ОРГАНИЗАЦИЯ
ОБЪЕДИНЕННЫХ НАЦИЙ

A

Генеральная Ассамблея

Distr.
LIMITED

A/CN.9/WG.IV/WP.76
25 May 1998

RUSSIAN
ORIGINAL: ENGLISH

КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ
Рабочая группа по электронной торговле
Тридцать третья сессия
Нью-Йорк, 29 июня — 10 июля 1998 года

ПРОЕКТ ЕДИНООБРАЗНЫХ ПРАВИЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

Записка Секретариата

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

1. На своей двадцать девятой сессии (1996 год) Комиссия 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 проектов 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. В отношении более четкого мандата для Рабочей группы было достигнуто согласие в 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 (1997 год) Комиссии 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, например, 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 правовым вопросам подписей в цифровой форме и сертификационных органов (далее именуемые "единообразными правилами").

4. В отношении конкретной сферы применения и формы таких единообразных правил Комиссия в целом согласилась с тем, 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 очевидной ведущей роли криптографии публичных ключей в зарождающейся практике электронной торговли, подготавливаемые единообразные правила должны соответствовать нейтральному с точки зрения носителей информации подходу, который взят за основу в Типовом законе ЮНСИТРАЛ об электронной торговле. Таким образом, единообразные правила не должны препятствовать использованию других методов удостоверения подлинности. Кроме того, при решении вопросов, связанных с криптографией публичных ключей, в этих единообразных правилах, возможно, необходимо будет учесть различия в уровнях обеспечения надежности и признать различные правовые последствия и уровни ответственности, соответствующие различным видам услуг, оказываемых в контексте подписей в цифровой форме. Что касается сертификационных органов, то Комиссия, хотя она и признала ценность стандартов, определяемых рыночными отношениями, в целом согласилась с тем, что Рабочая группа может

надлежащим образом предусмотреть разработку минимального свода стандартов, которые должны будут строго соблюдаться сертификационными органами, особенно в случае необходимости трансграничной сертификации[2].

5. Рабочая группа приступила к разработке единообразных правил на своей тридцать второй сессии на основе записки, подготовленной Секретариатом (A/CN.9/WG.IV/WP.73). Секретариату было поручено подготовить на основе этих обсуждений и заключений свод пересмотренных положений, с возможными вариантами, для рассмотрения Рабочей группой на одной из будущих сессий (доклад о работе этой сессии см. в A/CN.9/446). Что касается включения путем ссылки, то Рабочая группа приняла текст проекта положения, постановила представить его Комиссии для рассмотрения и возможного включения в качестве статьи 5бис в Типовой закон ЮНСИТРАЛ об электронной торговле и просила Секретариат подготовить пояснительную записку для добавления в Руководство по принятию Типового закона (A/CN.9/446, пункт 24).

6. В настоящей записке содержатся пересмотренные проекты положений, подготовленные с учетом обсуждений и решений Рабочей группы, а также обсуждений и решений Комиссии на ее тридцатой сессии, воспроизведенных выше. В частности, эти проекты положений основываются на принятой Рабочей группой рабочей гипотезе, согласно которой ее работа в области подписей в цифровой форме будет вестись в виде подготовки проекта законодательных положений (A/CN.9/437, пункт 27). Они также призваны отразить принятое Рабочей группой на ее тридцать первой сессии решение о том, что возможные единообразные правила должны вытекать из статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле (далее именуемого "Типовым законом") и должны считаться устанавливающими порядок возможного использования надежного метода "с целью идентификации лица" и "указания на то, что это лицо согласно" с информацией, содержащейся в сообщении данных.

7. В ходе подготовки настоящей записки Секретариату оказывала содействие группа экспертов, состоящая как из экспертов, приглашенных Секретариатом, так и из экспертов, назначенных заинтересованными правительствами и международными организациями.

8. В соответствии с применимыми инструкциями, касающимися более строгого контроля за документами Организации Объединенных Наций и ограничения их объема, пояснительные замечания к проектам положений являются настолько краткими, насколько это возможно. Дополнительные разъяснения будут даны устно в ходе сессии.

