Организация Объединенных Наций A/CN.9/WG.IV/WP.86

Генеральная Ассамблея

Distr.: Limited
18 August 2000

Russian
Original: English

Комиссия Организации Объединенных Наций по праву международной торговли

Рабочая группа по электронной торговле
Тридцать седьмая сессия
Вена, 18–29 сентября 2000 года

Электронные подписи

Проект руководства по принятию единообразных правил 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 шестую сессии подготовке проекта единообразных правил ЮНСИТРАЛ об электронных подписях (далее в тексте – "единообразные правила"). Доклады о работе этих сессий содержатся в документах A/CN.9/437, 446, 454, 457, 465 и 467. При подготовке единообразных правил Рабочая группа отметила, что было бы полезно представить в комментарии дополнительную информацию относительно единообразных правил. С учетом подхода, использованного при разработке Типового закона ЮНСИТРАЛ об электронной торговле, была выражена общая поддержка предложению о подготовке сопровождающего проект единообразных правил руководства с целью предоставления помощи государствам в деле принятия и применения единообразных правил. Это руководство, которое в значительной степени может основываться на подготовительных материалах, использованных в ходе работы над единообразными правилами, было бы также полезным и для других пользователей единообразных правил.

2. На своей тридцать шестой сессии Рабочая группа обсудила тему электронных подписей на основе записки, подготовленной Секретариатом (A/CN.9/WG.IV/WP.84). После обсуждения Рабочая группа утвердила содержание проектов статьей 1 и 3–11 единообразных правил и передала их в редакционную группу для обеспечения соответствия между различными положениями единообразных правил. Секретариату было предложено подготовить проект

руководства по принятию утвержденных положений. При условии одобрения Комиссией, Рабочая группа рекомендовала, чтобы проекты статей 2 и 13 единообразных правил вместе с руководством по принятию были рассмотрены Рабочей группой на одной из будущих сессий[3].

3. На своей тридцать третьей сессии (июнь-июль 2000 года) Комиссия отметила, что Рабочая группа на ее тридцать шестой сессии приняла текст проектов статей 1 и 3–11 единообразных правил. Было указано, что некоторые вопросы по-прежнему нуждаются в разъяснении, поскольку Рабочая группа приняла решение исключить из 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 создания 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 юридических последствий.

4. После обсуждения Комиссия выразила признательность Рабочей группе за ее усилия и прогресс, достигнутый в разработке 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[4].

5. В приложении к настоящей записке содержатся часть первая и глава I части второй подготовленного Секретариатом проекта руководства. Глава II части второй содержится в документе A/CN.9/WG.IV/WP.86/Add.1.

Приложение

ЕДИНООБРАЗНЫЕ ПРАВИЛА ЮНСИТРАЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

И

РУКОВОДСТВО ПО ПРИНЯТИЮ

2001 год

СОДЕРЖАНИЕ

Часть первая

ЕДИНООБРАЗНЫЕ ПРАВИЛА ЮНСИТРАЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ (2001 ГОД)

Проекты статей 1 и 3-11 единообразных правил ЮНСИТРАЛ об электронных подписях (2001 год)

(как они приняты Рабочей группой ЮНСИТРАЛ по электронной торговле на ее тридцать шестой сессии, проведенной в Нью-Йорке 14-25 февраля 2000 года)

Статья 1. Сфера применения

Настоящие Правила применяются в тех случаях, когда электронные подписи используются в контексте* торговой** деятельности. Они не имеют преимущественной силы по отношению к любой правовой норме, предназначенной для защиты потребителей.

* Комиссия предлагает следующий текст для государств, которые, возможно, пожелают расширить сферу применения настоящих Правил:

"Настоящие Правила применяются 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 и концессии; совместные предприятия и другие формы промышленного или предпринимательского сотрудничества; перевозка товаров и пассажиров воздушным, морским, железнодорожным и автомобильным транспортом.

Статья 3. Равный режим для технологий создания электронных подписей

Ни одно из положений настоящих Правил, 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) настоящих Правил, или иным образом отвечает требованиям применимого права.

Статья 4. Толкование

1) При толковании настоящих Правил следует учитывать их международное происхождение и необходимость содействовать достижению единообразия в их применении и соблюдению добросовестности.

2) Вопросы, которые относятся к предмету регулирования настоящих Правил и которые прямо в них не разрешены, подлежат разрешению в соответствии с общими принципами, на которых основаны настоящие Правила.

