ОРГАНИЗАЦИЯ
ОБЪЕДИНЕННЫХ НАЦИЙ

A

Генеральная Ассамблея

Distr.
LIMITED

A/CN.9/WG.IV/WP.73
12 December 1997

RUSSIAN
ORIGINAL: ENGLISH

КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ
Рабочая группа по электронной торговле
Тридцать вторая сессия
Вена, 19—30 января 1998 года

ПРОЕКТ ЕДИНООБРАЗНЫХ ПРАВИЛ О ПОДПИСЯХ В ЭЛЕКТРОННОЙ ФОРМЕ

Записка Секретариата

СОДЕРЖАНИЕ

V.97-29153

ВВЕДЕНИЕ

1. Комиссия на ее двадцать девятой сессии (1996 года) приняла решение включить в свою повестку дня вопросы о подписях в цифровой форме и сертификационных органах. Рабочей группе по электронной торговле было предложено рассмотреть целесообразность и возможность подготовки единообразных правил по этим темам. Было выражено согласие с тем, что работа, которая должна быть проведена Рабочей группой на ее тридцать первой сессии, может охватывать подготовку проекта правил по определенным аспектам вышеуказанных тем. Рабочей группе было предложено представить Комиссии достаточные элементы для принятия обоснованного решения в отношении рамок единообразных правил, которые будут разрабатываться. Что касается более четкого мандата для Рабочей группы, было достигнуто согласие о том, что единообразные правила, которые следует подготовить, должны охватывать такие вопросы, как: правовая основа, поддерживающая процессы сертификации, включая появляющуюся технологию удостоверения подлинности и сертификации в цифровой форме; применимость процесса сертификации; распределение риска и ответственности пользователей, поставщиков и третьих сторон в контексте использования методов сертификации; конкретные вопросы сертификации через применение регистров; и включение путем ссылки[1].

2. На тридцатой сессии Комиссии (1997 года) ей был представлен доклад Рабочей группы о работе ее тридцать первой сессии (A/CN.9/437). Что касается целесообразности и возможности подготовки единообразных правил по вопросам подписей в цифровой форме и сертификационных органов, Рабочая группа сообщила Комиссии, что она достигла консенсуса в отношении важного значения и необходимости работы в направлении согласования норм права в этой области. Хотя она не приняла окончательного решения в отношении формы и содержания такой работы, она пришла к предварительному выводу о том, что практически можно подготовить проект единообразных правил по крайней мере по вопросам подписей в цифровой форме и сертификационных органов и, возможно, по связанным с этими вопросами проблемам. Рабочая группа напомнила о том, что наряду с подписями в цифровой форме и сертификационными органами в рамках будущей работы в области электронной торговли, возможно, также потребуется рассмотреть следующие темы: вопросы технических альтернатив криптографии публичных ключей; общие вопросы о функциях, выполняемых поставщиками услуг, являющимися третьими сторонами; и заключение контрактов в электронной форме (A/CN.9/437, пункты 156—157). В отношении вопроса включения путем ссылки Рабочая группа пришла к выводу о том, что необходимость в проведении Секретариатом дальнейшего исследования отпала, поскольку основополагающие вопросы хорошо известны и поскольку ясно, что многие аспекты "войны форм" и договоров присоединения необходимо будет оставить на урегулирование на основе применимых национальных законов в силу причин, связанных, в частности, с защитой потребителей и другими соображениями публичного порядка. Рабочая группа решила, что этот вопрос должен быть рассмотрен в качестве первого основного пункта ее повестки дня в начале следующей сессии (A/CN.9/437, пункт 155).

3. Комиссия дала высокую оценку работе, выполненной Рабочей группой на ее тридцать первой сессии, одобрила заключения Рабочей группы и поручила ей подготовить единообразные правила по юридическим вопросам подписей в цифровой форме и сертификационных органов (именуемые в дальнейшем "Единообразные правила").

4. В отношении конкретной сферы применения и формы Единообразных правил Комиссия пришла к общему мнению, что на данном начальном этапе принятие решения невозможно. Было сочтено, что, хотя Рабочая группа может надлежащим образом сосредоточить свое внимание на вопросах подписей в цифровой форме с учетом предполагаемой ведущей роли криптографии публичных ключей в зарождающейся практике электронной торговли, Единообразные правила должны соответствовать нейтральному с точки зрения носителей средств информации подходу, который взят за основу в Типовом законе ЮНСИТРАЛ об электронной торговле. Таким образом, Единообразные правила не должны исключать использование других методов удостоверения подлинности. Кроме того, при решении вопроса криптографии публичных ключей в Единообразных правилах, возможно, необходимо будет учесть различия в уровнях безопасности и признать различные юридические последствия и уровни ответственности, соответствующие разным видам услуг, оказываемых в контексте подписей в цифровой форме. Что касается сертификационных органов, то Комиссия, хотя она и признала ценность стандартов, определяемых рыночными отношениями, в целом согласилась с тем, что Рабочая группа может надлежащим образом предусмотреть разработку минимального свода стандартов, которые должны будут

строго соблюдаться сертификационными органами, особенно в случае необходимости трансграничной сертификации.

5. В качестве дополнительного вопроса, подлежащего рассмотрению в контексте будущей работы в области электронной торговли, было указано на то, что Рабочей группе, возможно, придется на более позднем этапе обсудить вопросы юрисдикции, применимого права и урегулирования споров на основе использования сети Интернет. Комиссия была информирована, что в июне 1997 года под эгидой Гаагской конференции по международному частному праву будет проведен коллоквиум по вопросам юрисдикции и применимого права в рамках Интернет. Комиссии было также сообщено о том, что на международной конференции, которую проводит Организация экономического сотрудничества и развития (ОЭСР) в ноябре 1997 года, будет предпринята попытка выработать скоординированный подход заинтересованных правительств, межправительственных организаций, неправительственных организаций и групп предпринимателей частного сектора к вопросам электронной торговли. Комиссия выразила надежду, что Секретариат сможет принять участие в этих двух мероприятиях и представить доклад об их работе[2].

6. Данная записка содержит пересмотренный проект положений, подлежащих рассмотрению для возможного их включения в Единообразные правила. Эти положения касаются подписей в цифровой форме, других электронных подписей, сертификационных органов и соответствующих правовых вопросов. Они подготовлены по материалам обсуждений и в соответствии с решениями, принятыми Рабочей группой на ее тридцать первой сессии и содержащимися в докладе о работе этой сессии (A/CN.9/437), а также по материалам обсуждений и в соответствии с решениями, принятыми Комиссией на ее тридцатой сессии и изложенными выше. В частности, проект положений основан на принятой Рабочей группой рабочей гипотезе о том, что ее деятельность в области подписей в цифровой форме будет состоять в выработке проектов законодательных положений (A/CN.9/437, пункт 27). Проект положений должен также соответствовать принятому Рабочей группой на своей предыдущей сессии решению, в соответствии с которым возможные единообразные правила, касающиеся подписей в цифровой форме, должны быть подготовлены на основе статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле (именуемого в дальнейшем "Типовой закон") и должны рассматриваться как устанавливающие порядок, при котором может использоваться надежный метод "для идентификации лица" и "указания на то, что это лицо согласно" с информацией, содержащейся в сообщении данных. В целом до принятия окончательного решения относительно взаимосвязи между Типовым законом, Единообразными правилами и возможными правилами для включения путем ссылки (см. A/CN.9/437, пункты 151—155) данный проект положений должен соответствовать закрепленным в Типовом законе принципам и использованной в нем терминологии (A/CN.9/437, пункт 26).

7. В настоящей записке не затрагиваются вопросы юрисдикции, применимого права и урегулирования споров на основе использования сети Интернет, вопросы заключения и исполнения контрактов через посредство электронных средств связи, а также любые другие вопросы, которые, возможно, необходимо будет рассмотреть на одной из последующих сессий Рабочей группы. Рабочей группе будет представлен устный доклад о коллоквиуме по вопросам юрисдикции и применимого права в рамках Интернет, который состоялся в июне 1997 года под эгидой Гаагской конференции по международному частному праву, а также о конференции, проведенной ОЭСР в ноябре 1997 года (см. пункт 5, выше).

8. В подготовке настоящей записки Секретариату помогала группа экспертов, в состав которой входили как эксперты, приглашенные Секретариатом, так и эксперты, назначенные заинтересованными правительствами и международными организациями.

I. ОБЩИЕ ЗАМЕЧАНИЯ

9. Цель Единообразных правил, как это отражено в проекте положений, представленном в части II настоящей записки, состоит в том, чтобы облегчить все расширяющееся использование электронных подписей в международных хозяйственных сделках. Основываясь в качестве исходного материала на множестве уже действующих или разрабатываемых в ряде стран законодательных документов, данный проект положений имеет целью предотвратить разночтения в правовых нормах, применимых к электронной торговле, путем установления свода стандартов, на базе которых можно будет определять — возможно, с помощью сертификационных органов, для чего также предлагаются некоторые основные правила, — юридические последствия использования подписей в цифровой форме и других электронных подписей.

10. Уделяя особое внимание частно-правовым аспектам коммерческих сделок, Единообразные правила не предназначены для разрешения всех вопросов, которые могут возникнуть в связи со все расширяющимся использованием электронных подписей. Так, в частности, в Единообразных правилах не затрагиваются аспекты государственной политики, административного права, права потребителей и уголовного права, которые, возможно, необходимо учитывать национальным законодательным органам при установлении всеобъемлющих правовых рамок использования электронных подписей.

11. Будучи основанными на Типовом законе, Единообразные правила призваны, в частности, отражать: принцип нейтральности с точки зрения носителей информации; подход, в соответствии с которым не должны дискриминироваться функционально эквивалентные традиционные принципы и практики использования бумажных документов; а также расширение толкования автономии сторон. Они предназначаются для применения как в качестве минимальных стандартов в "открытой" среде (то есть когда стороны связываются между собой по электронным средствам связи без предварительной договоренности), так и в качестве правил умолчания в "закрытой" среде (то есть когда стороны связаны правилами и процедурами в связи с ранее заключенными контрактами, которым они должны следовать при использовании электронных средств связи).

II. ПРОЕКТ ПОЛОЖЕНИЙ О ПОДПИСЯХ В ЦИФРОВОЙ ФОРМЕ, ДРУГИХ ЭЛЕКТРОННЫХ ПОДПИСЯХ, СЕРТИФИКАЦИОННЫХ ОРГАНАХ И СООТВЕТСТВУЮЩИХ ПРАВОВЫХ ВОПРОСАХ

РАЗДЕЛ I. СФЕРА ПРИМЕНЕНИЯ И ОБЩИЕ ПОЛОЖЕНИЯ

12. При рассмотрении проекта положений, предлагаемых для включения в Единообразные правила, Рабочая группа может пожелать рассмотреть в более общем плане взаимосвязь между Единообразными правилами и Типовым законом. В частности, Рабочая группа может пожелать внести в Комиссию предложения, предусматривающие либо представление единообразных правил о подписях в цифровой форме в виде отдельного юридического документа, либо включение их в расширенный вариант Типового закона, например, в качестве новой части III Типового закона.

