия любого сертификата в соответствии с Типовым законом. В подпункте (d) перечисляются дополнительные элементы, подлежащие включению в сертификат или иным образом предоставляемые в распоряжение полагающейся стороны или доступные для нее, в тех случаях, когда эти элементы будут необходимы для того или иного конкретного сертификата. Подпункт (e) не предназначен для применения к таким сертификатам, как сертификаты на отдельные сделки, являющиеся одновременными сертификатами, или к недорогостоящим сертификатам для использования в ситуациях, не связанных со значительным риском, применительно к которым аннулирование может и не предусматриваться.

139. Вполне можно считать, что выполнения обязанностей и обязательств, установленных в статье 9, можно разумно ожидать от любого поставщика сертификационных услуг, а не только от тех поставщиков, которые выдают "дорогостоящие" сертификаты. Однако авторы Типового закона постарались не требовать от подписавшего или поставщика сертификационных услуг проявления той степени предусмотрительности или надежности, какая не имеет разумного отношения к целям, в которых используется электронная подпись или сертификат. Таким образом, Типовой закон предусматривает решение, которое увязывает обязательства, установленные в статьях 8 и 9, с созданием юридически значимых электронных подписей (A/CN.9/483, пункт 117). Ограничивая сферу применения статьи 9 целым рядом ситуаций, в которых сертификационные услуги предоставляются для подкрепления электронной подписи, которая может быть использована в качестве подписи, имеющей юридическую силу, Типовой закон не направлен на создание новых категорий правовых последствий для подписей (там же, пункт 119).

Пункт 2

140. В пункте 2 воспроизводится базовая норма ответственности, устанавливаемая в статье 8(2) в отношении подписавшего. В результате включения этого положения определение последствий ответственности оставлено на усмотрение национального права. Авторы формулировки пункта 2, которая применяется с учетом применимых норм национального права, не преследовали цели подготовки такого положения, которое толковалось бы в качестве нормы, устанавливающей абсолютную ответственность. Отнюдь не предполагалось, что в результате действия пункта 2 будет создан такой порядок, при котором будет исключаться возможность для поставщика сертификационных услуг доказать, например, отсутствие вины или небрежности, способствовавшей причинению ущерба.

141. Первые проекты статьи 9 содержали дополнительный пункт, в котором рассматривались последствия ответственности, устанавливаемой в пункте 2. В ходе подготовки Типового закона было отмечено, что поставщики сертификационных услуг выполняют посреднические функции, которые являются жизненно важными для электронной торговли, и что вопрос об ответственности таких лиц,

оказывающих профессиональные услуги, не может быть удовлетворительно решен путем принятия одного положения, аналогичного пункту 2. Хотя в пункте 2, по всей вероятности, устанавливается надлежащий принцип применительно к подписавшим, он, возможно, не является достаточным для охватываемых статьей 9 видов профессиональной и коммерческой деятельности. Один из путей устранения этого недостатка мог бы заключаться в перечислении в тексте Типового закона тех факторов, которые следует учитывать при оценке любого ущерба, причиненного в результате невыполнения поставщиком сертификационных услуг требований пункта 1. В конечном итоге было решено включить в настоящее Руководство неисчерпывающий перечень примерных факторов. При оценке ущерба во внимание принимаются в том числе следующие факторы: a) затраты на получение сертификата; b) характер сертифицируемой информации; c) наличие и степень любого ограничения цели, для которой может использоваться сертификат; d) наличие любого заявления, ограничивающего масштаб или степень ответственности поставщика сертификационных услуг; и e) любое действие полагающейся стороны, способствовавшее причинению ущерба.

Справочные документы ЮНСИТРАЛ

A/CN.9/483, пункты 114–127;
A/CN.9/467, пункты 105–129;
A/CN.9/WG.IV/WP.84, пункты 54–60;
A/CN.9/465, пункты 123–142 (проект статьи 12);
A/CN.9/WG.IV/WP.82, пункты 59–68 (проект статьи 12);
A/CN.9/457, пункты 108–119;
A/CN.9/WG.IV/WP.80, пункты 22–24.