Статья 5. Изменение по договоренности

Допускается отход от настоящих Правил или изменение их действия по договоренности за исключением случаев, когда такая договоренность не будет действительной или не будет иметь юридических последствий согласно законодательству принимающего государства [или за исключением случаев, когда настоящие Правила предусматривают иное].

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) способ создания электронной подписи в том контексте, в котором он используется, связан с автором подписи и ни с каким другим лицом;

b) способ создания электронной подписи в момент подписания находился под контролем автора подписи 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:

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

b) для 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 автора подписи

1) Каждый автор подписи обязан:

a) проявлять разумную осмотрительность для недопущения несанкционированного использования его подписывающего устройства;

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

i) автору подписи известно, что подписывающее устройство было скомпрометировано; или

ii) обстоятельства, известные автору подписи, обусловливают существенный риск того, что подписывающее устройство могло быть скомпрометировано;

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

2) Автор подписи несет ответственность за невыполнение требований пункта 1.

Статья 9. Поведение поставщика сертификационных услуг

1) 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 лицо, которое идентифицировано в сертификате, имело контроль над подписывающим устройством в момент подписания;

iii) что подписывающее устройство функционировало на дату или до даты выдачи сертификата;

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

i) метод, использованный для идентификации автора подписи;

ii) любые ограничения в отношении целей или стоимостного объема, в связи с которыми может использоваться подписывающее устройство или сертификат;

iii) что подписывающее устройство функционирует и не было скомпрометировано;

iv) любые ограничения в отношении масштаба или объема финансовой ответственности, оговоренные поставщиком сертификационных услуг;

v) существуют ли средства для направления автором подписи уведомления о том, что подписывающее устройство было скомпрометировано;

vi) предлагается ли услуга по своевременному аннулированию;

e) обеспечивает автора подписи средством для направления уведомления о том, что подписывающее устройство было скомпрометировано, и обеспечивает функционирование службы своевременного аннулирования;

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

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

[Статья 10. Надежность

При вынесении определения в отношении надежности и степени надежности любых систем, процедур и людских ресурсов учитываются 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 хранение записей;

d) наличие информации для авторов подписей, 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; и

g) любые другие соответствующие факторы.]

Статья 11. Поведение полагающейся стороны

Полагающаяся сторона несет правовые последствия в случае:

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

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

i) для проверки действительности, приостановления действия или аннулирования сертификата; и

ii) для соблюдение любых ограничений в отношении сертификата.

Часть вторая

РУКОВОДСТВО ПО ПРИНЯТИЮ ЕДИНООБРАЗНЫХ ПРАВИЛ ЮНСИТРАЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ (2001 ГОД)

Цель настоящего Руководства

1. При подготовке и принятиии единообразных правил ЮНСИТРАЛ об электронных подписях (далее в тексте – "единообразные правила") Комиссия Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ) учитывала, что единообразные правила дадут в распоряжение государств более эффективное средство для модернизации их законодательства, если исполнительным правительственным органам и законодателям будет предоставлена справочная информация и пояснения, которые могут оказать им помощь в применении единообразных правил. Комиссия также учитывала вероятность того, что единообразные правила будут применяться в ряде государств, в которых недостаточно известны методы передачи сообщений, рассматриваемые в единообразных правилах. Настоящее Руководство, которое в значительной мере основывается на подготовительных материалах, использованных в ходе работы над единообразными правилами, также предназначено для оказания помощи другим пользователям текста, таким, как судьи, арбитры, 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, использованная при подготовке единообразных правил, состояла в том, что проект единообразных правил будет сопровождаться таким руководством. Например, в отношении ряда вопросов было принято решение отказаться от их урегулирования в самих единообразных правилах, однако рассмотреть их в Руководстве, с тем чтобы государства могли бы воспользоваться соответствующими рекомендациями при принятии единообразных правил. Цель представленной в настоящем Руководстве информации состоит в том, чтобы пояснить, почему в единообразные правила были включены положения, являющиеся важнейшими базовыми нормами законодательного инструмента, предназначенного для достижения целей единообразных правил.

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[8], на которой были приняты единообразные правила, а также на обсуждениях, проведенных в Рабочей группе по электронной торговле, которая осуществляла подготовительную работу.