13. Представляется, что если Единообразные правила будут разработаны в качестве отдельного документа или как добавление к Типовому закону, они должны будут основываться на положениях, соответствующих статьям 1 (Сфера применения), 2 a), c) и e) (Определения "сообщения данных", "составителя" и "адресата"), 3 (Толкование), 7 (Подпись) и 13 (Атрибуция сообщений данных) Типового закона. Хотя эти статьи не воспроизводятся в настоящей записке, следует отметить, что проект положений Единообразных правил был подготовлен Секретариатом на основе предположения о том, что такие положения явятся частью Единообразных правил. Что касается сферы применения Единообразных правил, следует иметь в виду, что, согласно статье 1 Типового закона, сделки с участием потребителей — даже не будучи основным предметом регулирования Единообразных правил — не будут исключены из сферы их действия до тех пор, пока закон, применимый к сделкам с потребителями в государстве, которое вводит у себя в действие Единообразные правила, не вступит с ними в противоречие (см. A/CN.9/WG.IV/WP.71, пункты 49—50).

14. Что же касается вопроса автономии сторон, то простой ссылки на статью 4 (Изменение по договоренности) Типового закона для нахождения удовлетворительного решения может оказаться недостаточно ввиду того, что статья 4 устанавливает различие между положениями Типового закона, которые по условиям договора могут быть изменены, и теми положениями, которые следует рассматривать как обязательные, если только изменение по договоренности не допускается законом, применимым вне сферы действия Типового закона. В связи с вопросом об электронных подписях практическое значение "закрытых" сетей делает необходимым обеспечить широкое признание автономии сторон. Однако возможно, что придется принимать во внимание и государственную политику в плане ограничения свободы договоров, в том числе законы о защите потребителей от неправильно составленных типовых договоров. Поэтому Рабочая группа может пожелать включить в Единообразные правила положение, соответствующее статье 4 1) Типового закона и предусматривающее придание — если иное не установлено Единообразными правилами или каким-либо иным применимым законом — выданным, полученным или признанным в соответствии с согласованными между сторонами сделки процедурами электронным подписям и сертификатам той юридической силы, которая предусмотрена соответствующим соглашением. Кроме того, Рабочая группа может рассмотреть вопрос об установлении правила толкования, согласно которому при определении степени надежности, в связи с какой-либо конкретной целью, того или иного сертификата, электронной подписи или сообщения данных, проверяемых на основании соответствующего сертификата, следует принимать во внимание все связанные с ними соглашения, в которых участвуют стороны договора, а также любые варианты их поведения и все соответствующие торговые обычаи.

15. 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 (см. A/CN.9/WG.IV/WP.71, пункт 51).

РАЗДЕЛ II. ЭЛЕКТРОННЫЕ ПОДПИСИ

Часть I. Защищенные электронные подписи

Статья 1. Определения

Для целей настоящих Правил:

a) "Подпись" означает любой символ или любые виды процедур обеспечения защиты, используемые или принятые каким-либо лицом [или от имени какого-либо лица] с целью идентификации этого лица и указания на то, что это лицо согласно с информацией, к которой данная подпись прилагается;

b) "Электронная подпись" означает [подпись] [данные], исполненные в электронной форме и внесенные в текст либо приложенные к тексту, либо ассоциируемые с текстом сообщения [и используемые каким-либо лицом [или от имени какого-либо лица] с целью идентификации этого лица и указания на то, что это лицо согласно с информацией, содержащейся в сообщении данных] [и используемые с целью удовлетворения условиям [статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле]];

c) "Защищенная электронная подпись" означает электронную подпись, которая

i) представляет собой подпись в цифровой форме в значении статьи 4 и удовлетворяет требованиям, предусмотренным статьей 5; или

ii) на время ее исполнения может быть каким-либо иным образом удостоверена как подпись соответствующего конкретного лица посредством процедуры обеспечения защиты, а именно: связана исключительно с использующим ее лицом; дает возможность быстрой, объективной и автоматизированной идентификации этого лица; исполнена таким образом или с применением таких средств, которые подконтрольны лишь использующему ее лицу; и связана с сообщением данных, к которому она относится, таким образом, что изменение сообщения делает данную электронную подпись недействительной; или

iii) [во взаимоотношениях сторон, причастных — в ходе своей обычной работы — к созданию, отправлению, получению, хранению или обработке сообщений данных каким-либо иным способом] является разумной с коммерческой точки зрения в обстоятельствах, оговоренных заранее, и должным образом применяется сторонами.

Справочный материал

A/CN.9/437, пункты 29—50 и 90—113 (проекты статей A, B и C);
A/CN.9/WG.IV/WP.71, пункты 52—60.

Замечания

16. Проект статьи 1 должен отражать решение, принятое Рабочей группой на своей тридцать первой сессии, согласно которому Единообразные правила, в соответствии с нейтральным с точки зрения носителей информации подходом, принятым в Типовом законе, не должны препятствовать использованию любого метода, который в соответствии со статьей 7 Типового закона являлся бы "как надежным, так и соответствующим", в качестве альтернативы собственноручным и другим подписям на бумажных документах. Хотя основным предметом регулирования Единообразных правил могут стать вопросы подписей в цифровой форме, следует все же принять более общий подход и рассмотреть также вопросы, касающиеся других способов использования электронных подписей (см. A/CN.9/437, пункт 22).

17. Таким образом, в соответствии с определениями терминов "подпись" и "электронная подпись", данными в подпунктах a) и b), сфера применения Единообразных правил формулируется достаточно широко и охватывает все способы, которые могут быть применены для обеспечения функциональной эквивалентности собственноручной подписи, как это предусматривается статьей 7 Типового закона. Следует заметить, что определение термина "подпись", являющееся простым воспроизведением в форме определения пункта 1 a) статьи 7 Типового закона, не имеет целью заменить или каким-либо иным образом изменить определение терминов "подпись" или "собственноручная подпись", которые могут быть даны в других документах, помимо Единообразных правил (например, во внутреннем законодательстве или в прецедентном праве). Данное определение призвано служить главным образом в качестве основы для последующих определений терминов "электронная подпись" и "защищенная электронная подпись". Оно может быть использовано и как полезный справочный материал в странах, где еще не принято действующее определение термина "подпись".

18. Трехуровневое определение, содержащееся в проекте статьи 1 (то есть определение терминов "подпись", "электронная подпись" и "защищенная электронная подпись"), предназначено служить Рабочей группе аналитическим инструментом, а также отразить различия, ставшие привычными при разработке законодательства в ряде стран. Однако, в зависимости от содержания положений Единообразных правил, могут понадобиться не все эти три определения. Если Рабочая группа решит сосредоточить свое внимание на одном из правовых последствий использования электронных подписей (то есть на признании их в качестве функционального эквивалента собственноручным подписям), то потребуется рассмотрение лишь одной категории — "электронные подписи". В таком случае нынешние определения "электронная подпись" и "защищенная электронная подпись" могут быть объединены в одну

правовую категорию независимо от количества и разнообразия методов, подлежащих рассмотрению в рамках этой правовой категории.

19. Основное определение, из которого следует исходить при установлении сферы применения Единообразных правил, представлено в подпункте c) под заголовком "защищенная электронная подпись". В порядке редакции можно заметить, что слово "защищенная" не означает, что применение того или иного технического способа может фактически или юридически обеспечить абсолютную защиту. Оно используется лишь для обозначения более высокой степени достоверности электронной подписи согласно набору критериев, соответствие которым может повлечь за собой определенные правовые последствия.

20. Будучи предназначенным служить основой для определения правовых последствий, которые могут вытекать из использования электронных подписей, подпункт c) призван также отразить "двойственный подход", принятый Рабочей группой на ее предыдущей сессии. "Двойственный подход" возник на основе двух обсуждаемых альтернативных вариантов, а именно установление критериев для выдачи государством полномочий на деятельность сертификационных органов и признание оперативных критериев сертификационных органов, действующих за пределами созданной государством инфраструктуры для использования публичных ключей. Рабочая группа пришла к выводу, что оба эти подхода могут и не быть взаимоисключающими. Различие между двумя ситуациями может заключаться в условиях, при которых наступают различные правовые последствия, признаваемые за подписями в цифровой форме в одном и другом случае. Что касается сертификационных органов, уполномоченных ("лицензированных") государством, то выполнение сертификационным органом применимых оперативных критериев будет представлять собой предварительное условие для выдачи полномочий такому сертификационному органу, что, в свою очередь, будет условием признания юридической действительности сертификатов, выдаваемых этим сертификационным органом. Во второй ситуации сертификационному органу до начала его деятельности не нужно будет доказывать, что оперативные критерии выполнены. Однако, если выдаваемые им сертификаты будут оспариваться (например, в суде или арбитраже), разрешающему спор органу необходимо будет дать оценку надежности сертификата путем определения того, был ли он выдан сертификационным органом, удовлетворяющим этим критериям (см. A/CN.9/437, пункт 48).

21. Наряду с тем, что подпункт c) предусматривает возможность деятельности как лицензированных, так и нелицензированных сертификационных органов, он еще более расширяет сферу применения Единообразных правил, распространяя их действие на удостоверяющие подлинность устройства, при которых не требуется доверие к любого рода сертификационному органу или "заслуживающей доверия третьей стороне". Таким образом, ссылка на "защищенный" статус позволяет применять оба порядка лицензирования, с помощью которых государство, введшее в действие эти Правила, сможет определять качество и достоверность подписей в цифровой форме, а также устанавливать те виды рыночной практики, при которых можно полагаться на другие формы электронных подписей.

22. Согласно подпункту c) i), защищенный статус по данным Единообразным правилам будет предполагаться в том случае, если подпись в цифровой форме исполняется в соответствии с действующей инфраструктурой в государстве, вводящем данные Правила для использования публичных ключей. В отсутствие такой инфраструктуры или в дополнение к ней, а также при условии соблюдения соответствующих минимальных требований защищенный статус может быть предоставлен любому типу электронной подписи (то есть подписям в цифровой форме или другим электронным подписям, исполняемым при участии или без участия сертификационных органов или иных заслуживающих доверия третьих сторон). С целью установления базового стандарта, на основании которого может определяться качество подобных электронных подписей, в подпункт c) ii) внесены четыре критерия: исключительность, идентификация, надежность и связь с подписываемой информацией.

