ОРГАНИЗАЦИЯ
ОБЪЕДИНЕННЫХ НАЦИЙ

A

Генеральная Ассамблея

Distr.
LIMITED

A/CN.9/WG.IV/WP.71
31 December 1996

RUSSIAN
ORIGINAL: ENGLISH

КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ
Рабочая группа по электронной торговле
Тридцать первая сессия
Нью-Йорк, 18—28 февраля 1997 года

ПЛАНИРОВАНИЕ БУДУЩЕЙ РАБОТЫ В ОТНОШЕНИИ ЭЛЕКТРОННОЙ ТОРГОВЛИ: ПОДПИСИ В ЦИФРОВОЙ ФОРМЕ, СЕРТИФИКАЦИОННЫЕ ОРГАНЫ И СВЯЗАННЫЕ С ЭТИМ ПРАВОВЫЕ ВОПРОСЫ

Записка Секретариата

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

ВВЕДЕНИЕ

1. После принятия Типового закона ЮНСИТРАЛ об электронной торговле Комиссия на своей двадцать девятой сессии приступила к рассмотрению будущей работы в области электронной торговли на основе предварительного обсуждения, проведенного Рабочей группой по электронному обмену данными на своей тридцатой сессии (A/CN.9/421, пункты 109—119). Было достигнуто общее согласие в отношении того, что ЮНСИТРАЛ должна продолжать свою работу по разработке правовых норм, которые могли бы привнести предсказуемость в область электронной торговли, тем самым активизируя торговлю во всех регионах.

2. Были высказаны новые предложения в отношении возможных тем и приоритетов будущей работы. Одно из предложений состояло в том, чтобы Комиссия приступила к разработке правил, касающихся подписей в цифровой форме. Было отмечено, что внедрение законов о подписях в цифровой форме вместе с законами, признающими действия "заверяющих органов" (далее именуемых "сертификационными органами") или иных лиц, уполномоченных выдавать электронные сертификаты или иные формы гарантий в отношении происхождения или атрибуции сообщений данных, "подписанных" в цифровой форме, во многих странах рассматривается как необходимое условие для развития электронной торговли. Было отмечено, что возможность полагаться на подписи в цифровой форме станет фактором, способствующим увеличению числа заключенных контрактов, а также возможности передавать права на товары или другие права при помощи электронных средств. В ряде стран сейчас готовятся новые законы, регулирующие вопросы подписей в цифровой форме. Было отмечено, что в этой сфере развития законодательства нет единообразия. Если Комиссия решит заняться работой в этой области, она будет иметь возможность унифицировать новые законы или по крайней мере установить общие принципы в области электронной подписи и тем самым обеспечить международную правовую базу для такой коммерческой деятельности.

3. Это предложение получило значительную поддержку. Однако было высказано общее мнение о том, что, если Комиссия решит заняться работой в области подписей в цифровой форме через свою Рабочую группу по электронному обмену данными, она должна дать Рабочей группе четкий мандат. Также считалось, что, поскольку ЮНСИТРАЛ не может взяться за подготовку технических стандартов, необходимо позаботиться о том, чтобы она не оказалась вовлеченной в технические вопросы, относящиеся к подписям в цифровой форме. Было отмечено, что, как признала Рабочая группа на своей тридцатой сессии, возможно, потребуется провести работу по вопросам, связанным с сертификационными органами, и что такую работу будет, вероятно, необходимо провести с учетом точки зрения регистров и поставщиков услуг. Однако Рабочая группа также сочла, что ей не следует заниматься рассмотрением каких-либо технических вопросов о приемлемости использования того или иного конкретного стандарта (A/CN.9/421, пункт 111). Была высказана обеспокоенность в отношении того, что работа по подписям в цифровой форме может выйти за пределы сферы торгового права и затронуть общие вопросы гражданского или административного права. В ответ на это было заявлено, что то же самое относится к положениям Типового закона и что Комиссия не должна уклоняться от разработки полезных правил по той причине, что такие правила могут также оказаться полезными за пределами сферы торговых отношений.

4. Другое предложение, основанное на предварительном обсуждении, проводившемся в Рабочей группе, заключалось в том, что будущая работа должна быть сконцентрирована на поставщиках услуг. В качестве вопросов, которые могут быть затронуты при обсуждении проблем, связанных с поставщиками услуг, были упомянуты следующие: минимальные стандарты, которые должны соблюдаться в отсутствие соглашения с заинтересованной стороной; объем риска, который принимают на себя "конечные" стороны; последствия таких правил или соглашений для третьих сторон; распределение рисков, сопряженных с неправомерным вторжением в операции или иными несанкционированными действиями; и объем обязательных гарантий, если таковые предусматриваются, или иных обязательств при предоставлении платных услуг (A/CN.9/421, пункт 116).

5. Было выражено общее мнение о том, что ЮНСИТРАЛ было бы целесообразно проанализировать отношения между поставщиками услуг, пользователями и третьими сторонами. Было отмечено, что весьма важно направить такие усилия на разработку международных норм и стандартов коммерческого поведения в этой области в целях поддержания торговли с помощью

электронных средств, а не ставить перед собой задачу установить режим, регламентирующий деятельность поставщиков услуг, или другие правила, которые могли бы обусловить затраты, не приемлемые для применения ЭДИ на рынке (см.A/CN.9/421, пункт 117). Вместе с тем было выражено мнение о том, что тема поставщиков услуг может оказаться слишком широкой и охватывать слишком много различных фактических ситуаций, чтобы ее можно было рассматривать в качестве одного рабочего пункта. Было достигнуто общее согласие о том, что вопросы, относящиеся к поставщикам услуг, уместно было бы рассматривать в контексте каждой новой области деятельности, которой будет заниматься Рабочая группа.

6. Еще одно предложение заключалось в том, чтобы Комиссия приступила к подготовке новых общих правил, необходимых для разъяснения того, как традиционные контрактные функции могут выполняться через посредство электронной торговли. Как было указано, существует большая неопределенность в отношении того, что значат термины "исполнение", "поставка" и другие в контексте электронной торговли, когда оферта, акцепт и поставка товаров могут осуществляться через открытые компьютерные сети по всему миру. Быстрый рост компьютеризированной торговли, а также числа сделок через "Интернет" и другие системы придал этой теме первостепенное значение. Была высказана мысль о том, проведенное Секретариатом исследование могло бы уточнить объем такой работы. Если Комиссия после анализа такого исследования решит продолжить свою работу, одним из вариантов было бы включение таких правил в раздел "Специальные положения" Типового закона ЮНСИТРАЛ об электронной торговле.

7. Еще одно предложение состояло в том, чтобы Комиссия сосредоточила свое внимание на вопросе включения путем ссылки. Было отмечено, что Рабочая группа согласилась с тем, что эта тема может быть надлежащим образом рассмотрена в контексте более общей работы по вопросам регистров и поставщиков услуг (A/CN. 9/421, пункт 114). Комиссия достигла общей договоренности о том, что этим вопросом можно заняться в контексте работы по сертификационным органам.

8. После обсуждения Комиссия согласилась с уместностью включения вопроса о подписях в цифровой форме и сертификационных органах в повестку дня Комиссии, при том условии, что это даст возможность заняться и другими темами, предложенными Рабочей группой для будущей работы. Что касается более четкого мандата для Рабочей группы, то было также достигнуто согласие в отношении того, что единообразные правила, которые следует подготовить, должны охватывать такие вопросы, как: правовая база процессов 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.

9. Комиссия просила Секретариат подготовить справочное исследование по вопросам подписей в цифровой форме и поставщиков услуг на основе анализа законов, которые готовятся сейчас в различных странах. На основе этого исследования Рабочая группа должна рассмотреть целесообразность и возможность подготовки единообразных правил по вышеупомянутым темам. Было выражено согласие с тем, что работа, которая должна быть проведена Рабочей группой на ее тридцать первой сессии, может охватывать подготовку проектов правил по определенным аспектам вышеуказанных тем. Рабочей группе было предложено представить Комиссии достаточную информацию для принятия обоснованного решения в отношении сферы применения единообразных правил, которые будут разрабатываться. С учетом широких масштабов деятельности, охватываемой Типовым законом ЮНСИТРАЛ об электронной торговле, и возможной будущей работы в области электронной торговли было решено переименовать Рабочую группу по электронному обмену данными в Рабочую группу по электронной торговле[1].