Статья 10. Надежность

Для целей статьи 9(1)(f) при определении того, являются ли – или в какой мере являются – любые системы, процедуры и людские ресурсы, используемые поставщиком сертификационных услуг, надежными, могут учитываться следующие факторы:

a) финансовые и людские ресурсы, в том числе наличие активов;

b) качество систем аппаратного и программного обеспечения;

c) процедуры для обработки сертификатов и заявок на сертификаты и хранения записей;

d) наличие информации для подписавших, идентифицированных в сертификатах, и для потенциальных полагающихся сторон;

e) регулярность и объем аудита, проводимого независимым органом;

f) наличие заявления, сделанного государством, аккредитующим органом или поставщиком сертификационных услуг в отношении соблюдения или наличия вышеуказанного; или

g) любые другие соответствующие факторы.

Гибкость понятия "надежность"

142. Первоначально статья 10 разрабатывалась как часть статьи 9. Хотя впоследствии эта часть была выделена в отдельную статью, ее цель в первую очередь заключается в том, чтобы содействовать толкованию понятия "надежные системы, процедуры и людские ресурсы" в статье 9(1)(f). Статья 10 является неисчерпывающим перечнем факторов, которые следует принимать во внимание при определении надежности. Цель этого перечня заключается в том, чтобы установить гибкое понятие "надежности", содержание которого может изменяться в зависимости от ожиданий, связанных с сертификатом в контексте, в котором он был создан.

Справочные документы ЮНСИТРАЛ

A/CN.9/483, пункты 128–133;
A/CN.9/467, пункты 114–119.

Статья 11. Поведение полагающейся стороны

Полагающаяся сторона несет правовые последствия в случае:

a) непринятия ею разумных мер для проверки надежности электронной подписи; или

b) когда электронная подпись подкрепляется сертификатом, непринятия ею разумных мер:

i) для проверки действительности, приостановления действия или аннулирования сертификата; и
ii) для соблюдения любых ограничений в отношении сертификата.

Разумность доверия

143. В статье 11 отражена идея о том, что сторона, которая намеревается полагаться на электронную подпись, должна учитывать вопрос о том, является ли такое доверие разумным с учетом обстоятельств и в какой мере оно таковым является. Это положение не преследует цели урегулировать вопрос о действительности электронной подписи, который разрешается согласно статье 6 и который не должен зависеть от поведения полагающейся стороны. Вопрос о действительности электронной подписи должен быть отделен от вопроса о том, является ли разумным поведение полагающейся стороны, которая полагается на подпись, не удовлетворяющую стандарту, установленному в статье 6.

Вопросы, связанные с потребителями

144. Хотя статья 11 может налагать определенное бремя на полагающиеся стороны, особенно в тех случаях, когда такими сторонами являются потребители, следует напомнить о том, что Типовой закон не преследует цели создания преимущественного порядка по сравнению с любыми нормами, регулирующими вопросы защиты потребителей. Однако Типовой закон может сыграть полезную

роль в предоставлении всем заинтересованным сторонам, включая полагающиеся стороны, информации относительно стандарта разумного поведения, который необходимо соблюдать в отношении электронных подписей. Кроме того, установление стандарта поведения, согласно которому полагающаяся сторона должна проверить надежность подписи с помощью имеющихся в ее распоряжении доступных средств, может быть сочтено чрезвычайно важным для развития любой системы инфраструктуры публичных ключей.

Понятие "полагающаяся сторона"

145. Согласно его определению понятие "полагающаяся сторона" призвано охватить любую сторону, которая может полагаться на электронную подпись. Таким образом, в зависимости от обстоятельств "полагающейся стороной" может быть любое лицо, имеющее или не имеющее договорные отношения с подписавшим или поставщиком сертификационных услуг. Можно даже представить себе ситуацию, когда "полагающейся стороной" будет сам поставщик сертификационных услуг или подписавший. Однако широкое понятие "полагающейся стороны" не должно приводить к возложению на абонента сертификата обязательства проверять действительность сертификата, который он приобретает у поставщика сертификационных услуг.