23. Требование, чтобы защищенная электронная подпись была "связана исключительно" с исполнившим ее лицом, призвано исключить какую бы то ни было вероятность — помимо случаев подделки или какого-либо иного ненадлежащего поведения — исполнения одной и той же подписи более чем одним лицом. Предполагается, что требование исключительности может также быть выполнено с применением подписи, имеющей биометрические параметры, которые включают некоторые особенности, присущие лишь исполнившему ее лицу, такими как отпечатки пальцев или снимок сетчатки глаза. Что касается подписи в цифровой форме, требование исключительности будет также удовлетворено в том случае, когда пара ключей, используемых исполняющим подпись лицом,

подбирается произвольно и имеет достаточную кодовую длину, а поэтому вероятность создания такого же сочетания пары ключей кем-нибудь еще чрезвычайно низкая.

24. Защищенная подпись должна иметь такие параметры, чтобы ее можно было использовать для идентификации подписавшегося. Это не означает, что сама подпись должна состоять из имени подписавшегося или включать его. Идентификация путем сверки с другими источниками информации будет достаточной. Так, например, с помощью подписи в цифровой форме можно идентифицировать подписавшегося путем сверки с сертификатом, выданным сертификационным органом. Главное требование состоит в том, чтобы процесс идентификации был относительно быстрым, объективным и автоматизированным. Хотя предполагается, что на основании собственноручной подписи можно идентифицировать подписавшегося, такая идентификация обычно не может быть осуществлена быстро и в автоматизированном режиме, а зачастую и не является объективной. Во многих случаях сама подпись не поддается прочтению. Но даже если она и поддается прочтению и с ее помощью можно в конечном счете идентифицировать подписавшегося, длительность и надежность процесса идентификации могут не всегда удовлетворять требованиям электронной торговли. Так, собственноручную подпись не всегда можно надежно идентифицировать как подпись того или иного конкретного лица (если не предполагать определенное допущение этого факта или наличие свидетеля акта подписания) без заключения эксперта-графолога, проведшего сравнительный анализ признанных подписей предполагаемого подписавшегося с данной конкретной подписью, требующей подтверждения. Результат в таком случае вряд ли может быть получен быстро или в автоматизированном режиме, а заключение эксперта будет во многих отношениях скорее субъективным, чем объективным. И наоборот, проверка персонального идентификационного номера (ПИН) через автоматический определитель даст банку возможность в автоматизированном режиме объективно и быстро установить, что данное конкретное лицо, снимающее деньги со счета, имеет конкретный адрес и конкретный номер счета. Такое лицо не сможет отрицать, что заявление о снятии денег содержит его подпись (хотя может отрицать, что подписывало это заявление; но этот вопрос уже относится к требованию о надежности).

25. Помимо идентификации лица как подписавшего сообщение, примененная при подписании процедура может послужить и разумно надежной гарантией того, что лицо, идентифицированное в качестве подписавшего, действительно подписало сообщение. Такому требованию надежности может удовлетворять защитная процедура, предписывающая следование определенному образу действий или применение определенных средств, которые находятся под исключительным контролем лица, являющегося автором подписи. Привлечение заслуживающей доверие третьей стороны может также явиться одним из способов повышения степени надежности. Требование надежности может быть удовлетворено и с помощью каких-либо иных средств. Рабочая группа может пожелать обсудить и другие подходы, с помощью которых возможно обеспечить приемлемую степень надежности.

26. Защищенная подпись должна быть привязана к подписываемому сообщению таким образом, что с изменением содержания сообщения подпись теряет действительность. Наличие такой привязки можно рассматривать как важнейшее требование к защищенной подписи, поскольку в противном случае подпись может быть просто изъята из одного сообщения и вставлена в другое.

27. Подпункты c) i) и ii) должны применяться в отсутствие предварительного договорного соглашения об электронных подписях, заключенного между отправителем и адресатом подписанного сообщения. Однако, если следовать подходу, принятому в Типовом законе, то может возникнуть необходимость в том, чтобы Единообразными правилами подтверждалась юридическая действительность договоров, в том что касается удостоверения подлинности сообщений. Поэтому подпункт c) iii) придает юридическую силу соглашениям, достигаемым в рамках закрытых систем. Рабочая группа может пожелать обсудить вопрос о том, нужно ли использовать формулировку, взятую в квадратные скобки ("во взаимоотношениях сторон, причастных — в ходе своей обычной работы — к созданию, отправлению, получению, хранению или обработке сообщений данных каким-либо иным способом") и отражающую формулировку Типового закона, для ограничения последствий автономии сторон с точки зрения делового использования электронных подписей вплоть до исключения из этой сферы потребительских сделок (см. A/CN.9/437, пункт 24).

Статья 2. Презумпции

1) В отношении сообщения данных, подлинность которого удостоверяется при помощи защищенной электронной подписи, исходят из опровержимой презумпции, что:

a) сообщение данных не было изменено с момента приложения к нему защищенной электронной подписи;

b) защищенная электронная подпись является подписью лица, к которому она относится; и

c) защищенная электронная подпись была приложена этим лицом с намерением подписать сообщение.

2) В отношении сообщения данных, подлинность которого удостоверяется при помощи электронной подписи, не являющейся защищенной, ничто в настоящих Правилах не затрагивает действующие юридические или доказательные нормы, относящиеся к бремени доказывания подлинности или целостности сообщения данных или электронной подписи.

3) Положения настоящей статьи не применяются к следующему: [...].

[4) Презумпции, содержащиеся в пункте 1), могут быть опровергнуты:

a) доказательствами того, что защитная процедура, примененная для проверки электронной подписи, не должна быть в целом признана как заслуживающая доверия в силу развития техники, использованной процедуры обеспечения защиты или по каким-либо иным причинам;

b) доказательствами того, что процедура обеспечения защиты, согласованная сторонами в соответствии со статьей 1 c) iii), не была проведена заслуживающим доверия образом; или

c) доказательствами, связанными с фактами, о которых доверяющая сторона была осведомлена, что они могут свидетельствовать о неразумности проявления доверия к данной защитной процедуре. Коммерческая разумность процедуры обеспечения защиты, согласованной сторонами в соответствии со статьей 1 c) iii), должна определяться с учетом целей процедуры и коммерческих обстоятельств на момент достижения сторонами согласия о принятии этой процедуры, включая характер сделки, опыт сторон, объем аналогичных сделок, заключенных одной или обеими сторонами, наличие альтернативных вариантов, предложенных соответствующей стороне, но отвергнутых ею, стоимость альтернативных процедур, а также характер процедур, обычно используемых в аналогичных видах сделок.]

Справочный материал

A/CN.9/437, пункты 43, 48 и 92.

Замечания

28. В проекте статьи 2 основное внимание уделено правовым последствиям признания статуса "защищенной электронной подписи". На своей предыдущей сессии Рабочая группа обсудила возможность подхода к некоторым вопросам, касающимся электронных подписей (например, ответственности сертификационных органов и атрибуции сообщений, подписанных в цифровой форме), на основании презумпций (см. A/CN.9/437, пункты 58, 70 и 120—121).

29. Концепция защищенной электронной подписи и вытекающие из соответствующего статуса опровержимые презумпции можно рассматривать как имеющие решающее значение для создания жизнеспособной системы электронной торговли. В сделках, заключаемых с использованием бумажных документов, доверяющая сторона может использовать для определения подлинности документа и

подписи ряд показателей. К ним относятся тип используемой бумаги (иногда с водяными знаками, цветным фоном или другими показателями надежности), на которой приводится сообщение, использование фирменных бланков и собственноручных подписей, либо доставка запечатанных конвертов через заслуживающую доверия третью сторону (например, почтовую службу). Однако в электронных сообщениях ни один из этих факторов надежности не присутствует. Все, что может быть передано, — это набор электронных импульсов, которые во всех отношениях идентичны друг другу и легко могут быть скопированы или изменены. Таким образом, во многих случаях адресату и какой-либо другой стороне, полагающейся на электронное сообщение, важно знать — когда она принимает сообщение или решает довериться ему, — является ли соответствующее сообщение подлинным, сохранена ли целостность его содержания и сможет ли она установить оба эти факта в случае возникновения в последующем какого-либо спора (например, доказать в суде невозможность отрицания соответствующего сообщения данных составителем). В этих целях наличие опровержимых презумпций в отношении защищенных подписей может явиться для доверяющих сторон своеобразной гарантией, которая позволит им заниматься коммерческой деятельностью, будучи уверенными в том, что в случае необходимости их сделки легче будет принудительно осуществить.

30. Последствия презумпций, представленных в статье 2, следует отличать от последствий атрибуции, предусматриваемой статьей 3. Презумпции статьи 2 призваны облегчить бремя доказывания источника происхождения электронного сообщения, когда получатель проверяет предполагаемый источник сообщения с помощью защищенной электронной подписи. Таким образом, от лица, к которому относится соответствующая подпись, требуется доказать, что независимо от того, что адресат провел проверку защищенной электронной подписи и доверился процедуре обеспечения защиты, подпись этому лицу не принадлежит. В порядке обоснования принятия такой презумпции можно заметить, что обычно необходимые доказательства того, кто в действительности отправил сообщение, находятся у лица, к которому относится подпись. Например, в случае подписи в цифровой форме, в плане доказательства того, что личный ключ был похищен, скопирован, скомпрометирован или использован без разрешения каким-либо третьим лицом, в лучшем положении, чем любая другая доверившаяся сторона, обычно находится лицо, к которому относится соответствующая подпись. Кроме использовавшейся процедуры обеспечения защиты, получатель послания обычно не располагает никакими другими доказательствами того, что лицо, к которому относится подпись, действительно направило соответствующее сообщение. Однако, согласно проекту статьи 3, даже в том случае, когда сторона, к которой относится подпись, сможет доказать, что она не отправляла соответствующего сообщения, она тем не менее может быть признана обязанной возместить убытки, понесенные разумно доверившимся получателем (при условии соблюдения требований проекта статьи 3).

31. В соответствии с подходом, принятым в статье 7 Типового закона, пункт 1) не создает презумпции, согласно которой сообщение с защищенной электронной подписью является обязательством, имеющим юридическую силу. В пункте 1) лишь содержится презумпция, что защищенная электронная подпись проставляется предполагаемым подписавшимся с намерением подписать сообщение. Если имеются доказательства того, что лицо, чья подпись проставлена, стало жертвой ошибки, неправильного толкования, принуждения или какого-либо иного обстоятельства, делающего подпись недействительной, то соответствующее послание может быть признано не имеющим юридических последствий, но при этом поднимать подобные вопросы должно лицо, отрицающее юридические последствия сообщения данных.

32. Из пункта 2) явствует, что в отсутствие защищенной электронной подписи ничто в Единообразных правилах не изменяет обычных правил в отношении доказывания, в том что касается бремени доказывания источника сообщения. Пункт 3) сформулирован как и аналогичные положения Типового закона. Он предназначен облегчить исключение некоторых ситуаций из сферы изъятий проекта статьи 2 в случаях, когда такого исключения требуют законные интересы государства, вводящего в действие Единообразные правила. Такое государство может, например, постановить, что презумпции, предусмотренные в проекте статьи 2, не применяются в области уголовного права. В пункте 4) перечислены некоторые способы, с помощью которых можно опровергнуть презумпции, предусмотренные пунктом 1). Рабочая группа может пожелать рассмотреть вопрос о том, нужно ли включать такое иллюстративное положение в текст Единообразных правил или его следует рассматривать в контексте какого-либо руководства или комментария.