Глава I. Введение к единообразным правилам

I. ЦЕЛЬ И ПРОИСХОЖДЕНИЕ ЕДИНООБРАЗНЫХ ПРАВИЛ

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 могут быть названы "электронные подписи"). Опасность того, что в различных странах будут использованы различающиеся законодательные подходы к урегулированию вопросов о цифровых 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. Единообразные правила, которые разрабатывались с учетом фундаментальных принципов, лежащих в основе статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле (далее в тексте – "Типовой закон"), применительно к выполнению функции подписи в электронной среде, направлены на то, чтобы оказать помощь государствам в создании современной, унифицированной и взвешенной законодательной базы для более эффективного регулирования вопросов электронных подписей. В единообразных правилах, которые являются скромным, однако важным дополнением к Типовому закону, предлагаются практические стандарты, на основании которых может быть оценена техническая надежность электронных подписей. Кроме того, единообразные правила устанавливают связь между такой технической надежностью и юридическими последствиями, создания которых можно ожидать в случае использования какой-либо конкретной электронной подписи. Единообразные правила являются существенным дополнением к Типовому закону, поскольку в них применяется подход, согласно которому юридическая сила какого-либо конкретного способа электронного подписания может быть определена заранее (или оценена до фактического использования). Таким образом, единообразные правила преследуют 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 юридические 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. авторы подписей, полагающиеся стороны и третьи стороны – поставщики услуг), единообразные правила могут оказать помощь в развитии более согласованной коммерческой практики в "киберпространстве".

5. Цели единообразных правил, 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 предусмотренных в единообразных правилах (и Типовом законе) процедур 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. Единообразные правила являются новым дополнением к серии принятых ЮНСИТРАЛ международных документов, которые либо специально направлены на удовлетворение нужд электронной торговли или которые 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. Документом ЮНСИТРАЛ в области электронной торговли, который носит наиболее специальный характер (и, возможно, является наиболее известным), 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. Цель Типового закона 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 концепций "письменных", "подписанных" и "подлинных" документов в Типовом законе используется подход функциональной эквивалентности.

9. В период подготовки Типового закона некоторые страны приняли специальные положения для регулирования ряда аспектов электронной торговли. Однако законодательства, регулирующего всю электронную торговлю в целом, не существует. Это может привести к возникновению неопределенности относительно юридического 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 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 способствовать ограничению способности коммерческих предприятий выходить на международные рынки.

11. Кроме того, на международном уровне Типовой закон в ряде случаев может быть полезным в качестве инструмента для толкования действующих международных конвенций и других международных документов, создающих юридические препятствия для использования 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 инструментов принятие Типового закона в качестве правила толкования может представлять собой средство признания использования электронной торговли без необходимости дополнения соответствующего международного инструмента специальным протоколом.

C. История подготовки единообразных правил

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[5].

13. На 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 вопросами проблемам 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 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 юридическим 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 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. Таким образом, единообразные правила не должны препятствовать использованию других методов удостоверения подлинности. Кроме того, при решении вопросов криптографии публичных ключей в единообразных правилах, возможно, необходимо будет учесть различия в уровнях защиты и признать различные юридические 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 необходимости трансграничной сертификации[6].

15. Рабочая группа приступила к разработке единообразных правил на основе записки Секретариата (A/CN.9/WG.IV/WP.73) на своей тридцать второй сессии.

16. На тридцать первой сессии (1998 год) Комиссии был представлен доклад Рабочей группы о работе ее тридцать второй сессии (A/CN.9/446). Комиссия выразила признательность Рабочей группе за ее усилия по подготовке проекта единообразных правил об электронных подписях. 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 проект единообразных правил об электронных подписях постепенно превращается в документ, который можно будет применять на практике.

17. Комиссия вновь подтвердила принятое на ее тридцатой сессии решение относительно возможности разработки 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[7].

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 тридцать второй сессии (1999 год) Комиссии были представлены доклады Рабочей группы о работе ее тридцать третьей (июнь-июль 1998 года) и тридцать четвертой (февраль 1999 года) сессий (A/CN.9/454 и 457). Комиссия выразила признательность Рабочей группе за ее усилия по подготовке проекта единообразных правил об электронных подписях. 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 единообразные правила.

20. Было высказано мнение, 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. 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 концентрации 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 раздельных 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 первоочередного 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[8].

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 3–11 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

ситуаций, 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 юридических последствий.