Несоблюдение требований статьи 11

146. В качестве возможного последствия установления общего обязательства, согласно которому полагающаяся сторона должна проверять действительность электронной подписи или сертификата, возникает вопрос о той ситуации, которая может возникнуть в случае несоблюдения полагающейся стороной требований статьи 11. Если полагающаяся сторона не выполнит эти требования, она должна быть лишена возможности воспользоваться к своей выгоде подписью или сертификатом, если разумная проверка показала бы, что подпись или сертификат являются недействительными. Эту ситуацию, возможно, потребуется урегулировать на основании права, применимого за пределами Типового закона.

Справочные документы ЮНСИТРАЛ

A/CN.9/467, пункты 130–143;
A/CN.9/WG.IV/WP.84, пункты 61–63;
A/CN.9/465, пункты 109–122 (проекты статей 10 и 11);
A/CN.9/WG.IV/WP.82, пункты 56–58 (проекты статей 10 и 11);
A/CN.9/457, пункты 99–107;
A/CN.9/WG.IV/WP.80, пункты 20–21.

Статья 12. Признание иностранных сертификатов и электронных подписей

1) При определении того, обладает ли – или в какой мере обладает – сертификат или электронная подпись юридической силой, не учитываются:

a) место выдачи сертификата или создания или использования электронной подписи, или

b) местонахождение коммерческого предприятия эмитента или подписавшего.

2) Сертификат, выданный за пределами [*принимающее государство*], обладает такой же юридической силой в [*принимающее государство*], как и сертификат, выданный в [*принимающее государство*], если он обеспечивает по существу эквивалентный уровень надежности.

3) Электронная подпись, созданная или используемая за пределами [*принимающее государство*], обладает такой же юридической силой в [*принимающее государство*], как и электронная подпись, созданная или используемая в [*принимающее государство*], если она обеспечивает по существу эквивалентный уровень надежности.

4) При определении того, обеспечивает ли сертификат или электронная подпись по существу эквивалентный уровень надежности для целей пункта 2 или 3, следует учитывать признанные международные стандарты и любые другие соответствующие факторы.

5) В тех случаях, когда, независимо от положений пунктов 2, 3 и 4, стороны договариваются между собой в отношении использования определенных видов электронных подписей или сертификатов, такая договоренность признается достаточной для цели трансграничного признания, за исключением случаев, когда такая договоренность не будет действительной или не будет иметь правовых последствий согласно применимому праву.

Общее правило о недискриминации

147. Пункт 1 призван отразить основополагающий принцип, согласно которому одно лишь место происхождения никоим образом не является фактором, определяющим, следует ли и в какой степени следует признавать иностранные сертификаты и электронные подписи обладающими юридической силой. Определение того, обладает ли – или в какой мере обладает – сертификат или электронная подпись юридической силой, должно зависеть не от места выдачи сертификата или создания электронной подписи (см. документ A/CN.9/483, пункт 27), а от его технической надежности.

"по существу эквивалентный уровень надежности"

148. Цель пункта 2 заключается в том, чтобы предусмотреть общий критерий для трансграничного признания сертификатов, без которого поставщики сертификационных услуг могут нести неразумное бремя, будучи вынуждены получать лицензии во многих странах. Для этой цели пункт 2 устанавливает пороговый уровень технического соответствия иностранных сертификатов, основанный на сопоставлении степени их надежности в сравнении с требованиями в отношении надежности, установленными принимающим государством согласно Типовому закону (там же, пункт 31). Этот критерий должен применяться независимо от характера процедуры сертификации в рамках правовой системы, где был выдан сертификат или сделана подпись (там же, пункт 29).

Уровень надежности, разнящийся в каждой правовой системе

149. Посредством ссылки на центральное понятие "по существу эквивалентного уровня надежности" пункт 2 признает, что могут существовать значительные

различия в отдельных правовых системах. Требование эквивалентности, установленное в пункте 2, не означает, что уровень надежности иностранного сертификата должен быть абсолютно идентичным уровню надежности внутреннего сертификата (там же, пункт 32).