Статья 3. Атрибуция

1) Вариант А Согласно [статье 13 Типового закона ЮНСИТРАЛ об электронной торговле] составитель сообщения данных, на котором проставлена защищенная электронная подпись составителя, [связан содержанием] [считается лицом, подписавшим] сообщения таким же образом, как если бы это сообщение существовало в [собственноручно] подписанной форме в соответствии с законом, применимым к содержанию этого сообщения.

Вариант В Во взаимоотношениях держателя частного ключа с любой третей стороной, доверяющей подписи в цифровой форме, которая поддается [проверке] [удостоверению] с помощью соответствующего сертифицированного публичного ключа, такая подпись в цифровой форме [считается подписью данного держателя ключа] [удовлетворяет условиям, предусмотренным [статьей 7 1) Типового закона ЮНСИТРАЛ об электронной торговле]].

2) Пункт 1) не применяется, если:

a) [составитель] [держатель ключа] сможет доказать, что [защищенная электронная подпись] [частный ключ] использовалась(лся) без его разрешения и что [составитель] [держатель ключа] не имел возможности предотвратить такое использование в пределах разумной осмотрительности; или

b) доверяющая сторона узнала или должна была узнать, если бы она запросила информацию у [составителя] [сертификационного органа] или как-либо иначе проявила разумную осмотрительность, что данная [защищенная электронная] [в цифровой форме] подпись не является подписью [составителя] [держателя частного ключа].

Справочные материалы

A/CN.9/437, пункты 118—124 (проект статьи E);
A/CN.9/WG.IV/WP.71, пункты 64—65.

Замечания

33. На своей предыдущей сессии Рабочая группа в целом посчитала, что в контексте Единообразных правил не следует пытаться воспроизводить принципы статьи 13 Типового закона (см. A/CN.9/437, пункты 119—120). Было, однако, высказано мнение о необходимости прояснить взаимосвязь между Единообразными правилами и статьями 7 и 13 Типового закона. С этой целью Вариант А пункта 1), отражающий принцип, который Рабочая группа на своей предыдущей сессии признала в целом приемлемым (см. A/CN.9/437, пункт 120), был сформулирован широко и в него были включены как подпись в цифровой форме, так и альтернативные способы, которые могут использоваться для исполнения защищенной подписи в цифровой форме.

34. Вариант В создает презумпцию, согласно которой подпись в цифровой форме удовлетворяет требованиям о "надежном методе", содержащимся в статье 7 Типового закона. Рабочая группа может пожелать рассмотреть вопрос о том, должна ли эта презумпция быть расширена таким образом, чтобы она распространялась не только на подписи в цифровой форме, но и на другие случаи использования защищенной электронной подписи. Если Рабочая группа пожелает ограничить сферу применения положения о подписи в цифровой форме, то необходимо будет соответствующим образом переместить проект статьи 3.

35. Рабочая группа может пожелать обсудить вопрос о том, можно ли использовать проект статьи 3 в целях более конкретного определения, когда лицо может считаться ответственным за содержание сообщения данных, если это сообщение не было фактически отправлено этим лицом и передавалось с использованием открытых сетей [то есть без предварительной договоренности непосредственно между

составителем и получателем сообщения (или в контексте "системных правил") в отношении процедуры, которую следует применять при атрибуции сообщения данных]. Хотя в статье 13 3) a) Типового закона речь идет о применении "процедуры, предварительно согласованной с составителем", напрямую ситуацию использования открытых сетей этот Закон не регулирует. Учитывая высокую степень безопасности, присущую защищенным электронным подписям, Рабочая группа может пожелать рассмотреть вопрос о том, может ли быть установлено общее правило, предусматривающее, что получатель сообщения данных, разумно доверяющий защищенной электронной подписи, вправе рассматривать такое сообщение как исходящее от составителя.

36. В качестве примера подобного рода положения Рабочая группа может пожелать рассмотреть следующую формулировку:

> За исключением тех случаев, когда это предусмотрено каким-либо иным применимым законом, защищенная электронная подпись признается подписью лица, к которому она предположительно относится, независимо от наличия или отсутствия согласия на эту подпись с его стороны, если:
>
> a) электронная подпись явилась результатом действий какого-либо лица, которое приобрело номера доступа, коды, компьютерные программы или какую-либо иную необходимую для создания подписи информацию из источника, находившегося под контролем предполагаемого подписавшегося, в результате чего создалось впечатление, что подпись исходила от этого предполагаемого подписавшегося;
>
> b) такой доступ имел место в результате того, что предполагаемый подписавшийся не проявил разумной осмотрительности; и
>
> c) получатель добросовестно в ущерб себе доверился очевидному источнику этого сообщения данных.

Из этой формулировки следует то, что риск убытков распределяется между обеими заинтересованными сторонами, то есть между предполагаемым составителем, который на самом деле не подписывал данное сообщение, и получателем, добросовестно доверившимся этому сообщению в рамках разумной с коммерческой точки зрения процедуры обеспечения безопасности. Риск убытков возлагается лишь на предполагаемого составителя в том случае, если на таком сообщении проставлена подпись предполагаемого составителя по его вине. Подобная ситуация может возникнуть, когда подпись проставляется лицом, получившим необходимую информацию из источника, находившегося под контролем предполагаемого составителя, и когда такой доступ имел место в результате того, что предполагаемый подписавшийся не проявил разумной осмотрительности. В подобном случае, если получатель разумно доверяет сообщению данных, будет нести ответственность предполагаемый составитель. Во всех прочих случаях риск убытков будет лежать на получателе независимо от того, насколько разумно он доверится сообщению. Ссылка в начальной части статьи на "иной применимый закон" может оказаться необходимой для исключения из сферы действия предлагаемого правила сделок с потребителями.

Часть II. Подписи в цифровой форме

Статья 4. Определение

Для целей настоящих Правил,

Вариант A "подпись в цифровой форме" означает тип электронной подписи, состоящей в таком преобразовании сообщения данных с использованием резюмирующей функции сообщения и асимметрической криптосистемы, что любое лицо, располагающее первоначальным, не подвергшимся преобразованию, сообщением данных и публичным ключом подписавшегося может точно определить:

a) было ли такое преобразование осуществлено с использованием частного ключа подписавшегося, соответствующего его публичному ключу; и

b) было ли первоначальное сообщение данных изменено после произведенного преобразования.

Вариант В a) "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 определить, что эта числовая величина была получена с помощью частного ключа составителя;

b) математические процедуры, используемые для подготовки подписей в цифровой форме в соответствии с 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 ключом составителя, может точно определить:

i) было ли такое преобразование осуществлено с использованием частного ключа, который соответствует публичному ключу составителя; и

ii) было ли первоначальное сообщение изменено после произведенного преобразования.

Справочные материалы

A/CN.9/437, пункты 30—38 (проект статьи A);
A/CN.9/WG.IV/WP.71, пункты 18—45 и 55—56.

Замечания

37. Различия между вариантами A и B являются по большей части различиями редакционного характера. Если Вариант B отражает выводы, к которым Рабочая группа пришла на своей предыдущей сессии (см. A/CN.9/437, пункт 32), то Вариант A содержит более простую формулировку, основанную на определении понятия "электронная подпись". По обоим вариантам термин "подпись в цифровой форме" определяется без упоминания "сертификационных органов" или "сертификатов".

38. Не предпринималось попыток дать определения терминов "частный ключ", "публичный ключ", "пара ключей" или каких-либо иных понятий, связанных с криптографией по методу публичного ключа. Хотя на предыдущей сессии Рабочей группы выдвигались предложения о разработке дополнительных определений, было выражено опасение, что включение в единообразные правила нормативного характера большого числа определений может войти в противоречие с традиционным законодательством многих стран. Рабочая группа может пожелать обсудить вопрос о возможном количестве необходимых дополнительных определений (см. A/CN.9/437, пункт 29).

Статья 5. Правовые последствия

1) В случаях, когда сообщение данных или какая-либо его часть подписываются с использованием подписи в цифровой форме, эта подпись считается, по отношению к данной части сообщения, защищенной электронной подписью, если:

a) подпись в цифровой форме проставлена в течение срока действия [имеющего юридическую силу] сертификата и проверена путем ссылки на публичный ключ, указанный в сертификате; и

b) сертификат считается устанавливающим четкую связь между публичным ключом и личностью соответствующего лица в силу того, что:

i) сертификат был выдан сертификационным органом, лицензированным [уполномоченным] ... *[принимающее государство указывает орган или ведомство, компетентное лицензировать сертификационные органы и принимать постановления в отношении функционирования лицензированных сертификационных органов]*; или

ii) сертификат был выдан каким-либо иным образом сертификационным органом в соответствии со стандартами, установленными ... *[принимающее государство указывает орган или ведомство, компетентное устанавливать признанные стандарты функционирования лицензированных сертификационных органов]*.

2) В случаях, когда сообщение данных или какая-либо его часть подписываются с использованием подписи в цифровой форме, не удовлетворяющей требованиям, изложенным в пункте 1), подпись в цифровой форме считается, по отношению к данной части сообщения, защищенной электронной подписью, если имеются достаточные доказательства того, что данный сертификат устанавливает четкую связь между публичным ключом и личностью его держателя.

3) Положения настоящей статьи не применяются по отношению к следующему: [...].

Справочные материалы

A/CN.9/437, пункты 43, 48 и 92.

Замечания

39. При надлежащем применении подписи в цифровой форме должны являться защищенными электронными подписями. Однако необходимо еще решить вопрос о том, когда применение подписи в цифровой форме осуществляется таким образом, что она приобретает защищенный статус. Не все подписи в цифровой форме, поддающиеся проверке путем сверки с сертификатом, являются защищенными, особенно если нет уверенности в точности идентификации ее держателя или подлинности публичного ключа. К числу важнейших факторов, определяющих защищенность подписи в цифровой форме, относятся следующие: 1) должным ли образом сертификационный орган идентифицировал держателя ключа; 2) должным ли образом сертификационный орган установил подлинность публичного ключа держателя; 3) не скомпрометирован ли частный ключ держателя; и 4) заслуживает ли доверия процесс проверки (например, отвечают ли необходимым требованиям алгоритм публичного ключа и длина ключа).

40. В пункте 1) устанавливаются два базовых критерия определения того, в каких случаях подпись в цифровой форме может считаться защищенной электронной подписью. В соответствии с первым критерием такая подпись должна быть проставлена в течение срока действия имеющего юридическую силу сертификата и проверяться путем сверки с публичным ключом, указанным в сертификате. Срок действия сертификата обычно начинается в момент его выдачи и заканчивается в момент истечения этого срока либо в момент аннулирования или приостановления действия сертификата.