24. После обсуждения Комиссия выразила признательность Рабочей группе за ее усилия и прогресс, достигнутый в разработке проекта 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[9]. *[Примечание Секретариата: данный раздел, посвященный истории подготовки единообразных правил, будет окончательно доработан и, возможно, изложен в более сжатом виде после завершения рассмотрения и принятия единообразных правил Комиссией].*

II. ЕДИНООБРАЗНЫЕ ПРАВИЛА В КАЧЕСТВЕ ИНСТРУМЕНТА УНИФИКАЦИИ ЗАКОНОДАТЕЛЬСТВА

25. Как и Типовой закон, единообразные правила представляют собой законодательный текст, рекомендуемый государствам для включения в их национальное законодательство. В отличие от международной конвенции типовые законодательные положения не требуют, чтобы принимающие их государства уведомляли 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 единообразных правил (или любого другого типового закона, являющегося результатом работы ЮНСИТРАЛ).

26. 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 единообразных правил в свои правовые системы. В целом, при принятии единообразных правил (или типового закона) рекомендуется в максимально возможной степени придерживаться единообразного текста, с тем чтобы максимально повысить прозрачность национального законодательства для его иностранных пользователей.

III. ОБЩИЕ СООБРАЖЕНИЯ ОТНОСИТЕЛЬНО ЭЛЕКТРОННЫХ ПОДПИСЕЙ[10]

A. Функции подписей

27. Статья 7 Типового закона ЮНСИТРАЛ об электронной торговле основывается на признании функций подписи в условиях использования бумажных документов. В ходе подготовки Типового закона 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; 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 единообразными правилами и статьей 7 Типового закона более подробно рассматривается ниже в пунктах 67 и 70–75 настоящего Руководства.

28. 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

29. Обсуждая вопросы о целесообразности и практической возможности подготовки единообразных правил и об определении сферы применения таких единообразных правил, ЮНСИТРАЛ изучила различные электронные способы 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.

30. Как это уже указывалось выше, 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 концентрации внимания на вопросах ИПК, состоит в том, что это позволит облегчить составление единообразных правил за счет ссылок на три функции (или роли) применительно к электронным подписям, а именно на функцию выдачи ключа (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 раздельных субъекта или же одно и то же лицо выполняет две из этих функций (например, в случаях, когда сертификационный орган также является полагающейся стороной). Уделение первоочередного внимания функциям, типичным для ИПК, а не какой-либо конкретной модели, может 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

31. 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.

32. Рабочей группе ЮНСИТРАЛ по электронной торговле в ходе подготовки единообразных правил не было представлено сколь-либо подробной информации о технических и правовых последствиях использования устройств проставления "подписей", в которых применяются иные методы, чем криптография с использованием публичных ключей. С учетом наличия достаточной предварительной информации о правовых последствиях цифровых подписей и существования законопроектов по этому вопросу в ряде стран работа ЮНСИТРАЛ концентрировалась в первую очередь на вопросах цифровых подписей, проставляемых с помощью криптографии с использованием публичных ключей.

33. В то же время ЮНСИТРАЛ стремилась выработать такие единообразные правила, которые способствовали бы использованию как цифровых подписей, так и электронных подписей в других формах. С этой целью ЮНСИТРАЛ попыталась подойти к урегулированию юридических вопросов, связанных с электронными подписями, на таком уровне, который был бы промежуточным между высоким уровнем общей применимости Типового закона и более специальными правилами, которые могут потребоваться для урегулирования вопросов, связанных с конкретными методами. В любом случае согласно принципу нейтральности Типового закона по отношению к носителям данных, единообразные правила не должны толковаться как препятствующие применению любых других методов электронного подписания, которые уже существуют или могут появиться в будущем.

2. Подписи в цифровой форме, проставляемые с помощью криптографии с использованием публичных ключей[11]

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

a) Технические понятия и терминология

i) Криптография

35. 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, "асимметрическими криптосистемами" в том случае, если они полагаются на использование асимметрических алгоритмов.

36. 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

37. 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 личный 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[12]. 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.

38. 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

39. 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 "отмечаток" 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

40. 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.

41. 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

42. 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.

43. 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 сертификационные органы

44. 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.

45. 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.

46. 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[13].

47. 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 (случай, который часто называют "нерасторжением"), если сделка окажется неблагоприятной для подразумеваемого подписывающего лица.

48. 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 единообразных правилах 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)

49. 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 следующее: 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) проверка правильности идентификации конечных пользователей и предоставление им услуг; 8) предоставление услуг в отношении нерасторжения; 9) предоставление услуг по фиксации времени передачи сообщения; 10) управление кодовыми ключами, используемыми для кодирования в целях обеспечения конфиденциальности, если применение такого метода санкционировано.