Уровень надежности, разнящийся в пределах правовой системы

150. Кроме того, следует отметить, что на практике поставщики сертификационных услуг выдают сертификаты с различным уровнем надежности в зависимости от целей, для которых их клиенты предполагают использовать такие сертификаты. С учетом своего относительного уровня надежности отнюдь не все сертификаты могут иметь юридическую силу внутри данной страны или за ее пределами. В связи с этим при применении понятия эквивалентности, как оно используется в пункте 2, следует учитывать, что эквивалентность должна устанавливаться между сертификатами аналогичного вида. Однако в Типовом законе не была предпринята попытка установить соответствие между сертификатами различных видов, выдаваемыми различными поставщиками сертификационных услуг в различных правовых системах. Типовой закон был разработан таким образом, чтобы предусмотреть возможность иерархии различных видов сертификатов. На практике суд или третейский суд, которому необходимо принять решение о юридической силе иностранного сертификата, как правило, будет рассматривать каждый сертификат по существу, стремясь сопоставить его с наиболее соответствующим уровнем в принимающем государстве (там же, пункт 33).

Равный статус сертификатов и других видов электронных подписей

151. Пункт 3 устанавливает в отношении электронных подписей такую же норму, как и норма, установленная в пункте 2 в отношении сертификатов (там же, пункт 41).

Признание определенной юридической силы в результате соблюдения законодательства иностранного государства

152. Пункты 2 и 3 касаются исключительно критерия трансграничной надежности, который должен использоваться при оценке надежности иностранного сертификата или электронной подписи. Однако в ходе разработки Типового закона учитывалось, что принимающие его государства могут пожелать исключить необходимость проверки надежности конкретных подписей или сертификатов, когда принимающее государство удостоверилось в том, что законодательство страны происхождения подписи или сертификата обеспечивает надлежащий стандарт надежности. Что касается правовых методов возможного заблаговременного признания надежности сертификатов и подписей, отвечающих законодательству иностранного государства, принимающим государством (например, одностороннее заявление или международный договор), то Типовой закон не содержит какого-либо конкретного предложения на этот счет (там же, пункты 39 и 42).

Факторы, которые следует учитывать при оценке эквивалентности иностранных сертификатов и подписей по существу

153. В ходе разработки Типового закона пункт 4 первоначально был сформулирован как перечень факторов, которые следует учитывать при определении того, обеспечивает ли сертификат или подпись по существу

эквивалентный уровень надежности для целей пункта 2 или 3. Позднее обнаружилось, что большинство этих факторов уже перечислены в статьях 6, 9 и 10. Повторное изложение этих факторов в контексте статьи 12 было бы излишним. В качестве альтернативного варианта включение в пункт 4 перекрестных ссылок на соответствующие положения Типового закона, в которых упоминаются соответствующие критерии, возможно с добавлением других критериев, особенно важных для трансграничного признания, имело бы своим результатом разработку слишком сложной формулировки (см., в частности, документ A/CN.9/483, пункты 43–49). В конечном счете в пункт 4 была включена неконкретная ссылка на "любые соответствующие факторы", в числе которых факторы, перечисленные в статьях 6, 9 и 10 и относящиеся к оценке внутренних сертификатов и электронных подписей, являются особенно важными. Кроме того, в пункте 4 учитываются последствия существования того факта, что оценка эквивалентности иностранных сертификатов несколько отличается от оценки надежности поставщика сертификационных услуг согласно статьям 9 и 10. С учетом этого в пункт 4 была добавлена ссылка на "признанные международные стандарты".

Признанные международные стандарты

154. Понятие "признанный международный стандарт" следует толковать широко – как охватывающее международные технические и коммерческие стандарты (т. е. существующие на рынке стандарты), а также стандарты и нормы, принятые правительственными или межправительственными органами (там же, пункт 49). "Признанным международным стандартом" может быть изложение принятых видов технической, правовой и коммерческой практики, будь то разработанных государственным или частным сектором (или обоими секторами), нормативного или толковательного характера, которые являются общепризнанными как международно-применимые. Такие стандарты могут иметь форму требований, рекомендаций, руководящих принципов, кодексов поведения или изложения наилучших видов практики или норм (там же, пункты 101–104).