41. Ко второму этапу относится установление гарантий того, что сам сертификат точно идентифицирует соответствующее лицо в качестве держателя частного ключа, соответствующего публичному ключу, указанному в сертификате. Степень достоверности сертификата может быть оценена путем сверки со стандартами, процедурами и прочими требованиями, устанавливаемыми признанными органами принимающего государства. Такие стандарты могут устанавливаться посредством утверждения сертификационными органами третьих сторон, добровольного лицензирования сертификационных органов, в иных же случаях требуется соответствие нормам, принятым в государстве, вводящем у себя в действие настоящие Правила.

42. И наоборот, согласно пункту 2), если суд или какой-либо иной орган, занимающийся установлением фактов, определит в качестве доказательства, что содержащаяся в сертификате информация соответствует действительности, то достоверность сертификата становится очевидной. Однако на этом этапе от органа, занимающегося установлением фактов, требуется в каждом конкретном случае установить, был ли сертификат выдан сертификационным органом, надлежащим образом идентифицировавшим держателя публичного ключа и установившим подлинность ключа этого держателя.

43. В соответствии с "двойственным подходом", принятым Рабочей группой, проект статьи 5 призван обеспечить максимально широкие возможности в плане установления достоверности сертификата, выданного сертификационным органом. Такая гибкость имеет особое значение в свете того факта, что использование подписи в цифровой форме является делом новым и модели ее использования, равно как и варианты регулирования, еще не до конца разработаны. Поэтому важно облегчить процесс расширения использования подписей в цифровой форме в электронной торговле, установив при этом стандарты, необходимые для предположительного определения, в том что касается надежности сообщения данных, на котором проставлена подпись в цифровой форме.

44. Важно также отметить, что в то время как один из вариантов проекта статьи 5 содержит установление точности сертификатов судебными органами, другой предполагает точность сертификата в случае его выдачи сертификационным органом, уполномоченным вводящим настоящие Правила государством или если этот сертификат иным образом удовлетворяет определенным стандартам, установленным этим государством. В таком случае для придания подписи статуса защищенной электронной подписи решения судебного органа о точности сертификата не требуется. Второй вариант может оказаться полезным для занимающихся электронной торговлей лиц, которые будут заранее знать, что любой их акт, совершаемый с доверием к соответствующему сообщению, может быть исполнен в принудительном порядке. Однако презумпция точности сертификата может быть опровергнута доказательством того, что сертификат, выданный таким уполномоченным сертификационным органом, на самом деле не является точным или надежным.

[Статья 6. Подписи, проставляемые юридическими лицами

Юридическое лицо может идентифицировать сообщение данных путем добавления к этому сообщению публичного 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.]

Справочные материалы

A/CN.9/437, пункты 114—117 (проект статьи D);
A/CN.9/WG.IV/WP.71, пункты 61—63.

Замечания

45. На предыдущей сессии раздавалось много голосов за исключение проекта статьи 6. Однако после проведенного обсуждения Рабочая группа постановила, что этот проект статьи должен быть заключен в квадратные скобки, с тем чтобы продолжить его обсуждение на одной из следующих сессий (A/CN.9/437, пункты 115 и 117). И хотя положение, соответствующее проекту статьи 6, может рассматриваться как необоснованно противоречащее другим сводам правовых норм (например агентскому праву и нормам акционерного права, касающимся представительства компаний физическими лицами), оно может оказаться полезным на данном этапе разработки Единообразных правил в качестве напоминания о том, что Рабочей группе может понадобиться более глубоко обсудить вопрос о параметрах, в пределах которых настоящие Единообразные правила должны подтверждать деятельность "электронных агентов" с целью удостоверения подлинности сообщений данных в автоматическом режиме.

Часть III. Другие электронные подписи

46. Поскольку в Секретариат не поступило никакой информации относительно каких-либо иных, кроме подписей в цифровой форме, способов удостоверения подлинности, которые могли бы подлежать регулированию на основании настоящих Единообразных правил, то для включения в данную часть проекта никаких конкретных положений подготовлено не было. Рабочая группа может пожелать обсудить вопрос о том, следует ли такие способы удостоверения подлинности разрабатывать в настоящих Единообразных правилах более подробно. Если Рабочая группа придет к заключению, что такие способы не следует разрабатывать более подробно, то Единообразные правила будут по-прежнему создавать благоприятный режим для более широкого использования альтернатив подписям в цифровой форме посредством принципа недискриминации, отраженного в определениях терминов "подпись" и "защищенная электронная подпись", а также посредством признания правового статуса за любым способом удостоверения подлинности, который будет квалифицироваться как "защищенная электронная подпись".

РАЗДЕЛ III. СЕРТИФИКАЦИОННЫЕ ОРГАНЫ И СООТВЕТСТВУЮЩИЕ ВОПРОСЫ

Статья 7. Сертификационный орган

1) Для целей настоящих Правил "сертификационный орган" означает:

a) любые лицо или организацию, лицензированные [уполномоченные] ... *[принимающее государство указывает орган или ведомство, компетентное лицензировать сертификационные органы и принимать постановления в отношении функционирования лицензированных сертификационных органов]* действовать в соответствии с настоящими Правилами; или

b) любые лицо или организацию, которые в порядке своей обычной деловой практики занимаются выдачей сертификатов по криптографическим ключам, используемым для подписи в цифровой форме.

[2) Сертификационный орган может предлагать или облегчать регистрацию и фиксацию времени передачи и приема сообщений данных, а также выполнять другие функции в отношении сообщений, защищенных с помощью подписей в цифровой форме.]

Справочные материалы

A/CN.9/437, пункты 39—50 и 90—97 (проект статьи B);
A/CN.9/WG.IV/WP.71, пункты 18—45 и 57—58.

Замечания

47. Как указывалось в связи с проектом статьи 1, Единообразные правила должны обеспечить правовое признание как ситуации, когда принимающее государство желает осуществлять регулирование деятельности сертификационных органов с помощью инфраструктуры для использования публичных ключей или каких-либо иных схем лицензирования, так и ситуации, когда нелицензированные сертификационные органы могут свободно функционировать, соблюдая стандарты, выработанные практикой рыночных отношений (см. пункты 17—18, выше).

48. В том что касается лицензированных сертификационных органов, в пункте 1) не делается никакой попытки определить критерии, которые принимающее государство должно применять в отношении инфраструктуры для использования публичных ключей или какой-либо иной схемы лицензирования сертификационных органов. Причина того, что такие критерии не рассматриваются, заключается в наличии у подобных инфраструктур для использования публичных ключей весомого компонента государственной политики, который может нелегко поддаваться гармонизации на международном уровне с помощью типовых законодательных положений. В случае, если Рабочая группа займется более детальным изучением критериев применения той или иной схемы лицензирования, она может пожелать рассмотреть следующие факторы, которые следует учитывать при оценке надежности какого-либо сертификационного органа: 1) независимость (то есть отсутствие финансового или какого-либо иного интереса в затрагиваемых сделках); 2) финансовые ресурсы и наличие финансовых возможностей нести риск ответственности за ущерб; 3) компетентность управленческого персонала, опыт в области технологии использования публичных ключей и знание надлежащих процедур обеспечения защиты данных; 4) длительная перспектива работы (от сертификационных органов может потребоваться представить доказательства сертификации или наличия декодирующих ключей через много лет после исполнения соответствующих сделок в связи с судебным иском или имущественным требованием); 5) одобрение аппаратного и программного обеспечения; 6) сохранение аудиторских документов и проведение ревизии независимым органом; 7) существование плана действий в непредвиденных случаях (например, программного обеспечения, позволяющего восстанавливать данные в чрезвычайных случаях, или ключа, находящегося на хранении у третьей стороны); 8) подбор персонала и руководство им; 9) меры по защите собственного 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 утеряны или скомпрометированы); 17) отделение функции сертификации от каких-либо иных видов деловой активности, которыми может заниматься данный сертификационный орган (см. A/CN.9/WG.IV/WP.71, пункт 44 и A/CN.9/437, пункт 45).

49. В пункте 1) b) дается определение "сертификационного органа" как органа, занимающегося выдачей сертификатов, и при этом отсутствует какое-либо упоминание о наделении его соответствующими полномочиями со стороны государственных органов. Подобное положение, взятое в сочетании с пунктом 2), также призвано отразить тот факт, что, хотя сертификационные органы могут выполнять иные функции и оказывать услуги помимо выдачи сертификатов, подобные функции и услуги находятся вне сферы применения настоящих Единообразных правил и не должны учитываться при рассмотрении правовых последствий электронных подписей. Рабочая группа может пожелать обсудить вопрос о том, следует ли положение, соответствующее содержанию пункта 2), который носит в основном

описательный характер, включать в текст настоящих Единообразных правил или его лучше отразить в соответствующем руководстве или комментарии.

Статья 8. Сертификат

Для целей настоящих правил "сертификат" означает сообщение данных [или какую-либо иную запись], в котором по меньшей мере:

a) идентифицируется выдавший его сертификационный орган;

b) называются или идентифицируются его держатель либо соответствующие устройство или электронный агент, находящиеся под контролем держателя;

c) содержится публичный ключ, соответствующий частному ключу, находящемуся под контролем держателя;

d) указываются срок действия [и существующие ограничения, если таковые имеются, относительно сферы использования публичного ключа]; и

e) подписан [в цифровой форме] сертификационным органом, выдавшим сертификат.

Справочные материалы

A/CN.9/437, пункты 98—113 (проект статьи C);
A/CN.9/WG.IV/WP.71, пункты 18—45 и 59—60.

Замечания

50. Хотя сертификат может использоваться для выполнения различных функций и содержать дополнительную информацию помимо сферы действия Единообразных правил, единственное назначение сертификата с точки зрения настоящих Единообразных правил — привязать публичный ключ к конкретному держателю. Такая привязка может быть сделана непосредственно путем указания имени держателя публичного ключа в сертификате. Она может быть произведена и косвенно путем описания некоторых атрибутов держателя (например, путем указания на то, что он является агентом по закупкам, наделенным правом заключать договоры о закупках товаров на сумму, не превышающую какую-то определенную величину) либо путем описания машины, устройства или агентского программного обеспечения, находящихся под контролем держателя. Так, например, сертификат выдается служащему какой-либо корпорации и в нем указываются лишь пределы, в которых этому служащему дано право производить закупки. В этом случае сертификат может быть использован при закупках у торговых партнеров, когда личность служащего значения не имеет, а важно то, уполномочен ли этот служащий действовать от имени соответствующего идентифицированного лица (то есть нанимателя), а также пределы полномочий по закупкам этого служащего. Но в любом случае есть лицо, известное как "держатель", которое контролирует частный ключ, соответствующий публичному ключу, идентифицируемому в сертификате, и которое является лицом, по отношению к которому осуществляется атрибуция подписанных в цифровой форме сообщений, проверяемых путем сверки с сертификатом. Если такое лицо не идентифицируется, то сертификат нельзя использовать для проверки принадлежности подписи в цифровой форме указанному лицу.