I. ОБЩИЕ ЗАМЕЧАНИЯ

9. Цель единообразных правил, отраженная в проектах положений, которые изложены в части II настоящей записки, заключается в содействии более широкому использованию электронных подписей в международных коммерческих сделках. Опираясь на многие законодательные документы, которые действуют или в настоящее время разрабатываются в ряде стран, данные проекты положений направлены на предупреждение несогласованности правовых норм, применимых к электронной торговле, путем установления совокупности стандартов, на основе которых могут быть признаны правовые последствия подписей в цифровой форме и других электронных подписей, с возможной помощью сертификационных органов, для чего также предусматривается ряд основных правил.

10. Сосредоточиваясь на частноправовых аспектах торговых сделок, единообразные правила не пытаются решить все вопросы, которые могут возникать в контексте более широкого использования электронных подписей. В частности, единообразные правила не касаются аспектов публичного порядка, административного права, потребительского права или уголовного права, которые, возможно, необходимо принять во внимание национальным законодателям при создании всеобъемлющей правовой основы для электронных подписей.

11. Единообразные правила основываются на Типовом законе и призваны, в частности, отразить: принцип нейтралитета с точки зрения носителей информации, подход, согласно которому не следует игнорировать функциональные эквиваленты традиционных понятий и практики, основанных на

использовании бумажных документов, и широкое признание автономии сторон. Они предназначаются для использования в качестве как минимальных стандартов в "открытой" среде (т. е. когда стороны сносятся друг с другом с помощью электронных средств без предварительного согласия), так и субсидиарных правил в "закрытой" среде (т. е. когда стороны связаны существующими договорными нормами и процедурами, подлежащими соблюдению при передаче сообщений с помощью электронных средств).

II. ПРОЕКТЫ 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 проектов 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 представить Комиссии предложения в отношении того, должны ли единообразные правила о подписях в цифровой форме являться отдельным правовым документом или же их следует включить в расширенный вариант Типового закона, например, в качестве новой Части третьей Типового закона.

13. Если единообразные правила будут подготовлены в качестве отдельного документа, то, как представляется, они должны будут включать положения, аналогичные статьям 1 (Сфера применения), 2 (a), (c) и (d) (Определения терминов "сообщение данных", "составитель" и "адресат"), 3 (Толкование), 7 (Подпись) и 13 (Атрибуция сообщения данных) Типового закона. Хотя эти статьи не воспроизводятся в настоящей записке, следует отметить, что проекты положений единообразных правил разрабатывались Секретариатом на основе предположения о том, что эти положения станут частью единообразных правил. В отношении сферы применения единообразных правил следует иметь в виду, что согласно статье 1 Типового закона сделки, касающиеся потребителей, хотя и не будут в центре внимания единообразных правил, не исключаются из сферы их применения, если только законодательство, применимое к потребительским сделкам в принимающем государстве, не противоречит единообразным правилам.

14. Что касается вопроса об автономии сторон, то простая ссылка на статью 4 (Изменение по договоренности) может и не быть достаточной для удовлетворительного решения с учетом того факта, что статья 4 проводит различие между теми положениями Типового закона, которые можно свободно изменить по договору, и теми положениями, которые должны считаться обязательными, если только изменение по договоренности не разрешено законодательством, применимым за пределами сферы действия Типового закона. Что касается электронных подписей, то практическое значение "закрытых" сетей обусловливает необходимость обеспечить широкое признание автономии сторон. В то же время, возможно, потребуется принять во внимание и основывающиеся на публичном порядке ограничения свободы договора, включая законы, направленные на защиту потребителей от уловок, связанных с договорами присоединения. Таким образом, Рабочая группа может пожелать включить в единообразные правила положение, аналогичное статье 4(1) Типового закона и устанавливающее, что, если иное не предусмотрено единообразными правилами или другим применимым законом, за электронными подписями и сертификатами, которые были выданы или получены или на которые стороны сделки полагаются в соответствии с согласованными ими процедурами, будут признаваться последствия, указанные в соглашении сторон. Кроме того, Рабочая группа может рассмотреть возможность установления правила толкования, предусматривающего, что при определении того, является ли сертификат, электронная подпись или сообщение данных, проверенное путем ссылки на сертификат, достаточно надежным для той или иной конкретной цели, во внимание должны приниматься все соответствующие соглашения, в которых участвуют стороны, любая установившаяся в их отношениях практика и любое применимое торговое обыкновение.