---

[1] Официальные отчеты Генеральной Ассамблеи, пятьдесят первая сессия, Дополнение № 17 (A/51/17), пункты 216—224.

10. В настоящей записке содержится предварительное исследование по вопросам подписей в цифровой форме и смежным проблемам. Она была подготовлена на основе Типового закона ЮНСИТРАЛ об электронной торговле, а также с учетом законодательных документов, которые были недавно приняты или которые в настоящее время разрабатываются в ряде стран. Кроме того, исследование опирается на работу других организаций, в частности на проект единообразных международных правил удостоверения подлинности и сертификации, разрабатываемый Международной торговой палатой (МТП), и на Руководящие принципы, касающиеся подписи в цифровой форме, опубликованные Американской ассоциацией адвокатов, и отражает итоги работы совещания специальной группы экспертов, в котором участвовали специалисты в области подписей в цифровой форме и Секретариат ЮНСИТРАЛ.

11. В соответствии с последними инструкциями, относящимися к осуществлению более строгого контроля за документами Организации Объединенных Наций и ограничению их объема, пояснительные замечания по проектам положений настолько краткие, насколько это возможно. Дополнительные разъяснения будут даны устно.

I. ОБЩИЕ ЗАМЕЧАНИЯ ОТНОСИТЕЛЬНО ПОДПИСЕЙ В ЦИФРОВОЙ ФОРМЕ

A. Функции подписей

12. 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.

13. В условиях электронного обмена данными подлинник сообщения неотличим от копии, не имеет собственноручной подписи и не является бумажным документом. Возможность обмана велика из-за легкости перехвата и изменения информации в электронной форме, оставшихся незамеченными, и скорости обработки многочисленных сделок. 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. Подписи в цифровой форме и другие электронные подписи

14. При обсуждении целесообразности и возможности подготовки единообразных правовых норм, касающихся подписей в цифровой форме, и для оказания Комиссии содействия при рассмотрении сферы применения таких возможных единообразных правил Рабочая группа, возможно, пожелает изучить различные методы, используемые в настоящее время или еще находящиеся в стадии разработки, цель которых состоит в предоставлении функциональных эквивалентов собственноручным подписям и другим способам удостоверения подлинности, применяемым в условиях использования бумажных документов.

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

15. Следует напомнить, что наряду с "подписями в цифровой форме", основанными на криптографии с использованием публичных ключей, которые являются главным предметом данной записки, существуют различные другие средства, часто называемые способами проставления "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.

16. Рабочая группа может пожелать обсудить вопрос о том, следует ли расширить сферу этой работы, с тем чтобы она охватывала электронные подписи в целом. Такая работа потребует проведения Секретариатом дополнительных исследований с точки зрения технических и правовых последствий использования устройств проставления "подписей", в которых применяются иные методы, чем криптография с использованием публичных ключей. С учетом наличия достаточной

предварительной информации о правовых последствиях подписей в цифровой форме и существования законопроектов по этому вопросу в ряде стран в настоящей записке основное внимание уделяется вопросам подписей в цифровой форме, проставляемых с помощью криптографии с использованием публичных ключей.

17. При обсуждении целесообразности и возможности подготовки единообразных правил, которые будут применяться как к подписям в цифровой форме, так и к другим формам электронных подписей, Рабочая группа может пожелать рассмотреть вопрос о том, следует ли ЮНСИТРАЛ предпринять попытку разработать единообразные правила на уровне, который был бы промежуточным между высоким уровнем общей применимости Типового закона и более конкретными правилами, касающимися особенностей одного или нескольких конкретных методов. В любом случае согласно принципу нейтральности Типового закона по отношению к носителям данных, единообразные правила, которые предстоит разработать, если они сосредоточат внимание на подписях в цифровой форме, не должны препятствовать применению альтернативных методов.

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

a) Технические понятия и терминология

i) Криптография

18. Подписи в цифровой форме создаются и проверяются путем использования криптографии, являющейся отраслью прикладной математики, позволяющей преобразовывать сообщения в кажущуюся непонятной форму и обратно в подлинную форму. При проставлении подписей в цифровой форме 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 подписи в цифровой форме или преобразования данных в кажущуюся непонятной форму, а другой ключ — для удостоверения подлинности подписи в цифровой форме 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.

19. Хотя применение криптографии является одной из основных особенностей подписей в цифровой форме, тот простой факт, что подпись в цифровой форме 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 публичной политики, которые могут включать соображения национальной обороны. Однако применение криптографии в целях удостоверения подлинности путем создания подписи в цифровой форме не обязательно подразумевает использование кодирования для обеспечения конфиденциальности в процессе передачи сообщений, поскольку закодированная подпись в цифровой форме может быть всего лишь добавлена к незакодированному сообщению. Рабочая группа, возможно, захочет обсудить, в какой мере возможные единообразные правила, касающиеся подписей в цифровой форме, должны признавать применение криптографии для удостоверения подлинности в отличие от ее применения для целей обеспечения конфиденциальности.

---

[2] 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 (pp. 8—17).

20. В качестве примера причин, по которым разные правила могут быть необходимыми тогда, когда кодирование используется для целей обеспечения конфиденциальности и когда оно всего лишь используется в контексте подписей в цифровой форме, можно указать, что если кодирование используется для сохранения конфиденциальности сообщений, то во многих случаях важно располагать способом восстановления закодированных сообщений в случае потери частного ключа, когда закодированное сообщение имеет правовое или финансовое значение или же значение с точки зрения ответственности в публичном порядке. При надлежащем применении эти методы позволяют эмитенту пары ключей сохранить или воссоздать отсутствующий ключ. Однако, может быть, и нет необходимости в сохранении или воссоздании частного ключа, использовавшегося для создания подписей в цифровой форме, а наличие технической возможности сделать это может уменьшить доверие, которое пользователи и публика в целом могут испытывать ко всей этой системе.

ii) "Публичные и частные ключи"

21. Взаимно дополняющие ключи, используемые для проставления подписи в цифровой форме, произвольно называются "частным ключом", который используется подписывающим лицом для создания подписи в цифровой форме, и "публичным ключом", который обычно более широко известен и используется соответствующей стороной для проверки подлинности подписи в цифровой форме[3]. Если многим людям необходимо проверить подлинность подписей в цифровой форме 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[4]. Таким образом, хотя многие люди могут знать публичный ключ данного подписавшегося лица и использовать этот ключ для проверки подлинности его подписей, они не могут установить его частный ключ и использовать этот ключ для подделки подписей в цифровой форме.

22. Вместе с тем следует отметить, что понятие криптографии с использованием публичного ключа необязательно 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. При обсуждении вопросов, касающихся криптографии с использованием

---

[3] Предполагается, что пользователь частного ключа держит его в секрете. Следует отметить, что отдельному пользователю не нужно знать частный ключ. Такой частный ключ, по всей вероятности, должен 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.

[4] 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, накладных расходах на использование компьютера, 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).

публичных ключей, Рабочая группа может пожелать официально признать рамки, в которых криптография с использованием публичных ключей применяется в международной торговле. В то же время Рабочая группа, возможно, пожелает придерживаться технически нейтрального подхода, принимая во внимание нынешнюю технологию и не исключая при этом будущие изменения в методах вычислений, с помощью которых создаются пары ключей. Такая открытость техническим достижениям в компьютерной промышленности, помимо прочего, логически вытекала бы из решения Комиссии о том, что ЮНСИТРАЛ не может взяться за подготовку технических стандартов и что необходимо позаботиться о том, чтобы она не оказалась вовлеченной в технические вопросы, связанные с подписями в цифровой форме (см. выше, пункт 3).

iii) "Функция хеширования"

23. В дополнение к подготовке пар ключей, как для создания, так и для проверки подлинности подписи в цифровой форме используется еще один основополагающий процесс, обычно именуемый "функцией хеширования". Функция хеширования представляет собой математический процесс, основанный на использовании алгоритма, который создает цифровое обозначение или сжатую форму сообщения, которая часто называется "резюме сообщения" или "отпечаток" сообщения, в форме "величины хеширования" или "результата хеширования" стандартной длины, которая обычно намного меньше, чем само сообщение, но, тем не менее, по существу относится только к нему. Любое изменение в сообщении неизбежно дает иной результат хеширования, когда используется та же функция хеширования. В случае использования надежной функции хеширования, иногда именуемой "функцией одностороннего хеширования", фактически невозможно получить подлинное сообщение на основании осведомленности о его величине хеширования. Поэтому функции хеширования дают возможность того, чтобы программное обеспечение, используемое для создания подписей в цифровой форме, 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) "Подпись в цифровой форме"

24. Чтобы подписать какой-либо документ или любой другой элемент данных, подписывающее лицо сначала определяет точные границы того, что предстоит подписать. Точно обозначенная информация, подлежащая подписанию, может именоваться "сообщением". Затем путем использования функции хеширования подписывающее лицо с помощью программного обеспечения исчисляет результат хеширования, относящийся (для всех практических целей) только к данному сообщению. Далее подписывающее лицо с помощью программного обеспечения преобразует результат хеширования в подпись в цифровой форме, используя свой частный ключ. Таким образом, созданная подпись в цифровой форме относится только к сообщению и к частному ключу, использовавшемуся для ее создания.