51. Проект статьи 8 предназначен отразить элементы, которые рассматриваются Рабочей группой в качестве базовых компонентов сертификата. Это, в частности, предполагает, что сертификат должен: представлять собой сообщение данных; идентифицировать сертификационный орган; содержать публичный ключ держателя; идентифицировать держателя; а также быть подписанным в цифровой форме сертификационным органом (см. A/CN.9/437, пункт 101). Что касается обязательности представления сертификата в форме сообщения данных, то Рабочая группа может пожелать обсудить

вопрос о том, должны ли Единообразные правила распространять свое действие и на бумажные сертификаты.

52. На предыдущей сессии Рабочая группа приняла решение, что ей, возможно, придется рассмотреть вопрос о том, не будет ли установление императивной нормы относительно минимального объема содержащейся в сертификате информации противоречить применимому праву о защите данных. Было высказано мнение о том, что в силу характера элементов, перечисленных в проекте статьи 8, такой потенциальной коллизии удается избежать.

53. В определении понятия "сертификат" не проводится различия между различными уровнями защиты, обеспечиваемой в коммерческом порядке под общей рубрикой "сертификат". Однако, работая над подготовкой настоящих Единообразных правил, Рабочая группа может иметь в виду, что сертификационные органы обычно предлагают разные категории сертификатов. На предыдущей сессии Рабочей группы был выдвинут ряд предложений, направленных на то, чтобы Единообразные правила учитывали различные уровни защиты в связи с использованием таких сертификатов (см. A/CN.9/437, пункты 20, 56, 138 и 145). В качестве примера подобного разнообразия были приведены три нижеследующие категории "сертификатов", существующих на рынке.

54. Сертификаты категории I подтверждают, что имя и адрес электронной почты пользователя составляют не поддающееся толкованию собственное имя, включенное в регистр или "хранилище данных", содержащиеся у сертификационного органа. Обычно они используются в основном для поиска по Интернету и в личной электронной почте и имеют цель несколько повысить уровень защиты этих сетей. Сертификаты категории I не предназначены для удостоверения подлинности личности держателя. Они скорее выступают в качестве простого проверочного механизма недвусмысленности собственного имени в рамках хранилища данных, и предоставляют возможность ограниченной проверки адреса электронной почты. Имя держателя, указанное в сертификате категории I, рассматривается как непроверенная информация. Эти сертификаты обеспечивают весьма низкий уровень защиты. Они не предназначены для коммерческого использования, когда требуется доказывание соответствующей личности, и в этих целях полагаться на них не следует.

55. Сертификаты категории II подтверждают, что информация, представленная держателем при подаче заявки на сертификат, не противоречит информации, доступной через общепризнанные базы данных потребителей. Сертификаты категории II обычно используются для целей: 1) внутриучрежденческой электронной почты; 2) низкостоимостных сделок с невысокой степенью риска; 3) личной электронной почты; 4) замены пароля; 4) подтверждения программного обеспечения; и 5) услуг, предоставляемых в реальном времени по подписке. Сертификаты категории II обеспечивают определенный уровень гарантий в отношении личности держателя, основанных на обработке данных в автоматическом режиме в реальном времени.

56. Сертификаты категории III предоставляют серьезные гарантии в отношении личности держателя, поскольку они, в частности, связаны с требованием о личном (физическом) представлении держателя агенту сертификационного органа или о проверке его личности на основании надлежащих удостоверяющих личность документов. Соответствующий публичному частный ключ, указанный в сертификате категории III, должен составляться и храниться заслуживающим доверия образом согласно требованиям, установленным сертификационным органом. Сертификаты категории III используются на практике в некоторых электронных приложениях коммерческого характера, например при электронном обслуживании банковской деятельности, электронном обмене данными (ЭДИ) и предоставлении в реальном времени услуг, основанных на членстве пользователей. При процессах, связанных с сертификатами категории III, для получения доказательных сведений относительно личности отдельных подписчиков применяются различные процедуры. Такие подтвердительные процедуры обеспечивают более прочные, чем предоставляемые сертификатами категории II, гарантии в отношении личности заявителя.

57. Из вышеизложенного очевидно, что в нынешнюю сферу действия Единообразных правил включаются лишь сертификаты категории III. Рабочая группа может пожелать обсудить вопрос о том, следует ли расширить сферу действия Единообразных правил, чтобы она охватывала и более низкие категории сертификатов. Если такое решение будет принято, то тогда необходимо принять и решение относительно различных правовых последствий, вытекающих из сертификатов различных категорий, в

частности в том, что касается уровня ответственности, возложенной на сертификационные органы в связи с выдачей сертификатов более низких категорий. В противном случае определение понятия "сертификат" в Единообразных правилах придется, возможно, изменить таким образом, чтобы было ясно, что настоящие Единообразные правила не распространяются на сертификаты более низких категорий.

Статья 9. Заявление о практике сертификации

Для целей настоящих Правил "заявление о практике сертификации" означает заявление, опубликованное сертификационным органом, указавшим те виды практики, которые этот орган применяет при выдаче или каком-либо ином использовании сертификатов.

Справочные материалы

A/CN.9/437, пункты 60—62, 70, 110—111 и 149 (проект статьи J);
A/CN.9/WG.IV/WP.71, пункт 89.

Замечания

58. Степень, в которой любая полагающаяся на сертификат сторона может доверять подтверждаемой сертификатом привязке какого-либо лица к соответствующему публичному ключу, зависит от нескольких факторов. В число этих факторов входят виды практики и процедуры, применяемые сертификационным органом при удостоверении подлинности держателя пары ключей, а также оперативная политика, процедуры и механизмы контроля защиты соответствующего сертификационного органа. Заявления о практике сертификации часто представляются действующими сертификационными органами как один из главных элементов, с помощью которых они укрепляют доверие к надежности выдаваемых ими сертификатов, а в более широком плане — как стандарт качества и ответственности, на основании которого должны регулироваться взаимоотношения между сертификационными органами и их клиентами.

59. Заявление о практике сертификации — это заявление сертификационного органа о политике, которой он руководствуется, либо подробное изложение видов практики, процедур и систем, применяемых им в процессе своего функционирования, а также при выдаче, обслуживании и аннулировании сертификата. В число вопросов, указываемых в заявлении о практике сертификации, могут входить следующие: 1) процедуры, применяемые (до выдачи сертификата) в целях подтверждения подлинности личности заявителя, ходатайствующего о выдаче сертификата; 2) физические, процедурные методы контроля и контроль со стороны сотрудников, применяемые сертификационным органом в целях безопасного выполнения функций по разработке ключей, выдаче сертификатов, их аннулированию, аудиту и архивированию; 3) меры безопасности, принимаемые сертификационным органом в целях защиты криптографических ключей; и 4) любую относящуюся к делу информацию. Эти вопросы представляют важность как для держателя, получающего сертификат, так и для полагающихся на сертификат сторон, которые будут использовать сертификат, выданный сертификационным органом, в качестве основы при заключении сделок с его держателем.

60. Заявление о практике сертификации может быть представлено в различных формах, например в форме договора с участием всех заинтересованных сторон либо в форме публичного уведомления в адрес всех заинтересованных сторон. Основным элементом, однако, является уведомление в адрес сторон, полагающихся на сертификат. Заявление о практике сертификации должно представлять собой уведомление, исходящее от сертификационного органа и адресованное всем полагающимся на сертификат сторонам (включая его держателя), о видах практики, применяемой сертификационным органом при выдаче, обслуживании и аннулировании сертификатов.

Статья 10. Подтверждения, представляемые при выдаче сертификата

Вариант A

1) Выдавая сертификат, сертификационный орган подтверждает любому лицу, разумно полагающемуся на сертификат либо на подпись в цифровой форме, подлинность которой может быть проверена публичным ключом, указанным в этом сертификате, что:

a) при выдаче сертификата сертификационный орган выполнил все применимые требования настоящих Правил и — если сертификационный орган опубликовал сертификат или иным образом предоставил его в распоряжение любого такого полагающегося на сертификат лица — указанный в этом сертификате держатель [являющийся и правомерным держателем соответствующего частного ключа] согласился с ним;

b) указанный в сертификате держатель [правомерно] владеет частным ключом, соответствующим указанному в сертификате публичному ключу;

c) публичный и частный ключи держателя составляют действующую пару ключей;

d) вся содержащаяся в сертификате информация является точной на момент его выдачи, если сертификационный орган не указал в сертификате [или не включил путем ссылки в сертификате указание на то], что точность определенной информации не подтверждена; и

e) насколько известно сертификационному органу, в сертификате не упущены никакие существенные факты, которые, если бы об их существовании было известно, могли бы отрицательно сказаться на достоверности указанных выше подтверждений.

2) При условии соблюдения положений пункта 1) сертификационный орган, выдавший сертификат, подтверждает любому лицу, разумно полагающемуся на сертификат либо на подпись в цифровой форме, подлинность которой может быть проверена публичным ключом, указанным в этом сертификате, что сертификационный орган выдал данный сертификат в соответствии с любым применимым заявлением о практике сертификации [включенным путем ссылки в сертификат, или], уведомление о котором было направлено полагающемуся на сертификат лицу.

Вариант B

1) Выдавая сертификат, сертификационный орган подтверждает держателю и любому лицу, [добросовестно и] в течение срока действия сертификата полагающемуся на содержащуюся в нем информацию, что:

a) сертификационный орган [обработал] [подтвердил] [выдал] и будет обслуживать, а также, в случае необходимости, аннулирует данный сертификат в соответствии с:

i) настоящими Правилами;

ii) любым другим применимым законом, регулирующим выдачу данного сертификата; и

iii) любым применимым заявлением о практике сертификации, сделанным или включенным путем ссылки в сертификат либо уведомление о котором было направлено такому лицу (если было направлено);

b) сертификационный орган проверил личность держателя в пределах, указанных в сертификате или в каком-либо применимом заявлении о практике сертификации, либо — в отсутствие такого заявления о практике сертификации — соответствующим [надежным] [заслуживающим доверия] образом;

c) сертификационный орган проверил, что лицо, ходатайствующее о выдаче сертификата, является держателем частного ключа, соответствующего публичному ключу, указанному в сертификате;

d) за исключением того, что указано в сертификате или каком-либо применимом заявлении о практике сертификации, вся прочая информация, содержащаяся в сертификате, является, насколько это известно сертификационному органу, точной на момент выдачи сертификата;

e) если сертификационный орган опубликовал сертификат, идентифицированный в сертификате держатель согласился с ним.

[2) Если сертификационный орган выдал сертификат в соответствии с положениями закона какой-либо иной страны, то этот сертификационный орган должен также предоставить все гарантии и подтверждения — если такие необходимы, — которые требуются согласно закону, регулирующему выдачу сертификата.]