15. Помимо вышеупомянутых положений, Рабочая группа может пожелать рассмотреть вопрос о том, следует ли в преамбуле разъяснить цель единообразных правил, а именно содействие эффективному использованию цифровых сообщений путем создания основы для обеспечения неприкосновенности

сообщений и придания письменным и цифровым сообщениям равного статуса с точки зрения их правовых последствий.

РАЗДЕЛ II. ЭЛЕКТРОННЫЕ ПОДПИСИ

Часть I. Электронные подписи в целом

Статья 1. Определения

Для целей настоящих Правил:

a) "Электронная подпись" означает данные, исполненные в электронной форме и внесенные в текст либо приложенные к тексту, либо логически ассоциируемые с текстом сообщения и [они могут использоваться] используемые с целью [идентификации подписавшего это сообщение данных и указания на то, что подписавшийся согласен с информацией, содержащейся в сообщении данных] [выполнения условий, установленных в статье 7(1)(a) Типового закона ЮНСИТРАЛ об электронной торговле];

b) "[Усиленная] [Защищенная] электронная подпись" означает электронную подпись, которая [проставлена и] [со времени ее проставления] может быть проверена с помощью применения какой-либо процедуры защиты или комбинации процедур защиты, которое обеспечивает, что такая электронная подпись:

i) присуща исключительно подписавшемуся [для цели, с которой] [в контексте, в котором] она используется;

ii) может использоваться для объективной идентификации подписавшего сообщение данных;

iii) была проставлена и добавлена к сообщению данных подписавшимся или с использованием средства, находящегося под исключительным контролем подписавшегося; [или]

[iv) была проставлена и связана с сообщением данных, к которому она относится, таким образом, что любое изменение в сообщении данных было бы выявлено].

c) Вариант A

"Подпись в цифровой форме" означает такую электронную подпись, проставленную путем преобразования сообщения данных с использованием резюмирующей функции сообщения и кодирования полученного преобразования с помощью асимметрической криптосистемы с использованием частного ключа подписавшегося, что любое лицо, располагающее первоначальным, не подвергшимся преобразованию, сообщением данных, закодированным преобразованием и соответствующим публичным ключом подписавшегося, может [точно] определить:

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

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

Вариант B

"Подпись в цифровой форме" представляет собой такое криптографическое преобразование (с использованием асимметрического криптографического метода) цифровой формы сообщения данных, что любое лицо, располагающее сообщением данных и надлежащим публичным ключом, может определить:

i) что такое преобразование осуществлено с использованием частного ключа, соответствующего надлежащему публичному ключу; и

ii) что сообщение данных не было изменено после криптографического преобразования.

d) "Сертификационный орган" означает любое лицо или организацию, которые в рамках своих деловых операций занимаются выдачей сертификатов [личности] в отношении криптографических ключей, используемых для целей подписей в цифровой форме. [Настоящее определение применяется с учетом любого применимого закона, который требует, чтобы сертификационный орган получил лицензию, был аккредитован или функционировал таким образом, который указан в этом законе.]

e) "Сертификат [личности]" означает сообщение данных или иную запись, которые выдаются сертификационным органом и которые предназначены для подтверждения личности [или другой существенной характеристики] лица или организации, которые являются держателем определенной пары ключей.

f) "[Усиленный] [Защищенный] сертификат" означает сертификат [личности], выданный с целью поддержки [усиленных] [защищенных] электронных подписей.

g) "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.

h) "Подписавшийся" означает лицо, которое или от имени которого [использует электронную подпись] [используется электронная подпись] [использует данные в качестве электронной подписи] [данные используются в качестве электронной подписи].