25. Как правило, подпись в цифровой форме (результат хеширования сообщения, подписанный в цифровой форме) прилагается к своему сообщению и хранится или передается со своим 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 подпись в цифровой форме относится только к своему сообщению, она является бесполезной, если лишена постоянной связи со своим сообщением.

v) Проверка подлинности подписи в цифровой форме

26. Проверка подлинности подписи в цифровой форме представляет собой процесс проверки такой подписи путем обращения к подлинному сообщению и какому-либо данному публичному ключу и тем самым установления того, была ли эта подпись в цифровой форме создана для того же сообщения с использованием частного ключа, соответствующего упоминаемому публичному ключу. Проверка подписи в цифровой форме производится путем исчисления нового результата хеширования подлинного сообщения с помощью той же функции хеширования, которая использовалась для

создания данной подписи в цифровой форме. Затем, используя публичный ключ и новый результат хеширования, проверяющий устанавливает, была ли подпись в цифровой форме создана с использованием соответствующего частного ключа и совпадает ли вновь исчисленный результат хеширования с первоначальным результатом хеширования, который был преобразован в подпись в цифровой форме в процессе подписания.

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

b) Инфраструктура для использования публичных ключей (ИПК) и сертификационные органы

28. Чтобы проверить подпись в цифровой форме, 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 лица или образования 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.

29. 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, всемирная 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.

30. 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[5].

31. Предполагаемое подписывающее лицо может сделать публичное заявление о том, что подписи, проверяемые с помощью какого-либо данного 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

---

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

данного 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 подписи в цифровой форме (случай, который часто называют "нерасторжением"), если сделка окажется неблагоприятной для подразумеваемого подписывающего лица.

32. Решение этих проблем заключается в том, чтобы заручиться готовностью одной или нескольких доверенных третьих сторон установить связь между определенным подписавшим лицом или его именем и конкретным публичным ключом. Такую доверенную третью сторону обычно называют "сертификационным органом" в большинстве технических стандартов и руководящих принципов. В ряде стран создана иерархическая структура таких сертификационных органов, которую часто называют инфраструктурой для использования публичных ключей (ИПК).

i) Инфраструктура для использования публичных ключей (ИПК)

33. Создание инфраструктуры для использования 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) образованиям, 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 подписей в цифровой форме; (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 удостоверяющими личность 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 даты; (10) управление кодовыми ключами, используемыми для кодирования в целях обеспечения конфиденциальности, если применение такого метода санкционировано.

34. Инфраструктура для использования 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 "основной 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[6]; (2) различные сертификационные органы, занимающие более низкую ступень по сравнению с "основным" 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.

---

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

35. Рабочая группа может пожелать провести общее обсуждение вопросов, касающихся ИПК. Однако, как представляется, в отношении таких вопросов может быть нелегко достичь международного согласования. Создание ИПК может быть сопряжено с различными техническими вопросами, а также вопросами публичной политики, которые, возможно, лучше оставить на усмотрение каждого отдельного государства[7]. 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 государственными учреждениями или же частные образования также могут действовать в качестве сертификационных органов; (4) вопроса о том, должен ли процесс выдачи какому-либо образованию разрешения действовать в качестве сертификационного органа принимать форму прямого уполномочивания или "лицензирования" со стороны государства или же следует использовать другие методы контроля за качеством работы сертификационных органов, если им будет разрешено функционировать в отсутствие конкретного уполномочивания; (5) степени, в которой следует разрешить использование криптографии в целях обеспечения конфиденциальности; и (6) вопроса о том, должны ли государственные органы сохранять доступ к закодированной информации через механизм "ключа на хранении у третьей стороны" или как-либо иначе. Рабочая группа может пожелать вынести рекомендацию о том, что вышеупомянутые вопросы не следует затрагивать в ходе будущей работы Комиссии в отношении подписей в цифровой форме.

ii) Сертификационные органы

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

37. Чтобы удостоверить подлинность сертификата с точки зрения как его содержания, так и его источника, сертификационный орган подписывает его в цифровой форме. Подлинность подписи в цифровой форме 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 необязательно), 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 подпись в цифровой форме, 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 подписи в цифровой форме сертификационного органа.

---

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

38. Подпись в цифровой форме, 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 данная подпись в цифровой форме создана в течение "срока действия", указанного в сертификате, что является условием проверки подлинности подписи в цифровой форме.

39. Чтобы обеспечить доступность публичного ключа и данных о его соответствии конкретному держателю для использования при проверке подлинности, сертификат может внесен в хранилище или предоставляться каким-либо иным образом. Обычно хранилища представляют собой работающие в оперативном режиме базы данных по сертификатам и другой информации, которая может быть получена и использована для проверки подлинности подписей в цифровой форме. В зависимости от ввода, поиск сертификата может производиться автоматически путем направления с помощью программы проверки подлинности прямого запроса в базу данных для получения необходимых сертификатов.

40. 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 доверия 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 подпись в цифровой форме, подлинность которой может быть проверена путем ссылки на ненадежный сертификат.

41. Вполне понятно, что функционирование сертификационных органов может обеспечиваться государственными органами или поставщиками услуг, принадлежащими к частному сектору. В ряде стран по соображениям публичной политики предусматривается, что только государственные органы 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 государственными учреждениями или поставщиками услуг, принадлежащими к частному сектору, и требуется ли, чтобы сертификационные органы получили лицензию для осуществления своей деятельности, обычно в рамках ИПК действует более чем один сертификационный орган. Особую озабоченность вызывают 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 возникать озабоченность в отношении признания сертификатов сертификационными органами в зарубежных странах. Признание иностранных сертификатов часто называется "перекрестной сертификацией". 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 друг другу услуги, с тем чтобы их соответствующие пользователи могли сноситься друг с другом более эффективно и с большей уверенностью в надежности выдаваемых сертификатов.

42. В связи с перекрестной сертификацией или "увязыванием" сертификатов могут возникать правовые проблемы, когда принимается целый ряд мер по обеспечению многоуровневой защиты неприкосновенности данных. Примеры таких проблем могут включать определение того, чье неправильное поведение привело к убыткам и на чьи обозначения 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 имела места небрежность со стороны сертификационных органов, то ответственность не возникает.

43. На сертификационный орган или основной 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 выдаваемого публичного ключа и идентификационные данные 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 основным органом или вышестоящим сертификационным органом, или же любого другого соответствующего требования, на постоянной основе.

44. Рабочая группа может пожелать рассмотреть следующие факторы, которые необходимо принимать во внимание при оценке надежности какого-либо сертификационного органа: (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 наличия 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 данного сертификационного органа; (10) внутренняя безопасность; (11) процедуры прекращения операций, включая направление уведомления пользователям; (12) гарантии и обозначения (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 подписи в цифровой форме

45. Использование подписей в цифровой форме 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 подписи в цифровой форме используется результат хеширования, полученный как из подписанного сообщения, так и из какого-либо данного частного ключа, и относящийся только к ним. Чтобы результат хеширования был надежным, должна

существовать лишь ничтожная вероятность того, что такая же подпись в цифровой форме 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. Подпись в цифровой форме состоит из закодированного резюме сообщения;

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

6) отправитель направляет подпись в цифровой форме и (незакодированное или закодированное) сообщение получателю электронным способом;

7) получатель использует публичный ключ отправителя для проверки подлинности подписи в цифровой форме 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 подпись в цифровой форме на сообщении отправителя. Сертификационный орган обычно является доверенной третьей стороной, которая осуществляет сертификацию в системе подписей в цифровой форме. Сертификат содержит публичный ключ и имя отправителя (и, возможно, дополнительную информацию) и подписан в цифровой форме сертификационным органом.