Справочные материалы

A/CN.9/437, пункты 51—73 (проект статьи H);
A/CN.9/WG.IV/WP.71, пункты 70—72.

Замечания

61. Проект статьи 10 призван отразить принятое Рабочей группой решение о том, что в принципе в проекте Единообразных правил должны содержаться положения, касающиеся ответственности сертификационных органов в контексте их участия в механизмах использования подписей в цифровой форме (A/CN.9/437, пункт 55). Минимальный стандарт ответственности, предусмотренный в проекте статьи 10, должен применяться лишь по отношению к выдаче сертификатов для целей подписей в цифровой форме, как они определены в проекте статьи 4. В проекте Единообразных правил не следует пытаться урегулировать другие действия, которые могут осуществляться сертификационными органами, или оказываемые ими услуги. Такие действия и услуги могут регулироваться договорами между сертификационными органами и их клиентами или любыми другими применимыми нормами права (там же, пункт 71).

62. На своей тридцать первой сессии Рабочая группа пришла к общему мнению, что формулировка, сходная с положениями пункта 1) Варианта A, в большей своей части является приемлемой в качестве основы для дальнейшего обсуждения. Хотя пункт 1) и не содержит четко выраженной нормы об ответственности, он устанавливает минимальный стандарт, от которого стороны не должны отходить по частной договоренности. В частности, никакая оговорка, ограничивающая ответственность сертификационного органа, не должна рассматриваться как подпадающая под защиту или льготы, которые предусматриваются Единообразными правилами, если она противоречит вышеперечисленным требованиям. В случае заявлений об ответственности сертификационного органа этот орган будет считаться несущим ответственность за последствия выдачи сертификата, если он не сможет доказать, что выполнил требования, перечисленные в пункте 1). Однако, если сертификационный орган пожелает взять на себя обязательства более жесткие, чем перечисленные в пункте 1) подтверждения, он должен иметь возможность сделать это путем включения соответствующих положений в заявление о практике сертификации или иным способом (A/CN.9/437, пункт 70). Пункт 2) призван регулировать ситуации, когда заявления о практике сертификации содержат такие более жесткие стандарты.

63. Хотя Вариант B и сформулирован на основе Варианта A, в нем больший упор делается на саморегулирование со стороны сертификационных органов. В частности, согласно подпункту b), сертификационный орган не гарантирует, что держатель владеет частным ключом правомерно. Зато сертификационный орган гарантирует, что в целях установления привязки держателя к частному ключу он по меньшей мере выполнил процедуры, указанные в заявлении о практике сертификации, или применил "надежные" или "заслуживающие доверия" методы идентификации держателя. Из пункта 2) Варианта B со всей очевидностью вытекает, что пункт 1) a) ii) применяется также и по отношению к

сертификатам, выдаваемым по законам иностранных государств. Рабочая группа может пожелать обсудить вопрос о том, следует ли такое уточнение вносить в Единообразные правила, либо его следует поместить в соответствующем руководстве или комментарии.

Статья 11. Договорная ответственность

1) Во взаимоотношениях между сертификационным органом, выдавшим сертификат, и держателем этого сертификата [или какой-либо иной стороной, находящейся в договорных отношениях с сертификационным органом] права и обязательства сторон определяются достигнутым между ними соглашением.

2) При условии соблюдения статьи 10 сертификационный орган может, по соглашению между сторонами, снять с себя ответственность за любой ущерб, вызванный дефектами информации, указанной в сертификате, техническими ошибками или аналогичными обстоятельствами. Однако на оговорку, ограничивающую или снимающую ответственность сертификационного органа, нельзя ссылаться, если такие снятие или ограничение договорной ответственности будут, учитывая цель договора, в высшей степени несправедливыми.

3) Сертификационный орган не имеет права ограничивать свою ответственность, если будет доказано, что убытки последовали в результате действия или бездействия сертификационного органа, совершенных с намерением причинить ущерб или по грубой неосторожности и при понимании того, что ущерб может быть причинен.

Справочные материалы

A/CN.9/437, пункты 51—73 (проект статьи H);
A/CN.9/WG.IV/WP.71, пункты 70—72.

Замечания

64. В пункте 1) воспроизводится принцип автономии сторон в связи с режимом ответственности, применимым к сертификационному органу. В пункте 2) речь идет об оговорках о снятии ответственности, которые в целом, за двумя исключениями, объявляются допустимыми. Первое исключение объясняется ссылкой на проект статьи 10, предполагающей установление минимального стандарта, от которого стороны не должны иметь возможности отходить по частной договоренности (см. пункт 58, выше). Второе исключение основывается на Принципах международных коммерческих контрактов ЮНИДРУА (статья 7.1.6) и представляет собой попытку установить единообразный стандарт оценки общей приемлемости оговорок об изъятии. Можно отметить, что упоминание о "в высшей степени несправедливом" характере ограничения или снятия ответственности предполагает гибкий подход к оговоркам об изъятии. Такой подход может привести к более широкому признанию оговорок об ограничении или снятии ответственности, чем если бы в Единообразным правилах упоминался лишь закон, применимый помимо этих Правил.

65. Пунктом 3) регулируется ситуация, при которой убытки или иной ущерб возникают в результате преднамеренно неправомерного поведения сертификационного органа или его агентов. Предлагаемая норма по существу восходит к аналогичной формулировке, используемой во многих конвенциях о международных перевозках и включенной недавно в статью 18 Типового закона ЮНСИТРАЛ о международных кредитовых переводах.

Статья 12. Ответственность сертификационного органа перед сторонами, полагающимися на сертификаты

1) В отсутствие соглашения об обратном, выдающий сертификат сертификационный орган несет ответственность перед любым лицом, разумно полагающимся на сертификат, за:

a) [нарушение гарантии, предусмотренной статьей 10] [небрежность, проявившуюся в неправильном подтверждении достоверности информации, указанной в сертификате];

b) регистрацию аннулирования сертификата сразу же после получения уведомления о его аннулировании; и

c) [последствия неприменения] [небрежность в применении] следующего:

i) любой процедуры, указанной в заявлении о практике сертификации, опубликованном сертификационным органом; или

ii) любой процедуры, предусмотренной применимым законом.

2) Независимо от положений пункта 1) сертификационный орган не несет ответственности, если может доказать, что он или его агенты приняли все необходимые меры для избежания ошибок в сертификате или что ни он, ни его агенты не имели возможности принять такие меры.

3) Независимо от положений пункта 1) сертификационный орган вправе ограничить в сертификате [или каким-либо иным образом] цели, в которых данный сертификат может использоваться. Сертификационный орган не будет считаться ответственным за ущерб, возникший в результате использования данного сертификата в каких-либо иных целях.

4) Независимо от положений пункта 1) сертификационный орган вправе ограничить в сертификате [или каким-либо иным образом] стоимостной объем сделок, по которым данный сертификат будет действительным. Сертификационный орган не будет считаться ответственным за ущерб, возникший в результате совершения сделок и превышающий установленный предел стоимости.

Справочные материалы

A/CN.9/437, пункты 51—73 (проект статьи H);
A/CN.9/WG.IV/WP.71, пункты 70—72.

Замечания

66. Проект статьи 12 призван отразить выраженную на предыдущей сессии точку зрения, согласно которой Единообразные правила должны содержать норму, устанавливающую опровержимую презумпцию ответственности. Согласно такой норме, например, в случае ошибочной идентификации лица или ошибочной атрибуции публичного ключа какому-либо лицу сертификационный орган будет нести ответственность за убытки, понесенные потерпевшей стороной, если только он не докажет, что сделал все возможное, чтобы не допустить этой ошибки. Такая схема ответственности призвана обеспечить дополнительную защиту любому лицу, пользующемуся услугами сертификационного органа, не возлагая при этом абсолютной ответственности на сертификационный орган (см. A/CN.9/437, пункт 58).

67. В контексте обсуждения проектов статей 10—12 Рабочая группа может пожелать рассмотреть вопрос о том, должны ли устанавливаться пределы ответственности сертификационных органов и как такие пределы могут определяться (см. A/CN.9/437, пункты 63—67). На своей предыдущей сессии Рабочая группа обсудила различные предложения, касавшиеся возможных методов ограничения объемов ответственности, которую несут сертификационные органы. Один возможный подход мог бы заключаться в установлении фиксированной суммы. Другие предложенные подходы предусматривали ограничение ответственности путем указания коэффициента, на который должна перемножаться плата подписчика, процентной доли от стоимостного объема операции или процентной доли от фактического ущерба, понесенного пострадавшей стороной. Вместе с тем было указано, что ущерб, который может возникнуть в результате действий сертификационного органа, с трудом поддается количественной оценке, что осложняет его использование в качестве объективного критерия для установления фиксированного объема ответственности. Кроме того, услуги, оказываемые сертификационным органом, и взимаемая им за это плата зачастую никак не связаны со стоимостным объемом операций, к которым эти услуги относятся, или с ущербом, который могут понести стороны (там же, пункт 66). Что же касается предложенного сравнения положения сертификационного органа и положения перевозчика по международным конвенциям, применимым к перевозке грузов и пассажиров (там же, пункт 67), то предварительный обзор этих документов наводит на мысль о том, что пределы ответственности обычно устанавливаются какой-либо фиксированной суммой (например, при перевозке пассажиров), возможно, в сочетании со стоимостным объемом перевозимых товаров. Возможно, этот вопрос Рабочей группе необходимо будет рассмотреть на одной из последующих сессий, взяв за основу исследование, которое в будущем проведет Секретариат.

Статья 13. Аннулирование сертификата

1) В течение срока действия сертификата выдавший его сертификационный орган может аннулировать сертификат в соответствии с политикой и процедурами, регулирующими порядок аннулирования и предусмотренными применимым заявлением о практике сертификации, либо, в отсутствие таких политики и процедур, незамедлительно по:

a) получении требования об аннулировании от держателя, идентифицированного в сертификате, и подтверждении того, что лицо, требующее аннулирования, является [правомерным] держателем сертификата либо его агентом, обладающим полномочиями требовать такого аннулирования;

b) получении достоверных доказательств наступления смерти держателя, если таковым является физическое лицо; или

c) получении достоверных доказательств ликвидации или прекращения существования держателя, если таковым является юридическое лицо.

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 понесенный

третьими сторонами, полагавшимися на содержание сообщений, ущерб в результате того, что держатель не произвел аннулирования.

3) Независимо от того, дает ли свое согласие на аннулирование обозначенный в сертификате держатель, сертификационный орган, выдавший сертификат, обязан аннулировать сертификат сразу же после того, как ему станет известно, что:

a) изложенные в сертификате материальные факты не соответствуют действительности;

b) частный ключ или информационная система сертификационного органа были скомпрометированы таким образом, что это влияет на надежность сертификата; или

c) были скомпрометированы частный ключ или информационная система держателя сертификата.