Справочные материалы

A/CN.9/446, пункты 27—46 (проект статьи 1), 62—70 (проект статьи 4), 113—131 (проект статьи 8), 132—133 (проект статьи 9);
A/CN.9/WG.IV/WP.73, пункты 16—27, 37—38, 50—57 и 58—60;
A/CN.9/437, пункты 29—50 и 90—113 (проекты статей A, B и C); и
A/CN.9/WG.IV/WP.71, пункты 52—60.

Замечания

Определения "электронной подписи" и "[усиленной] [защищенной] электронной подписи

16. В соответствии с решением, принятым Рабочей группой на ее тридцать второй сессии (A/CN.9/446, пункт 30), определение "электронной подписи" содержит ссылку на статью 7 Типового закона. В зависимости от решения, которое будет принято в отношении взаимосвязи между единообразными правилами и Типовым законом, положения статьи 7(1)(a) Типового закона, возможно, потребуется изложить полностью.

17. Различие между широким понятием "электронной подписи" и более узкой категорией (предварительно названной "усиленной" или "защищенной" электронной подписью) было сохранено с целью подчеркнуть расхождения в правовом статусе этих двух видов процедур. С одной стороны, широкий

спектр неконкретизированных способов удостоверения подлинности (называемых "электронными подписями") может получить правовое признание как юридически значимая подпись при условии, что они отвечают критерию надежности, установленному в статье 7(1)(a) Типового закона, которую потребуется определить после использования электронной подписи и которая, как правило, требует вмешательства судьи, арбитра или иного лица, решающего вопрос факта. С другой стороны, определенное число способов удостоверения подлинности, указываемых с помощью административных процедур, которые должны определяться каждым принимающим государством, или же в результате прямого соглашения между сторонами, может получить заблаговременное признание в качестве функциональных эквивалентов собственноручных подписей.

Определение "подписи в цифровой форме"

18. Категория "подписей в цифровой форме" не определяется как подраздел "усиленных" электронных подписей. Это призвано отразить то обстоятельство, что хотя в большинстве ситуаций "цифровые" способы (с опорой или без опоры на сертификационные органы) будут использоваться для обеспечения правовых последствий, предусматриваемых для более "защищенной" категории электронных подписей, такие способы могут также использоваться в менее конкретном контексте. Таким образом, определение "подписи в цифровой форме" призвано подчеркнуть нейтральный с точки зрения носителей информации характер единообразных правил.

Определение "сертификационного органа"

19. Единообразные правила не устанавливают какое-либо требование в отношении стандартов, которым должны удовлетворять сертификационные органы прежде, чем им будет разрешено функционировать. Этот вопрос обсуждался Рабочей группой на предыдущих сессиях, а также затрагивается в проекте статьи 19. Если будет сочтено необходимым дать ориентиры принимающим государствам либо в тексте единообразных правил, либо в руководстве по принятию, то вниманию можно предложить следующий пример возможного положения:

Сертификационные органы должны:

a) обладать надежностью, необходимой для предоставления услуг по сертификации;

b) задействовать персонал, обладающий специальными познаниями, опытом и квалификацией, необходимыми для предоставления таких услуг;

c) использовать надежные системы и общепризнанное аппаратное и программное обеспечение, подходящее для предлагаемого вида услуг и степени защиты;

d) располагать достаточными финансовыми ресурсами в целях функционирования в соответствии с [настоящими Правилами];

e) хранить всю соответствующую информацию, касающуюся [усиленного] [защищенного] сертификата, в течение надлежащего периода времени, в частности для того, чтобы быть в состоянии представить доказательства сертификации в контексте какого-либо судебного иска. Такое хранение может обеспечиваться с помощью электронных средств;

f) публиковать всю соответствующую информацию, касающуюся надлежащего и защищенного использования услуг по сертификации и устанавливать процедуры рассмотрения жалоб и урегулирования споров; и

g) публиковать в отношении услуг, которыми может воспользоваться публика, всю соответствующую информацию, касающуюся используемых процедур и применяемой практики, положений и условий договоров, в частности принимаемых ими на себя обязательств относительно ответственности, а также применяемых ими процедур рассмотрения жалоб и урегулирования споров; соответственно, такие публикации должны быть легкодоступными.