50. 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[14]; 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.

51. 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[15]. 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 единообразных правилах не рассматриваются.

ii) Поставщик сертификационных услуг

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

57. 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 отсутствии 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.

58. 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.

59. 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.

60. При подготовке единообразных правил в качестве 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

61. 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).

VI. ОСНОВНЫЕ ЧЕРТЫ ЕДИНООБРАЗНЫХ ПРАВИЛ

A. Законодательная природа единообразных правил

62. Единообразные правила были подготовлены исходя из той предпосылки, что они будут непосредственно вытекать из статьи 7 Типового закона и будут 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).

63. При разработке проекта единообразных правил обсуждался вопрос о том, в какой форме они должны быть подготовлены, 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 единообразные правила 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).

B. Взаимосвязь с Типовым законом ЮНСИТРАЛ об элетронной торговле

1. Единообразные правила в качестве отдельного юридического документа

64. Существовала возможность включения единообразных правил в расширенный вариант Типового закона, например, в качестве новой части III Типового закона. С тем чтобы ясно указать, что единообразные правила могут быть приняты либо самостоятельно, либо в сочетании с Типовым законом, в конечном итоге было принято решение о том, что единообразные правила следует подготовить в качестве отдельного юридического документа (см. A/CN.9/465, пункт 37). Это решение основывалось в основном на том факте, что во время окончательной доработки единообразных правил Типовой закон уже успешно применялся в ряде стран, а многие другие страны рассматривали вопрос о его принятии. Подготовка расширенного варианта Типового закона 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 могла бы вызвать трудности для тех стран, которые недавно приняли этот документ.

2. Полное соответствие единообразных правил Типовому закону

65. При разработке единообразных правил предпринимались все возможные усилия для обеспечения их соответствия с Типовым законом как по существу, так и с точки зрения терминологии (A/CN.9/465, пункт 37). В единообразных правилах воспроизводятся общие положения Типового закона. Речь идет о статьях 1 (Сфера применения), 2(a), (c) и (e) (Определение терминов "сообщение

данных", "составитель" и "адресат"), 3 (Толкование), 4 (Изменение по договоренности) и 7 (Подпись) Типового закона.

66. Единообразные правила, которые основываются на Типовом законе, направлены, в частности, на то, чтобы отразить следующее: принцип нейтральности с точки зрения носителя информации; подход, согласно которому не допускается дискриминация 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). Они предназначены для использования как в качестве минимальных стандартов в "открытой" среде (т.е. в условиях, когда стороны обмениваются электронными сообщениями без предварительного соглашения), либо в качестве 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

67. В ходе подготовки единообразных правил было выражено мнение о том, что ссылка на статью 7 Типового закона в тексте статьи 6 должна толковаться в качестве ограничивающей сферу действия единообразных правил теми ситуациями, когда электронная подпись используется для удовлетворения императивных требований законодательства о том, что для обеспечения *действительности* некоторых документов они должны быть подписаны. Согласно этой точке зрения, в силу того, что в законодательстве содержатся лишь весьма немногочисленные подобные требования в отношении документов, используемых для целей коммерческих сделок, сфера действия единообразных правил является весьма узкой. В ответ на это мнение была высказана получившая общую поддержку точка зрения о том, что подобное толкование проекта статьи 6 (и статьи 7 Типового закона) не соответствует толкованию слова "законодательство", которое было принято Комиссией в пункте 68 Руководства по принятию Типового закона 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, и статьи 6 единообразных правил 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

68. Единообразные правила, являющиеся дополнением к Типовому закону ЮНСИТРАЛ об электронной торговле, преследуют цель установления важнейших принципов, направленных на обеспечение применения электронных подписей. Однако в качестве "рамочных" единообразные правила сами по себе не устанавливают всех норм и правил, которые могут потребоваться (в дополнение к договорным механизмам, согласованным пользователями) для применения этих методов в принимающем единообразные правила государстве. Кроме того, как это указывается в настоящем Руководстве, единообразные правила не преследуют

цели охватить все аспекты применения электронных подписей. Соответственно, принимающее государство, возможно, пожелает принять подзаконные акты, с тем чтобы подробно регламентировать процедуры, вводимые единообразными правилами, и учесть конкретные обстоятельства и их возможные изменения в этом государстве без ущерба для целей единообразных правил. Если решение о необходимости таких подзаконных актов будет принято, то принимающему единообразные правила государству рекомендуется уделить особое внимание необходимости в сохранении гибкости в использовании систем электронных подписей пользователями.