Признание договоренностей между заинтересованными сторонами

155. Пункт 5 предусматривает признание договоренностей между заинтересованными сторонами в отношении использования определенных видов электронных подписей или сертификатов в качестве достаточных для цели трансграничного признания (между этими сторонами) таких согласованных подписей или сертификатов (там же, пункт 54). Следует отметить, что согласно статье 5 пункт 5 этой статьи не предназначен для замены любых императивных норм права, в частности любого императивного требования в отношении собственноручных подписей, которые принимающие государства могут пожелать сохранить в применимом праве (там же, пункт 113). Пункт 5 необходим для придания силы договорным положениям, которые стороны могут согласовать между собой, о признании использования определенных видов электронных подписей или сертификатов (которые могут рассматриваться как иностранные в некоторых или во всех государствах, где стороны могут добиваться правового признания таких подписей или сертификатов) без проверки этих подписей или сертификатов на предмет эквивалентности по существу, предусмотренной пунктами 2, 3 и 4. Пункт 5 не затрагивает правового положения третьих сторон (там же, пункт 56).

Справочные документы ЮНСИТРАЛ

A/CN.9/483, пункты 25–58 (статья 12);
A/CN.9/WG.IV/WP.84, пункты 61–68 (проект статьи 13);
A/CN.9/465, пункты 21–35;
A/CN.9/WG.IV/WP.82, пункты 69–71;
A/CN.9/454, пункт 173;
A/CN.9/446, пункты 196–207 (проект статьи 19);
A/CN.9/WG.IV/WP.73, пункт 75;
A/CN.9/437, пункты 74–89 (проект статьи I);
A/CN.9/WG.IV/WP.71, пункты 73–75.

Примечания

[1] *Официальные отчеты Генеральной Ассамблеи, пятьдесят первая сессия, Дополнение № 17* (A/51/17), пункты 223–224.

[2] Там же, *пятьдесят вторая сессия, Дополнение № 17* (A/52/17), пункты 249–251.

[3] *Официальные отчеты Генеральной Ассамблеи, пятьдесят первая сессия, Дополнение № 17* (A/51/17), пункты 223–224.

[4] Там же, *пятьдесят вторая сессия, Дополнение № 17* (A/52/17), пункты 249–251.

[5] Там же, *пятьдесят третья сессия, Дополнение № 17* (A/53/17), пункты 207–211.

[6] Там же, *пятьдесят четвертая сессия, Дополнение № 17* (A/54/17), пункты 308–314.

[7] Там же, *пятьдесят пятая сессия, Дополнение № 17* (A/55/17), пункты 380–383.

[8] Этот раздел взят из документа A|CN.9/WG.IV/WP.71, часть I.

[9] Многочисленные элементы описания порядка функционирования системы подписей в цифровой форме в этом разделе основываются на Руководящих принципах, касающихся подписей в цифровой форме, разработанных Американской ассоциацией адвокатов (ABA Digital Signature Guidelines, pp. 8-17).

[10] Некоторые существующие стандарты, такие как Руководящие принципы, касающиеся подписей в цифровой форме, которые были разработаны Американской ассоциацией адвокатов, содержат ссылку на понятие "вычислительной невозможности" при описании предполагаемой необратимости этого процесса, т. е. отражают надежду на то, что невозможно установить тайный частный ключ пользователя на основании его публичного ключа. «"Вычислительная невозможность" является относительным понятием, основывающимся на ценности защищаемых данных, расходах на исчисления необходимых для защиты этих данных, продолжительности времени, в течение которого их необходимо защищать, и на затратах и времени, необходимых для неправомерного получения этих данных, причем эти факторы оцениваются как с точки зрения настоящего времени, так и с учетом будущего технического прогресса» (ABA Digital Signature Guidelines, p. 9, note 23).

[11] В случаях, когда публичные и частные криптографические ключи выдаются самими пользователями, может потребоваться, чтобы такая уверенность была обеспечена органами, сертифицирующими публичные ключи.

[12] Вопрос о том, должно ли правительство располагать техническими возможностями для хранения или воссоздания частных ключей, используемых для обеспечения конфиденциальности, может быть решен на уровне базового органа.

[13] Однако в контексте перекрестной сертификации необходимость обеспечения глобального взаимодействия требует, чтобы ИПК, созданные в различных странах, были в состоянии соотноситься друг с другом.