Определения "сертификата [личности]" и "[усиленного] [защищенного] сертификата"

20. Содержащиеся в подпунктах (e) и (f) определения основываются на высказанном на тридцать второй сессии Рабочей группы предложении отличать случаи, когда подписи в цифровой форме используются в целях международных торговых операций с намерением поставить подпись (т. е. идентифицировать подписавшегося и установить связь между подписавшимся и подписанной информацией), от других видов использования подписей в цифровой форме, например для определения уровня полномочий того или иного лица ("сертификаты полномочий") (см. A/CN.9/446, пункт 72). Хотя положения, содержащиеся в разделе III единообразных правил, касаются главным образом способов проставления подписи в цифровой форме в качестве средства установления заранее определенной эквивалентности собственноручным подписям, Рабочая группа может пожелать обсудить степень, в которой способы проставления подписи в цифровой форме следует рассматривать в других контекстах. Если единообразные правила будут сосредоточиваться на подписях в цифровой форме как эквиваленте собственноручных подписей, то, возможно, и не будет необходимости проводить различие между "сертификатами", "сертификатами личности" и "[усиленными] [защищенными] сертификатами". Можно напомнить о том, что любое менее защищенное использование подписей в цифровой форме может также охватываться общими положениями проекта статьи 2.

Статья 2. Правовые последствия электронной подписи

(1) В отношении сообщения данных, подлинность которого удостоверяется при помощи электронной подписи [иной, чем защищенная электронная подпись], электронная подпись отвечает любому правовому требованию, предъявляемому к какой-либо подписи, если эта электронная подпись является как надежной, так и соответствующей цели, для которой эта электронная подпись используется, с учетом всех обстоятельств, включая любую соответствующую договоренность.

(2) Пункт (1) применяется независимо от того, выражено ли правовое требование, упомянутое в нем, в форме обязательства или же законодательство просто предусматривает наступление определенных последствий, если подпись отсутствует.

(3) Если только это не указано прямо где-либо в [настоящем Законе], на электронные подписи, которые не являются [усиленными] [защищенными] электронными подписями, не распространяется действие положений, стандартов или же процедур лицензирования, установленных ... [указанными государством органами или ведомствами, упоминаемыми в статье], или презумпций, предусмотренных статьями 4, 5 и 6.

(4) Положения настоящей статьи не применяются в следующих случаях: [...].

Справочные материалы

A/CN.9/446, пункты 27—46 (проект статьи 1).

Замечания

21. Проект статьи 2 призван учесть правовые последствия электронных подписей, которые не отвечают требованиям, установленным для признания "усиленного" или "защищенного" статуса. Согласно мандату, полученному от Комиссии, и с учетом мнений, высказанных на тридцать второй сессии Рабочей группы (см. A/CN.9/446, пункты 4 и 45), цель этого проекта статьи заключается в обеспечении нейтральности единообразных правил с точки зрения носителей информации, разъяснении того, что использование менее защищенных способов удостоверения подлинности не запрещается, и обеспечении надлежащего признания автономии сторон, не разрешая им отходить от обязательных норм права, касающихся подписей. В пунктах (1), (2) и (4) всего лишь вновь излагаются положения, содержащиеся в статье 7 Типового закона. В пункте (3) упоминается различие, которое следует проводить между правовыми последствиями электронных подписей в целом в противопоставлении "усиленным" или "защищенным" способам удостоверения подлинности.

Часть II. [Усиленные] [Защищенные] электронные подписи

Статья 3. Презумпция подписания

(1) Сообщение данных презюмируется подписанным, [если] [[усиленная] [защищенная] электронная подпись приложена к этому сообщению данных] [[с момента] приложения к этому сообщению данных [усиленной] [защищенной] электронной подписи].

(2) Положения настоящей статьи не применяются в следующих случаях: [...].

Справочные материалы

A/CN.9/446, пункты 47—48 (проект статьи 2) и 49—61 (проект статьи 3);
A/CN.9/WG.IV/WP.73, пункты 28—36; и
A/CN.9/437, пункты 43, 48 и 92.