69. Следует отметить, что методы электронного подписания, рассматриваемые в единообразных правилах, могут – в дополнение к вопросам процедурного характера, которые, возможно, потребуется учесть в технических подзаконных актах, принимаемых в целях осуществления единообразных правил, – поставить определенные правовые вопросы, ответы на которые могут содержаться не в единообразных правилах, 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 единообразных правилах.

D. Дополнительная определенность в отношении юридических последствий электронных подписей

70. Одна из основных черт единообразных правил состоит в создании дополнительной определенности в отношении применения гибкого критерия, устанавливаемого в статье 7 Типового закона в связи с признанием электронной подписи в качестве функционального эквивалента собственноручной подписи.

Статья 7 Типового закона гласит 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: [...]".

71. Статья 7 основывается на признании функций подписи в сфере бумажных документов. При подготовке Типового закона 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.

72. 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.

73. В пункте 1(b) устанавливается гибкий подход к уровню надежности, обеспечиваемому способом идентификации, использованному 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.

74. При определении того, является ли метод, 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).

75. На основе гибкого критерия, изложенного в статье 7(1)(b) Типового закона в статьях 6 и 7 единообразных правил устанавливается механизм, с помощью которого может быть предусмотрен порядок для оперативного определения юридической действительности электронных подписей, удовлетворяющих объективному критерию технической надежности. В единообразных правилах признаются две категории электронных подписей. Первой и наиболее широкой из них является категория, описанная в статье 7 Типового закона. Она состоит из любого "способа", который может быть использован для выполнения юридического требования о собственноручной подписи. Юридическая сила 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 единообразными правилами. 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 единообразных правилах. 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.

E. Базовые правила поведения заинтересованных сторон

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

77. Что касается автора подписи, то единообразные правила исходят из базового принципа, заключающегося в том, что автор подписи обязан проявлять разумную осмотрительность в отношении своего электронного подписывающего устройства. Ожидается, что автор подписи будет проявлять разумную осмотрительность для недопущения несанкционированного использования такого подписывающего устройства. В тех случаях, когда автору подписи известно или должно было быть известно, 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 автор подписи будет проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений в отношении сертификата.

78. 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.

79. 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 автора подписи; 2) любого ограничения в отношении целей или стоимостного объема, в связи с которыми может использоваться подписывающее устройство или сертификат; 3) функционирующее состояние подписывающего устройства; 4) любое ограничение в отношении масштаба или объема финансовой ответственности поставщика сертификационных услуг; 5) существуют ли средства для направления автором подписи уведомления о том, что подписывающее устройство было скомпрометировано; и 6) предлагается ли услуга по своевременному аннулированию.

80. В единообразных правилах 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

81. С учетом темпов технического прогресса единообразные правила обеспечивают юридическое признание электронных подписей независимо от вида используемой технологии (например, цифровых подписей, основывающихся на использовании асимметричной криптографии или биометрических характеристик).

V. ПОМОЩЬ СО СТОРОНЫ СЕКРЕТАРИАТА ЮНСИТРАЛ

A. Помощь в подготовке законопроектов

82. В рамках своей деятельности по подготовке кадров и оказанию помощи Секретариат ЮНСИТРАЛ предоставляет государствам помощь в виде технических консультаций при подготовке законодательства на основе единообразных правил ЮНСИТРАЛ об электронных подписях. Такая же помощь представляется правительствам, рассматривающим законодательство, основанное на других типовых законах ЮНСИТРАЛ, или рассматривающим вопрос о

присоединении к одной из конвенций по праву международной торговли, подготовленных ЮНСИТРАЛ.

83. Более подробную информацию, касающуюся единообразных правил, 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 единообразных правилах

84. Секретариат будет рад получить замечания, касающиеся единообразных правил и руководства, а также информацию, касающуюся принятия законодательства, основанного на единообразных правилах. Единообразные правила, после их принятия, будут включены 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.

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] A/CN.9/467, пункты 18–20.

[4] *Официальные отчеты Генеральной Ассамблеи, пятьдесят пятая сессия, Дополнение № 17* (A/55/17), пункты 380–383.

[5] Там же, *пятьдесят первая сессия, Дополнение № 17* (A/51/17), пункты 223–224.

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

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

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

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

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

[11] 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).

[12] 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).

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

[14] 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.

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