II. ПРАВОВЫЕ ВОПРОСЫ И ВОЗМОЖНЫЕ ПОЛОЖЕНИЯ ДЛЯ РАССМОТРЕНИЯ В ЕДИНООБРАЗНЫХ ПРАВИЛАХ, КАСАЮЩИХСЯ ПОДПИСЕЙ В ЦИФРОВОЙ ФОРМЕ

A. Объем работы

46. При решении вопроса о включении пункта, касающегося подписей в цифровой форме и сертификационных органов, в свою повестку дня Комиссия на своей двадцать девятой сессии также согласилась с тем, что рассмотрение этого пункта следует использовать в качестве возможности обсуждения и других тем, предложенных Рабочей группой для будущей работы (см. выше, пункт 8). До начала обсуждения вопросов подписей в цифровой форме Рабочая группа может пожелать рассмотреть вопрос о целесообразности и возможности ограничения объема своей работы подписями в цифровой форме или его расширения для охвата также других механизмов удостоверения подлинности, которые могут иметься в настоящее время или вскоре будут разработаны для использования в электронной торговле (см. выше, пункты 15—17). Можно напомнить о том, что во время подготовки Типового закона Рабочая группа учитывала необходимость установления правовых норм, которые не были бы увязаны с данной стадией развития техники и торговли, а скорее предусматривали бы общие принципы, которые, как можно ожидать, оставались бы применимыми в течение ряда лет, независимо от возможных изменений в области технологии.

47. Широкое использование подписей в цифровой форме и риск того, что в различных странах будут приняты отличающиеся друг от друга законодательные подходы к подписям в цифровой форме, позволяют предположить, что единообразные законодательные положения являются необходимыми в

качестве конкретной правовой основы для использования этого метода удостоверения подлинности. Однако в соответствии с нейтральным по отношению к носителями информации подходом, принятым при подготовке Типового закона, Рабочая группа может пожелать обсудить вопрос о том, целесообразно ли заняться разработкой единообразных правил, которые применялись бы только к подписям в цифровой форме, или же следует разрабатывать такие единообразные правила, какие применялись бы и к другим методам удостоверения подлинности. Если Рабочая группа придет к выводу о том, что вышеупомянутый риск принятия в различных странах разных законов позволяет предположить, что необходимость в единообразных правилах, применимых к подписям в цифровой форме, является особенно острой, то Рабочая группа может также пожелать обсудить возможные пути разработки единообразных правил, касающихся подписей в цифровой форме, с тем чтобы избежать возникновения риска неправильного толкования таких единообразных правил как поощряющих использование подписей в цифровой форме в ущерб конкурирующим методам, которые могут также считаться приемлемыми примерами понятия "надежного метода", воплощенного в статье 7 Типового закона.

48. В отношении сертификационных органов Рабочая группа может также пожелать принять во внимание то, что во многих практических ситуациях деятельность какого-либо коммерческого образования в качестве сертификационного органа является всего лишь одним из аспектов более обширной деятельности этого коммерческого образования в качестве поставщика услуг. Таким образом, Рабочая группа может пожелать обсудить вопрос о том, следует ли ограничивать сферу применения единообразных правил, касающихся сертификационных органов, установлением правил поведения, применимых только в контексте деятельности какого-либо поставщика услуг, выступающего в качестве сертификационного органа, или же было бы целесообразным и возможным разработать правила, применимые к большему числу видов деятельности поставщиков услуг или "доверенных третьих сторон" в электронной торговле.

B. Сфера применения единообразных правил, касающихся подписей в цифровой форме, и общих положений

49. Настоящая записка готовилась на основе предположения о том, что возможные правила, касающиеся подписей в цифровой форме, должны прямо вытекать из статьи 7 Типового закона и должны рассматриваться как способ предоставления подробной информации относительно понятия надежного "метода, используемого для идентификации" какого-либо лица и "указания на то, что это лицо согласно" с информацией, содержащейся в сообщении данных. При рассмотрении общих положений, которые могут быть включены в совокупность единообразных правил, касающихся подписей в цифровой форме, Рабочая группа может пожелать обсудить в более общем плане взаимосвязь между такими единообразными правилами и Типовым законом ЮНСИТРАЛ об электронной торговле. В частности, Рабочая группа может пожелать внести предложения Комиссии относительно того, должны ли единообразные правила, касающиеся подписей в цифровой форме, представлять собой отдельный юридический документ или же их следует включить в расширенный вариант Типового закона, например, в качестве отдельной главы, включенной в Часть вторую Типового закона.

50. Независимо от того, будут ли единообразные правила, касающиеся подписей в цифровой форме, разработаны в качестве отдельного документа или как добавление к Типовому закону, представляется, что такие единообразные правила должны будут основываться на положениях, соответствующих статьям 1(Сфера применения), 2 (a), (c) и (e) (Определения "сообщения данных", "составителя" и "адресата"), 3 (Толкование), 4 (Изменение по договоренности), 6 (Письменная форма) и 7 (Подпись) Типового закона. Хотя такие положения не воспроизводятся прямо в настоящей записке, следует отметить, что проекты единообразных правил, касающихся подписей в цифровой форме, были подготовлены Секретариатом на основе предположения о том, что такие положения являются частью этих единообразных правил. В связи с этим следует также отметить, что положения, соответствующие статьям 2, 4, 6 и 7 Типового закона, содержатся в законодательстве о подписях в цифровой форме, которое разрабатывается в некоторых странах, а ссылки на Типовой закон также содержатся в таких текстах, как Руководящие принципы, касающиеся подписей в цифровой форме, Американской ассоциации адвокатов.

51. Помимо вышеупомянутых положений, Рабочая группа может пожелать рассмотреть вопрос о том, следует ли разъяснить в преамбуле к единообразным правилам цель этих правил, а именно содействие эффективному использованию цифровых сообщений путем создания основы обеспечения неприкосновенности данных и наделения письменных и цифровых сообщений равным статусом с точки зрения их юридической силы.

C. Конкретные правовые вопросы и проекты положений, касающиеся подписей в цифровой форме

1. Определения

52. Законы, постановления и руководящие принципы, которые уже осуществляются или разрабатываются в настоящее время в области подписей в цифровой форме и сертификационных органов, существенно различаются с точки зрения числа определений, на которые они полагаются. В зависимости от правовых традиций принимающего законы государства вопросы, касающиеся подписей в цифровой форме, могут решаться главным образом с помощью определений в соответствующих актах или же такие акты могут вообще не содержать каких-либо определений.

53. В соответствии с подходом, принятым при подготовке Типового закона, Рабочая группа может пожелать рассмотреть ограниченное число определений, касающихся таких важнейших понятий, как "подпись в цифровой форме", "сертификационные органы" и "сертификаты".

54. Рабочая группа может пожелать использовать в качестве основы для обсуждения нижеследующие возможные определения.

a) Подпись в цифровой форме

55. "Проект статьи A

1) Подпись в цифровой форме представляет собой числовую величину, которая добавлена к сообщению данных и которая при использовании известной математической процедуры, связанной с частным криптографическим ключом составителя, дает возможность достоверно определить, что эта числовая величина была получена с помощью частного криптографического ключа составителя.

2) Математические процедуры, используемые для подготовки санкционированных подписей в цифровой форме в соответствии с [настоящим Законом] [настоящими Правилами], основываются на кодировании с помощью публичного ключа. При применении к какому-либо сообщению данных эти математические процедуры производят преобразование сообщения таким образом, что лицо, располагающее первоначальным сообщением и публичным криптографическим ключом составителя, может точно определить

a) было ли такое преобразование произведено с использованием частного криптографического ключа, который соответствует частному криптографическому ключу составителя; и

b) было ли первоначальное сообщение изменено после произведенного преобразования.

3) Подпись в цифровой форме, добавленная к какому-либо сообщению данных, считается санкционированной, если ее подлинность можно проверить в соответствии с процедурами, установленными сертификационным органом, уполномоченным согласно [настоящему Закону] [настоящим Правилам].

4) [Соответствующий орган принимающего государства] устанавливает конкретные правила в отношении технических требований, которым должны отвечать подписи в цифровой форме и порядок проверки их подлинности".