3) После аннулирования сертификата согласно пункту 3) сертификационный орган должен известить держателя сертификата и полагающиеся на сертификат стороны в соответствии с политикой и процедурами, регулирующими порядок уведомления об аннулировании сертификата, который предусмотрен применимым заявлением о практике сертификации, или, в отсутствие таких политики и процедур, незамедлительно уведомить держателя сертификата и опубликовать уведомление об аннулировании сертификата, если последний был опубликован, и каким-либо иным путем раскрыть факт аннулирования после получения запроса от какой-либо стороны, полагавшейся на сертификат.

4) [Во взаимоотношениях между держателем сертификата и сертификационным органом] аннулирование вступает в силу с момента его [получения] [регистрации] сертификационным органом.

[5) Во взаимоотношениях между сертификационным органом и любой третьей стороной, полагающейся на сертификат, аннулирование вступает в силу с момента его [получения] [регистрации] сертификационным органом.]

Справочные материалы

A/CN.9/437, пункты 125—139 (проект статьи F);
A/CN.9/WG.IV/WP.71, пункты 66—67.

Замечания

68. Проект статьи 13 призван отразить различные точки зрения, высказанные на предыдущей сессии Рабочей группы, путем установления прекращения действия стандарта, регулирующего порядок аннулирования сертификатов. Однако сертификационный орган может всегда избежать этого прекращения стандарта, если сам установит в своем заявлении о практике сертификации процедуры, регулирующие порядок аннулирования сертификатов, и будет этим процедурам следовать. Что касается момента вступления аннулирования в силу, то Рабочая группа может пожелать принять решение о проведении различия между положением держателя сертификата и положением какой-либо иной стороны, полагающейся на сертификат (см. A/CN.9/437, пункт 130).

Статья 14. Приостановление действия сертификата

В течение срока действия сертификата выдавший его сертификационный орган должен приостановить действие сертификата в соответствии с политикой и процедурами, регулирующими порядок приостановления действия и предусмотренными применимым заявлением о практике сертификации, либо, в отсутствие таких политики и процедур, незамедлительно по получении требования об этом от лица, которого сертификационный орган разумно считает держателем, обозначенным в сертификате, либо лицом, уполномоченным действовать от имени такого держателя.

Справочные материалы

A/CN.9/437, пункты 133—135 (проект статьи F).

Замечания

69. На своей предыдущей сессии Рабочая группа приняла решение о том, что Единообразные правила должны содержать положение о приостановлении действия сертификатов (A/CN.9/437, пункты 133—134). Что касается момента вступления в силу приостановления действия, то Рабочая группа может пожелать принять решение о добавлении в Правила положений, сходных с пунктами 4) и 5) проекта статьи 13.

Статья 15. Регистр сертификатов

1) Сертификационные органы ведут общедоступный электронный регистр выданных сертификатов, указывающий, когда истекает срок действия отдельного сертификата либо когда его действие было приостановлено или он был аннулирован.

2) Регистр хранится сертификационным органом

Вариант A: в течение по меньшей мере [30] [10] [5] лет

Вариант B: ... *[принимающее государство указывает срок хранения в регистре соответствующей информации]*

после даты аннулирования или истечения срока действия любого сертификата, выданного этим сертификационным органом.

Вариант C: в соответствии с политикой и процедурами, установленными сертификационным органом в применимом заявлении о практике сертификации.

Справочные материалы

A/CN.9/437, пункты 140—148 (проект статьи G);
A/CN.9/WG.IV/WP.71, пункты 68—69.

Замечания

70. На предыдущей сессии принципиальных возражений по поводу включения в Единообразные правила положения о регистрации сертификатов не прозвучало (см. A/CN.9/437, пункт 142). Надлежащее ведение общедоступного регистра (именуемого иногда "хранилищем данных"), в состав которого входил бы, в частности, перечень аннулированных сертификатов (ПАС), можно считать важным элементом в деле установления достоверности подписей в цифровой форме. Занимаясь вопросом о порядке ведения подобных регистров и ПАС, Рабочая группа может пожелать рассмотреть и вопрос о том, стоит ли обязать полагающиеся на сертификат стороны проверять его статус через соответствующий регистр или ПАС до того, как они будут полагаться на действительность сертификата.

71. В более широком плане Рабочая группа может пожелать обсудить вопрос о том, должны ли Единообразные правила, устанавливающие минимальные стандарты функционирования сертификационных органов, регулировать также права и обязанности сторон, полагающихся на сертификаты.

Статья 16. Отношения между сторонами, полагающимися на сертификаты, и сертификационными органами

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

2) Сертификационный орган предоставляет по запросу 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, которое будет использоваться полагающимися на сертификаты сторонами;

f) условиях, на которых сертификационный орган может направлять полагающимся на сертификаты сторонам 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 держатель имеет право устанавливать ограничения в отношении использования сертификата.

3) 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.

4) 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.

5) 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 сертификационным органом.]

Справочные материалы

A/CN.9/437, пункты 149—150 (проект статьи J);
A/CN.9/WG.IV/WP.71, пункт 76.

Замечания

72. На своей предыдущей сессии Рабочая группа отметила, что различные элементы, перечисленные в проекте статьи 15, следует заключить в квадратные скобки, с тем чтобы рассмотреть их на более позднем этапе (см. A/CN.9/437, пункт 150).

РАЗДЕЛ IV. ПРИЗНАНИЕ ИНОСТРАННЫХ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Статья 17. Иностранные сертификационные органы, предлагающие услуги на основании настоящих Правил

Вариант A

1) Иностранные [лица] [организации] могут получить местную регистрацию в качестве сертификационных органов либо могут оказывать сертификационные услуги, находясь в другой стране и не получая местную регистрацию, если они удовлетворяют тем же объективным стандартам и следуют тем же процедурам, что и местные организации и лица, имеющие право стать сертификационными органами.

2) Вариант X Правило, изложенное в пункте 1), не применяется к следующему: [...].

Вариант Y Исключения из правила, изложенного в пункте 1), могут быть сделаны в пределах, которые диктуются соображениями национальной безопасности.

Вариант B

... /принимающее государство указывает орган или ведомство, компетентное устанавливать правила в связи с одобрением иностранных сертификатов/ управомочен одобрять иностранные сертификаты и устанавливать конкретные правила, касающиеся такого одобрения.

Справочные материалы

A/CN.9/437, пункты 74—89 (проект статьи I);
A/CN.9/WG.IV/WP.71, пункты 73—75.

Замечания

73. Проект статьи 17, в котором иностранным организациям разрешается получать оформление в качестве сертификационных органов, содержит констатацию принципа, согласно которому иностранные организации, отвечающие установленным для местных сертификационных органов стандартам, не должны подвергаться дискриминации. Хотя этот принцип может быть в целом приемлемым, возможно особо важно изложить его применительно к сертификационным органам, поскольку предполагается, что такие органы могут функционировать, не обосновываясь при этом физически или не приобретая какого-либо места ведения деловых операций в стране своего функционирования.

Статья 18. Подтверждение иностранных сертификатов местными сертификационными органами

Сертификаты, выданные иностранными сертификационными органами, могут использоваться для подписей в цифровой форме на тех же условиях, что и сертификаты, подпадающие под действие настоящих Правил, если они признаются сертификационным органом, функционирующим на основании... /закона принимающего государства/, и этот сертификационный орган гарантирует — в той же мере, что и в отношении своих собственных сертификатов — правильность содержащейся в сертификате информации, а также его действительность и законную силу.

Справочные материалы

A/CN.9/437, пункты 74—89 (проект статьи I);
A/CN.9/WG.IV/WP.71, пункты 73—75.

Замечания

74. Проект статьи 18 позволяет местному сертификационному органу гарантировать — в той же мере, что и в отношении своих собственных сертификатов — правильность содержащейся в иностранном сертификате информации, а также его действительность и законную силу. Он затрагивает вопросы, связанные с тем, что на предыдущей сессии Рабочей группы получило название "перекрестной сертификации". В проекте 18 по сути содержится положение о возложении ответственности на внутренний сертификационный орган в случае, если иностранный сертификат оказывается порочным (см. A/CN.9/437, пункты 77—78).

Статья 19. Признание иностранных сертификатов

1) Сертификаты, выданные иностранным сертификационным органом, признаются имеющими такую же юридическую силу, что и сертификаты, выданные сертификационными органами, функционирующими на основании... *[закона принимающего государства]*, если практика иностранного сертификационного органа обеспечивает степень надежности по меньшей мере эквивалентную той, которая требуется от сертификационных органов в соответствии с настоящими Правилами. [Такое признание может быть осуществлено путем опубликования соответствующего государственного решения либо путем заключения двустороннего или многостороннего соглашения между заинтересованными государствами.]

2) Подписи и записи, соответствующие законам другого государства в отношении подписей в цифровой форме и других электронных подписей, признаются имеющими такую же юридическую силу, что и подписи и записи, соответствующие настоящим Правилам, если законы этого другого государства требуют степени надежности по меньшей мере эквивалентной той, которая требуется от подобных записей и подписей согласно... *[праву принимающего государства]*. [Такое признание может быть осуществлено путем опубликования соответствующего государственного решения либо путем заключения двустороннего или многостороннего соглашения с другими государствами.]

3) За подписями в цифровой форме, проверяемыми путем сверки с сертификатом, выданным иностранным сертификационным органом, [суды и другие органы, занимающиеся установлением фактов] должны признавать юридическую силу в том случае, если такой сертификат является, с учетом всех обстоятельств, надежным в той мере, насколько это требуется для цели, для которой он был выдан.

4) Независимо от положений предыдущего пункта правительственные ведомства могут указать [путем публикации], что в оформлении представляемых этим ведомствам подписей должны участвовать какой-либо конкретный сертификационный орган, определенная категория сертификационных органов или категория сертификатов.

Справочные материалы

A/CN.9/437, пункты 74—89 (проект статьи I);
A/CN.9/WG.IV/WP.71, пункты 73—75.

Замечания

75. Проект статьи 19 затрагивает вопросы, связанные с тем, что на предыдущей сессии Рабочей группы получило название "перекрестной сертификации" (см. A/CN.9/437, пункты 77—78). В пунктах 1) и 2) предусматриваются способы определения надежности иностранных сертификатов и подписей еще до

начала какой-либо деловой операции (и до возникновения спора относительно степени надежности какой-либо подписи). Пункт 3) устанавливает стандарт, в соответствии с которым можно оценивать иностранные подписи и сертификаты в тех случаях, когда степень их надежности не была определена заранее. Пункт 4) сохраняет за правительственными ведомствами право устанавливать процедуры, которые следует соблюдать при общении с ними через электронные средства связи.

* * *

Примечания

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

[2] Там же, Пятьдесят первая сессия, Дополнение № 17 (A/52/17), пункты 249—251.