Замечания

56. В соответствии с функциональным подходом, принятым при подготовке Типового закона, в пунктах 1) и 2) предлагаемого положения дается краткое описание технических функций, выполняемых кодированием с помощью публичного ключа. Пункты 3) и 4) отражают принцип, согласно которому подписи в цифровой форме являются действительными только тогда, когда они проставляются в контексте инфраструктуры для использования публичных ключей (ИПК), созданной государственными органами.

b) Уполномоченные сертификационные органы

57. "Проект статьи B

1) ...[принимающее государство указывает орган или ведомство, компетентное уполномочивать сертификационные органы] может предоставлять сертификационным органам полномочия действовать во исполнение [настоящего Закона] [настоящих Правил]. Такие полномочия могут быть отозваны.

2) ...[принимающее государство указывает орган или ведомство, компетентное принимать постановления в отношении уполномоченных сертификационных органов] может устанавливать правила, регулирующие условия, на которых такие полномочия могут быть предоставлены, и принимать постановления, касающиеся функционирования сертификационных органов.

3) Уполномоченные сертификационные органы могут выдавать сертификаты в отношении криптографических ключей физических и юридических лиц.

4) Уполномоченные сертификационные органы могут предлагать или облегчать регистрацию и фиксацию даты передачи и получения сообщений данных, а также выполнять другие функции в отношении сообщений, защищенных с помощью подписей в цифровой форме.

5) ...[принимающее государство указывает орган или ведомство, компетентное устанавливать конкретные правила в отношении функций, которые должны выполняться уполномоченными сертификационными органами] может устанавливать более конкретные правила в отношении функций, которые должны выполняться уполномоченными сертификационными органами в связи с выдачей сертификатов отдельным физическим или юридическим лицам.

Замечания

58. Рабочая группа может пожелать обсудить вопрос о том, следует ли в разрабатываемых единообразных правилах прямо упоминать о критериях, которые необходимо принимать во внимание при предоставлении сертификационным органам полномочий осуществлять свою деятельность. Можно напомнить о том, что в контексте подготовки Типового закона такие критерии были оставлены для включения в Руководство по принятию Типового закона.

c) Сертификаты

59. "Проект статьи C

В сертификате, выдаваемом уполномоченным сертификационным органом в форме сообщения данных или как-либо иначе, по меньшей мере указываются:

a) имя пользователя [и адрес или место нахождения коммерческого предприятия];

b) [день и год рождения][достаточные идентификационные данные] пользователя, если пользователем является физическое лицо;

c) если пользователем является юридическое лицо, то название компании и любая соответствующая информация для идентификации этой компании;

e) название, адрес или место нахождения сертификационного органа;

f) публичный криптографический ключ пользователя;

g) любая необходимая информация, указывающая, каким образом проверка подлинности публичного криптографического ключа пользователя может быть произведена получателем подписи в цифровой форме, предоставленной в соответствии с сертификатом;

h) серийный номер сертификата; и

i) [дата выдачи и дата истечения срока действия][срок действия] сертификата".

Замечания

60. В проектах законодательства о подписи в цифровой форме, разрабатываемых в некоторых странах, указываются часть или все элементы, упомянутые в проекте статьи C, в качестве минимальной информации, которую требуется представлять в любом сертификате, выданном сертификационным органом. Однако в соответствии с решением, принятым Рабочей группой при подготовке Типового закона, не заниматься вопросами защиты личных данных Рабочая группа может пожелать учесть то, что во многих странах информация, например о дате рождения какого-либо лица, защищается как личные данные и что ее раскрытие с помощью электронных средств может регулироваться особыми нормами.

2. Подписи, проставляемые физическими и юридическими лицами

61. "Проект статьи D

1) Физические и юридические лица могут на равных основаниях получать сертификацию криптографических публичных ключей, используемых исключительно для целей идентификации.

2) Юридическое лицо может идентифицировать сообщение данных путем добавления к этому сообщению частного криптографического ключа, сертифицированного для этого юридического лица. Юридическое лицо рассматривается как [составитель][одобрившее направление] сообщения только в том случае, если это сообщение также подписано в цифровой форме физическим лицом, уполномоченным действовать от имени этого юридического лица".

Замечания

62. Вышеизложенное положение призвано разъяснить условия, на которых подписи в цифровой форме могут применяться с целью создания обязательств для юридических лиц. Оно основывается на различии между двумя функциями, выполняемыми "подписью" согласно статье 7 (1) (a) Типового закона, а именно идентификация автора сообщения и указание на то, что это лицо согласно с информацией, содержащейся в сообщении данных. В то время как эти две функции обычно выполняются путем использования одного ключа, сертифицированного для физического лица, публичные ключи, сертифицированные для юридических лиц, используются всего лишь для того, чтобы дать гарантию в отношении идентификации юридического лица как отправителя сообщения. Таким образом, "подпись в цифровой форме" юридического лица будет иметь ограниченную силу действия. Любое одобрение сообщения потребует, помимо "подписи в цифровой форме" (т. е. идентификации) юридического лица, подписи в цифровой форме физического лица, которая

одновременно идентифицирует это лицо и указывает от имени юридического лица на намерение согласиться с содержанием сообщения.

63. Хотя этот проект положения содержит ссылку на "физическое лицо, уполномоченное действовать от имени" юридического лица, он не призван заменить внутреннее агентское право. Таким образом, вопрос о том, располагает ли физическое лицо фактически и по закону полномочиями действовать от имени юридического лица, оставлен для решения в соответствующих правовых нормах за рамками единообразных правил.

3. Атрибуция сообщений, подписанных в цифровой форме

64. "Проект статьи E

1) Составитель сообщения данных, на котором проставлена подпись составителя в цифровой форме, связан содержанием сообщения таким же образом, как если бы это сообщение существовало в [собственноручно] подписанной форме в соответствии с законом, применимым к содержанию этого сообщения.

2) Адресат сообщения данных, на котором проставлена подпись в цифровой форме, имеет право считать это сообщение данных сообщением составителя и действовать на основании этого предположения, если:

a) для установления того, что это сообщение данных является сообщением составителя, адресат надлежащим образом применил публичный ключ составителя к сообщению данных в полученном виде и применение публичного ключа составителя показало, что полученное сообщение данных было закодировано с помощью частного криптографического ключа составителя и что первоначальное сообщение не было изменено после его кодирования посредством использования публичного криптографического ключа составителя;

или

b) сообщение данных, полученное адресатом, явилось результатом действий лица, взаимоотношения которого с составителем или с любым представителем составителя дали такому лицу возможность получить доступ к частному криптографическому ключу составителя.

3) Пункт 2 не применяется:

a) с момента, когда адресат узнал или должен был узнать, если бы он запросил информацию у уполномоченного сертификационного органа или как-либо иначе проявил разумную осмотрительность, что срок действия публичного криптографического ключа составителя истек или что сертификат, выданный этим сертификационным органом, был аннулирован или его действие было приостановлено;

или

b) в случае, предусмотренном пунктом 2 (b), с момента, когда адресат узнал или должен был узнать, если бы он проявил разумную осмотрительность или использовал любую согласованную процедуру, что данное сообщение данных не являлось сообщением данных составителя".

Замечания

65. Рабочая группа может пожелать обсудить вопрос о том, можно ли вопрос об атрибуции сообщений, подписанных в цифровой форме, решить просто путем ссылки на статью 13 Типового закона. Проект статьи E, который сформулирован по образцу статьи 13 Типового закона, призван проиллюстрировать принципы, содержащиеся в статье 13, в контексте подписей в цифровой форме.

Он основывается на необходимости обеспечить определенность в отношении правовых последствий подписей в цифровой форме, которые в настоящее время считаются высоконадежной процедурой удостоверения подлинности. Этот проект положения возлагает тяжелое бремя на составителя сообщения, имеющего подпись в цифровой форме этого составителя. Можно напомнить о том, что согласно статье 2 (c) Типового закона "составитель" означает любое лицо, которым или от имени которого сообщение данных, как предполагается, было отправлено. Этот проект положения указывает на необходимость того, чтобы любой пользователь подписи в цифровой форме обеспечивал защиту своего частного ключа, который, если его применить для кодирования сообщения, создаст неопровержимую презумпцию, что это сообщение данных является сообщением данных предполагаемого составителя.

4. Аннулирование сертификатов

66. "Проект статьи F

1) Держатель сертифицированнй пары ключей может аннулировать соответствующий сертификат. Аннулирование вступает в силу с момента его [регистрации][получения] сертификационным органом.

2) Держатель сертифицированной пары ключей обязан аннулировать соответствующий сертификат, если держатель узнает, что частный криптографический ключ был утерян или скомпрометирован или подвергается опасности неправильного использования в других отношениях. Если держатель не аннулирует сертификат в такой ситуации, то держатель несет ответственность за любой ущерб, понесенный третьими сторонами, которые полагались на содержание сообщений, в результате того, что держатель не произвел аннулирования".

Замечания

67. Рабочая группа может пожелать отметить, что если единообразные правила, касающиеся подписей в цифровой форме, будут предусматривать, что аннулирование сертификата вступает в силу в момент его получения сертификационным органом, то пункт 4 проекта статьи H (Ответственность) может быть исключен, поскольку не может быть основания для ответственности сертификационного органа за вину или небрежность при регистрации аннулирования.

5. Регистр сертификатов

68. "Проект статьи G

1) Уполномоченный сертификационный орган ведет общедоступный электронный регистр выданных сертификатов, указывающий, когда отдельный сертификат был выдан, когда истекает срок его действия и когда его действие было приостановлено или он был аннулирован.

2) Регистр хранится сертификационным органом в течение по меньшей мере [10] лет после даты аннулирования или истечения срока действия любого сертификата, выданного этим сертификационным органом".

Замечания

69. Рабочая группа может пожелать обсудить вопрос о том, должен ли регистр сертификатов быть общедоступным или же, возможно, существует какая-то необходимость ограничить доступ к нему заинтересованными сторонами. Что касается периода времени, в течение которого следует сохранять такой регистр, то Рабочая группа может пожелать рассмотреть вопрос о том, следует ли предусмотреть в качестве отдельного единообразного правила какой-либо фиксированный период времени, следует ли оставить определение продолжительности такого периода на усмотрение принимающих государств или же она должна попытаться установить более гибкий критерий,

например, указав, что регистр должен быть доступным для проверки подлинности сертификатов в течение срока действия каждого сертификата и до момента истечения периода времени, в течение которого сообщения, подписанные в цифровой форме согласно сертификатам сертификационного органа, будут использоваться или должна проверяться их подлинность, что может вызвать необходимость предусматривать несколько периодов времени в зависимости от действующих законов о погасительной и исковой давности.

6. Ответственность

70. "Прект статьи H

1) Уполномоченный сертификационный орган несет ответственность перед любым лицом, которое действовало добросовестно, полагаясь на сертификат, выданный этим сертификационным органом, за любой ущерб, вызванный пороками в регистрации, произведенной сертификационным органом, техническими поломками или аналогичными обстоятельствами [даже если этот ущерб не возник в результате][если этот ущерб возник в результате] небрежности сертификационного органа.

2) Вариант X Ответственность за любой отдельный ущерб не превышает [сумма]. ...[принимающее государство указывает орган или ведомство, компетентное пересмотреть размер максимальной суммы] может регулировать размер этой суммы один раз в два года с целью отразить изменения цен.

Вариант Y ...[принимающее государство указывает орган или ведомство, компетентное принимать постановления в отношении ответственности] может принимать постановления в отношении ответственности сертификационных органов.

3) В случае, если сторона, которая понесла ущерб, содействовала этому преднамеренно или в результате небрежности, размер компенсации может быть уменьшен или же она может не предоставляться.

[4) Если уполномоченный сертификационный орган получил уведомление об аннулировании сертификата, этот орган немедленно регистрирует такое аннулирование. Если данный орган не делает этого, то он несет ответственность за любой ущерб, понесенный в результате этого пользователем.]

Замечания

71. Рабочая группа может пожелать рассмотреть вопрос о том, следует ли расширить положение об ответственности с целью охвата других случаев, помимо небрежности сертификационного органа. Рабочая группа может также пожелать определить, должна ли и в какой степени применяться автономия сторон, с тем чтобы позволить сертификационным органам контролировать, по конфиденциальной договоренности с пользователями, меру, в которой они должны нести ответственность.

72. Рабочая группа может пожелать рассмотреть возможность включения следующего положения о "безопасной гавани":

"Сертификационный орган, который соблюдает [настоящий Закон][настоящие Правила] и любой применимый закон или договор, не несет ответственности за любой ущерб, который

1) понес держатель сертификата, выданного этим сертификационным органом, вследствие доверия держателя к этому сертификату, или

2) причинен вследствие доверия к сертификату, выданному этим сертификационным органом, к подписи в цифровой форме, подлинность которой может быть проверена

посредством обращения к публичному ключу, указанному в сертификате, выданном этим сертификационным органом, или к информации, представленной в таком сертификате".

7. Вопросы, касающиеся перекрестной сертификации

73. "Проект статьи I

1) Сертификаты, выданные иностранными сертификационными органами, могут использоваться для подписей в цифровой форме на тех же условиях, что и подписи в цифровой форме, подпадающие под действие [настоящего Закона][настоящих Правил], если они признаются уполномоченным сертификационным органом и этот уполномоченный сертификационный орган гарантирует, в той же мере, что и свои собственные сертификаты, правильность пунктов сертификата, а также его действительность и законную силу.

2) ...[принимающее государство указывает орган или ведомство, компетентное устанавливать правила в связи с одобрением иностранных сертификатов] управомочен одобрять иностранные сертификаты и устанавливать конкретные правила для такого одобрения.

Замечания

74. Проект статьи I основывается на том понятии, что признание иностранных сертификатов должно осуществляться под ответственность местного сертификационного органа на основе взаимности. При обсуждении вопросов перекрестной сертификации Рабочая группа может пожелать рассмотреть вопрос о том, следует ли требовать полной взаимности или же гарантии правильности и действительности иностранных сертификатов необязательно могут предоставляться на одном и том же уровне всеми органами, которые будут являться частью схемы перекрестной сертификации. Рабочая группа может также пожелать рассмотреть вопрос о том, следует ли в обязательном порядке требовать вмешательства правительства для признания иностранных сертификатов.

75. В качестве возможной альтернативы проекту статьи I Рабочая группа может рассмотреть подход, принятый в проекте законодательства в некоторых странах, согласно которому признание иностранных сертификатов может быть предоставлено только на основе двусторонних или многосторонних международных соглашений.

8. Взаимоотношения между пользователями и сертификационными органами

76. "Проект статьи J

1) Сертификационному органу разрешено запрашивать только такую информацию, которая является необходимой для идентификации пользователя.

2) По просьбе юридических или физических лиц, сертификационный орган предоставляет информацию о следующем:

a) условиях, на которых сертификат может использоваться;

b) условиях, связанных с использованием подписей в цифровой форме;

c) расходах, связанных с использованием услуг сертификационного органа;

d) политике или практике сертификационного органа в отношении использования, хранения и передачи информации личного характера;

e) технических требованиях сертификационного органа в отношении оборудования связи пользователя;

f) условиях, на которых сертификационный орган может направлять пользователям предупреждения в случае сбоев или неисправностей в функционировании оборудования связи;

g) любом ограничении ответственности сертификационного органа;

h) любых ограничениях, налагаемых сертификационным органом на использование сертификата;

i) условиях, на которых пользователь имеет право устанавливать ограничения в отношении использования сертификата.

2) Информация, указанная в пункте 1, предоставляется пользователю до заключения окончательного соглашения о сертификации. [Такая информация может быть предоставлена сертификационным органом в виде заявления о практике сертификации].

3) При условии направления уведомления за [один месяц] пользователь может расторгнуть соглашение о связи с сертификационным органом. Такое уведомление о расторжении вступает в силу в момент его получения сертификационным органом.

4) При условии направления уведомления [за три месяца] сертификационный орган может расторгнуть соглашение о связи с сертификационным органом. Такое уведомление о расторжении вступает в силу в момент его получения".

III. ВКЛЮЧЕНИЕ ПУТЕМ ССЫЛКИ

A. Предыдущее обсуждение

77. На двадцать восьмой сессии Рабочей группы было внесено предложение включить в проект типового закона ЮНСИТРАЛ о правовых аспектах электронного обмена данными (ЭДИ) и соответствующих средствах передачи данных положение, обеспечивающее признание того, что определенные условия, которые могут быть включены в запись данных посредством простой ссылки, будут иметь такую же юридическую силу, как если бы они в полном объеме были изложены в тексте этой записи данных. Было отмечено, что вопрос о включении путем ссылки определенных условий в сообщение ЭДИ имеет принципиальное значение для пользователей ЭДИ и что поэтому особенно важно обеспечить определенность в отношении порядка использования этого метода. Была высказана мысль о том, что ЭДИ, по всей видимости, представляет собой систему включения путем ссылки, поскольку сообщения ЭДИ не имеют смысла и весомого значения для заключения контракта без включения путем ссылки соответствующих стандартов передачи. Было решено, что Рабочая группа рассмотрит на одной из своих будущих сессий вопрос о включении условий в запись данных посредством простой ссылки на такие условия (A/CN.9/406, пункты 90 и 178).

78. На ее двадцать девятой сессии Рабочей группе были представлены два предложения по проекту положения о включении путем ссылки: одно — наблюдателем от Международной торговой палаты (A/CN.9/WG.IV/WP.65) и второе — Соединенным Королевством Великобритании и Северной Ирландии (A/CN.9/WG.IV/WP.66). Большинство придерживалось мнения о том, что этот вопрос недостаточно глубоко проработан для его включения в Типовой закон и требует дальнейшего изучения. Было отмечено, что оба предложения, представленные Рабочей группе, нуждаются в дальнейшей доработке по целому ряду вопросов, таких, как какого рода условия предполагается включать и при каких обстоятельствах. Кроме того, как было отмечено, может создаться впечатление, что оба эти предложения противоречат общим нормам договорного права. А также было указано, что вопрос включения путем ссылки в условиях применения электронных сообщений нет необходимости рассматривать в Типовом законе, поскольку с ним связаны по сути те же проблемы, что и с вопросом включения путем ссылки в условиях работы с бумажными документами, которые регулируются общим договорным правом. Наконец, было отмечено, что положение, определяющее разницу между включением путем ссылки в условиях использования бумажных документов и включением путем

ссылки сообщений ЭДИ, противоречило бы подходу, которого до сих пор придерживалась Рабочая группа и который направлен на обеспечение равного режима вне зависимости от носителя информации. В ответ было заявлено, что среди практиков широко распространено мнение о том, что вопрос включения путем ссылки в условиях ЭДИ носит более сложный характер, чем в условиях использования бумажных документов, например, в силу большего числа посылаемых сообщений, а также вследствие того, что характер условий, включаемых путем ссылки, возможно, труднее определить, если они существуют в форме сообщения данных. Кроме того, практики испытывают потребность в конкретных положениях, которые регулировали бы включение путем ссылки в условиях использования электронных сообщений. Другой момент заключается в том, что ввиду большого числа сообщений данных, задействованных при установлении конкретных договорных отношений посредством ЭДИ, вероятность возникновения проблемы, известной как "война форм", особенно велика в условиях обмена электронными сообщениями. Рабочая группа решила, что вопрос о включении путем ссылки, возможно, нуждается в дальнейшем рассмотрении в контексте будущей работы (A/CN.9/407, пункты 100—105 и 117).

79. На своей тридцатой сессии Рабочая группа в целом согласилась с тем, что работа по вопросу о включению путем ссылки в условиях ЭДИ является необходимой. Была высказана точка зрения о том, что в ходе любых попыток выработки правовых норм, касающихся включения в сообщения данных таких положений о ссылке, необходимо выполнить следующие три условия: (1) положение о ссылке должно быть включено в сообщение данных; (2) содержание документа, на который делается ссылка, например, общие условия, должно быть фактически известно стороне, против которой может использоваться документ, на который делается ссылка; и (3) данная сторона должна выразить согласие с документом, на который делается ссылка, помимо того, что он должен быть ей известен. По общему мнению, тема о включении путем ссылки может быть надлежащим образом рассмотрена в контексте более общей работы по вопросам регистров и поставщиков услуг (A/CN.9/421, пункт 114). На своей двадцать девятой сессии Комиссия достигла общей договоренности о том, что этим вопросом можно заняться в контексте работы по сертификационным органам (A/51/17, пункт 222).

B. Вероятная необходимость в разработке единообразных правил, касающихся включения путем ссылки

80. Включение путем ссылки представляет собой удобный способ сделать в каком-либо документе общую ссылку на положения, которые подробно изложены где-либо еще, вместо того, чтобы воспроизводить их полностью. Например, оно устраняет необходимость излагать обширные положения условий, касающихся стандартов, при проведении переговоров или заключении контрактов. Таким образом, эти условия могут быть внесены в документ или сообщение данных, которое содержит ссылку на них, просто путем достаточно точной идентификации этих условий и указания на намерение их включить. В условиях использования электронных сообщений включение путем ссылки может быть определено как метод включения одного сообщения или записи данных (или части содержащейся в нем информации) в состав другого отдельного сообщения или записи данных путем ссылки в нем на первое сообщение или запись в тексте второго и путем заявления о том, что первое сообщение или запись должны восприниматься или рассматриваться в качестве части второго сообщения или записи, как если бы они были полностью изложены в их тексте.

1. Традиционные правила, разработанные в условиях использования бумажных документов

a) Включение путем ссылки

81. В условиях использования сообщений в форме бумажных документов известны правовые вопросы, возникающие в связи с включением путем ссылки, и во многих правовых системах существуют правовые нормы, устанавливающие правовые условия, согласно которым информация, изложенная не полностью в каком-либо письменном документе, может на законных основаниях считаться частью этого документа. Например, согласно некоторым условиям ссылка на один или несколько ИНКОТЕРМС, таких, как "перевозка оплачена" (CPT) или "перевозка и страхование оплачены" (CIP), может быть включена в заказ на поставку или в счет-фактуру, в результате чего данные ИНКОТЕРМС будут рассматриваться в качестве одного из условий соответствующего договора

купли-продажи без фактического определения условий "CPT" или "CIP", изложенного полностью в каких-либо договорных документах. Включению ИНКОТЕРМС путем ссылки может способствовать то обстоятельство, что такие термины были разработаны Международной торговой палатой (МТП) конкретно для включения в договоры посредством использования их акронимов или сокращенных обозначений, которые широко известны и рекомендованы для использования как МТП, так и ЮНСИТРАЛ. Другим примером текста, который часто включается путем ссылки, являются Унифицированные правила и обычаи для документарных аккредитивов (УПО 500), разработанные МТП. Правовая аргументация в отношении разрешения включать такие тексты, как УПО 500, в какой-либо договор зачастую основывается на признании того, что такой текст отражает широко известную и признанную практику во всем мире и, как предполагается, известен всем заинтересованным сторонам.

82. В тех случаях, когда такое предположение не применимо, условия, установленные внутригосударственным правом для придания юридической силы включению путем ссылки, могут быть сопряжены с жесткими требованиями, такими, как фактическое знание всеми сторонами информации, включенной путем ссылки, или даже прямое одобрение этой информации стороной, против которой возбуждена процедура принудительного исполнения. Однако согласно некоторым национальным законодательствам требования к приданию юридической силы включению путем ссылки являются более мягкими. Например, некоторые традиционные правовые критерии включения путем ссылки могут сосредоточиваться на ясности положения, с помощью которого производится включение путем ссылки, и на доступности информации, включаемой путем ссылки.

b) "Война форм"

83. Вопрос о включении путем ссылки не следует смешивать с вопросом, который обычно называют "войной форм". Война форм может возникать в том случае, когда, например, общие условия договора, предлагаемые покупателем, изложены мелким шрифтом на обороте его заказа на поставку, тогда как отличающаяся от них совокупность общих условий изложена на обороте счета-фактуры, выданной продавцом. Если покупатель и продавец не заключили конкретного соглашения в отношении того, какие условия будут применяться к данному договору, и две находящиеся в противоречии совокупности положений и условий были сообщены сторонами на обороте их договорных документов, то может возникнуть необходимость устранения неопределенности в отношении того, какие именно условия будут регламентировать эту сделку. Во многих странах с целью устранения такой неясности были разработаны соответствующие нормы договорного права.

2. Вопросы, возникающие в условиях электронной торговли

a) Широкое использование включения путем ссылки

84. Включение путем ссылки имеет важное значение для широкого использования электронного обмена данными (ЭДИ), электронной почты, сертификатов в цифровой форме и других форм электронной торговли. Например, стандартные сообщения ЭДИ и электронные сообщения в целом обычно сруктурируются таким образом, что имеет место обмен большим числом сообщений, причем каждое сообщение содержит сжатую информацию и намного чаще, чем бумажные документы, полагается на ссылку на информацию, доступную где-либо еще. В ЭДИ и других высокоструктурированных и форматированных видах данных обычно широко используется включение путем ссылки для повышения эффективности обработки данных. На предыдущих сессиях Рабочей группы указывалось, что различные формы электронной торговли по существу являются системами включения путем ссылки. На практике сообщения ЭДИ потенциально являются менее определенными с правовой точки зрения, если только не обеспечена ясность в отношении действительности и юридической силы включения путем ссылки соответствующих правовых, технических и административных условий, положений, соглашений, стандартов, норм или руководящих принципов, которые могут быть применимыми к этим сообщениям.

85. Что касается ситуаций, когда возникает "война форм" в условиях использования бумажных документов, то следует иметь в виду, что системы передачи электронных сообщений не призваны и

даже не оборудованы для передачи с каждым сообщением таких текстов, как общие условия, обычно напечатанные на обороте бумажных документов. Включение всех соответствующих условий было бы дорогостоящим и неэффективным. Это замедлило бы и, возможно, застопорило бы передачу электронных сообщений и, может быть, даже снизило бы эффективность уведомления, вынуждая участвующие стороны распечатывать, или просматривать на экране такие длинные тексты. Поэтому необходимо разработать правила относительно того, каким образом такие тексты можно считать включенными в какое-либо сообщение. Цель таких правил должна заключаться в уменьшении, если это возможно, в условиях использования электронных сообщений таких трудностей, которые возникают в результате войны форм в условиях применения бумажных документов, или, по крайней мере, обеспечении того, чтобы решения, разработанные во многих национальных законодательствах для устранения таких трудностей в условиях использования бумажных документов, применялись бы также в условиях использования электронных сообщений. Следует отметить, что разработка таких правил не обязательно повлечет за собой изменение решений, которые могут вытекать из действующего внутригосударственного права и предусматривать возможные пути разрешения ситуации, сопряженной с "войной форм".

86. Стандарты включения сообщений данных путем ссылки в другие сообщения данных могут также иметь важное значение для использования сертификатов публичных ключей, поскольку эти сертификаты обычно представляют собой краткие записи с жестко предписываемым содержанием, которые являются ограниченными по размеру. Однако доверенная третья сторона, которая выдает сертификат, вероятно, потребует включения соответствующих пунктов, ограничивающих ее ответственность. Поэтому сфера действия, цели и юридическая сила сертификата в коммерческой практике будут неясными и неопределенными без внешних условий, включаемых путем ссылки. Это особенно касается случая международной передачи сообщений с участием различных сторон, которые придерживаются разной торговой практики и обычаев.

87. На предыдущих сессиях Рабочей группы неоднократно указывалось, что установление стандартов для включения сообщений данных путем ссылки в другие сообщения данных имеет решающее значение для роста инфраструктуры компьютеризированной торговли. Без правовой определенности, которой способствуют такие стандарты, компьютеризированные торговые сделки отягощались бы включением большого объема материалов, становясь в результате громоздкими для участвующих сторон, а также для системы, облегчающей исполнение такой сделки. Без таких единообразных стандартов может возникать значительный риск того, что применение традиционных критериев для определения исковой силы условий, которые стремятся включить путем ссылки, может быть неэффективным, когда речь идет о применении к соответствующим условиям электронной торговли, вследствие различий между традиционным механизмом и механизмом электронной торговли. Например, некоторые традиционные правовые критерии включения путем ссылки могут предусматривать определение того, являются ли включаемые условия "ясными и четкими", содержат ли они "приемлемую формулировку ссылки, удостоверяющую прямое намерение включить", или же является ли предполагаемое включение "ясным и убедительным". Такие критерии могут создавать непреднамеренные барьеры содействию электронной торговле. Возможно, необходимы конкретные правила, поскольку методы, используемые для направления уведомления и обеспечения доступа к информации, могут быть различными в условиях применения бумажных документов и в электронной торговле с тем возможным последствием, что в некоторых юрисдикциях традиционные правила включения путем ссылки могут приводить к неоправданной дискриминации против электронной торговли.

b) Доступность включенного текста

88. Электронная торговля в значительной мере полагается на механизм включения путем ссылки. Однако в то же время доступность полного текста информации, на которую делается ссылка, может быть существенно улучшена путем использования электронных средств передачи сообщений. Например, какое-либо сообщение может содержать единообразные ресурсные обнаружители (ЕРО), которые отправляют читателя к справочному документу. Такие ЕРО могут обеспечивать "гипертекстовые связи", позволяющие читателю просто направить указывающее устройство (такое, как "мышь") на ключевое слово, связанное с каким-либо ЕРО, и справочный текст появится.

89. Такие же методы могут использоваться в условиях обмена электронными сообщениями для обеспечения всем пользователям легкого доступа к самым разнообразным текстам, таким, как: (1) тексты, воплощающие установившуюся коммерческую практику (например, УПО 500); (2) технические стандарты, регламентирующие передачу сообщений; (3) заявления о практике сертификации, сделанные сертификационными органами; и (4) более конкретная информация, например об общих договорных условиях какой-либо компании. Однако на эти методы нельзя с уверенностью полагаться, не имея стандартов, касающихся включения сообщений данных путем ссылки в другие сообщения данных.

90. Необходимость разработки правил, касающихся включения путем ссылки в условиях использования электронных сообщений, обусловливается частотой, с которой сообщения данных содержат ссылки на информацию, зафиксированную где-либо еще, а также наличием технических средств, позволяющих проверить подлинность такой информации легче и быстрее, чем в условиях использования бумажных документов.

C. Возможные положения

91. При разработке возможных положений, касающихся включения путем ссылки в электронной торговле, Рабочая группа может пожелать принять во внимание то, что в некоторых юрисдикциях существующие правила, разработанные для применения в условиях использования бумажных документов, основываются на озабоченности по поводу того, что включенные условия или другая информация должны быть надлежащим образом доведены до сведения адресата или какой-либо третьей стороны, в зависимости от случая. Если такие нормы права существуют, то, может быть, целесообразно применять их независимо от того, осуществляется ли включение путем ссылки с помощью ЭДИ или какого-либо другого средства передачи сообщений.

92. Тем не менее представляется возможным сформулировать общий принцип, разъясняющий, что включение путем ссылки является правомерным в электронной торговле при условии разъяснения того, что этот принцип не затрагивает какие-либо нормы, которые могут существовать и касаться: 1) необходимости доведения содержания или местонахождения условий или другой информации до сведения любой стороны, к которой они применимы, или же их предоставления данной стороне; или 2) любого правового требования о том, что условия должны быть приняты, прежде чем они могут стать частью договора. Этот важный принцип заключается в том, что использование включения путем ссылки должно быть признано, с тем чтобы тот факт, что информация изложена лишь где-либо еще, сам по себе не препятствовал включению этой информации в сообщение данных, в котором содержатся ссылка на нее.

93. Рабочая группа может пожелать возобновить рассмотрение вопросов включения путем ссылки на основе следующих двух вариантов:

Вариант A

Если не согласовано иное, когда ссылка на [надлежащим образом] [разумным образом] доступные условия, положения, соглашения, стандарты, нормы или руководящие принципы полностью или частично содержится в каком-либо сообщении данных с [явным] намерением включить их в качестве части содержания или обеспечить каким-либо иным образом их юридическую силу, эти условия считаются включенными путем ссылки в это сообщение данных. В отношениях между сторонами такие условия считаются настолько юридически действительными и обязательными, как если бы они были полностью изложены в этом сообщении данных, насколько это допускается законом.

Вариант B

1) Настоящая статья применяется тогда, когда информация, записанная или переданная в сообщении данных, содержит ссылку, или может быть полностью удостоверена только с помощью такой ссылки, на информацию, записанную где-либо еще ("последующая информация").

2) При соблюдении пункта 3 сообщение данных имеет такую же силу, как если бы последующая информация была полностью изложена в этом сообщении данных или могла быть удостоверена только с помощью ссылки на нее, если в этом сообщении данных:

a) идентифицируется последующая информация:

i) путем указания общего наименования или описания; и

ii) путем определения записи, и частей этой записи, содержащей последующую информацию, и, когда эта запись не является общедоступной, места, в котором ее можно найти; и

b) прямо указывается или ясно подразумевается, что это сообщение данных должно иметь такую же силу, как и в случае, если бы последующая информация была полностью изложена в этом сообщении данных.

3) Ничто в настоящей статье не затрагивает:

a) какой-либо нормы права, требующей направления надлежащего уведомления о содержании информации, записанной где-либо еще, или о записи или месте, где такая информация может быть найдена, или требующей обеспечения доступа к этой записи или месту для другого лица; или

b) какой-либо нормы права, касающейся акцепта оферты с целью заключения договора.