Замечания

22. Формулировка этого проекта статьи, устанавливающего презумпцию того, что какое-либо сообщение данных должно считаться "подписанным", если его подлинность удостоверена защищенной электронной подписью, была изменена с учетом высказанного на тридцать второй сессии мнения о необходимости разъяснения взаимосвязи между определением защищенной электронной подписи и презумпциями, вытекающими из использования такой защищенной электронной подписи (см. A/CN.9/446, пункт 34).

23. Единообразные правила не содержат определения "подписи" и указания на какие-либо конкретные правовые последствия, которыми наделяется какая-либо "подпись" такого рода. Согласно проекту статьи 3 правовые последствия подписи должны определяться ссылкой на внутреннее право, находящееся за пределами сферы действия единообразных правил.

Статья 4. Презумпция атрибуции

(1) [Усиленная] [Защищенная] электронная подпись презюмируется подписью лица, которым или от имени которого она, как предполагается, была использована,

Вариант A — если только предполагаемый подписавшийся не устанавливает, что эта [усиленная] [защищенная] электронная подпись была проставлена без разрешения.

Вариант B — при условии, что доверяющая сторона устанавливает, что процедура защиты или комбинация процедур защиты, использовавшаяся для проверки подписи,

a) была коммерчески обоснованной при данных обстоятельствах;

b) была применена доверяющей стороной заслуживающим доверия образом; и

c) доверяющая сторона полагалась на эту подпись обоснованно и добросовестно.

(2) Положения настоящей статьи не применяются в следующих случаях: [...].

Справочные материалы

A/CN.9/446, пункты 49—61 (проект статьи 3);
A/CN.9/WG.IV/WP.73, пункты 33—36;
A/CN.9/437, пункты 118—124 (проект статьи E); и
A/CN.9/WG.IV/WP.71, пункты 64—65.

Замечания

24. Вариант A касается атрибуции электронной подписи путем возложения бремени доказывания согласно предложениям, высказанным на тридцать второй сессии Рабочей группы (см. A/CN.9/446, пункт 60). Вариант B возлагает бремя доказывания на доверяющую сторону.

Статья 5. Презумпция целостности

(1) Если предполагаемый подписавшийся использовал процедуру защиты, которая способна дать [достоверные] доказательства того, что сообщение данных или любая [[усиленная] [защищенная] электронная] [электронная] подпись на нем не была изменена с момента применения этой процедуры защиты к этому сообщению данных или к любой подписи, то тогда презюмируется [в отсутствие доказательств обратного], что это сообщение данных или подпись не были изменены.

(2) Положения настоящей статьи не применяются в следующих случаях: [...].

Справочные материалы

A/CN.9/446, пункты 47—48 (проект статьи 2);
A/CN.9/WG.IV/WP.73, пункты 28—32; и
A/CN.9/437, пункты 43, 48 и 92.

Замечания

25. В предыдущем проекте единообразных правил содержалась ссылка на проверку целостности сообщения данных как на один из элементов "защищенной электронной подписи". До сведения Секретариата было доведено, что проверка целостности сообщения данных может быть произведена с помощью отдельных процедур. Более того, вполне понятно, что определенные способы удостоверения подлинности могут достигнуть высокой степени защиты, требуемой согласно определению "усиленных" электронных подписей без проверки целостности сообщения данных.

26. Если Рабочая группа сочтет это более приемлемым, то формулировки положений проектов статей 3, 4 и 5 можно будет изменить для установления правовых последствий вместо презумпций.

Статья 6. Предварительное определение [усиленной] [защищенной] электронной подписи

(1) Процедура защиты или комбинация процедур защиты удовлетворяет требованиям [усиленной] [защищенной] электронной подписи, если об этом заявляет ...[орган или ведомство, указанное принимающим государством как компетентное сделать такое заявление...].

(2) Во взаимоотношениях лица, подписывающего сообщение данных, и любого лица, доверяющего подписанному сообщению, процедура защиты или комбинация процедур защиты считается отвечающей требованиям [усиленной] [защищенной] электронной подписи, если стороны прямо согласились с этим.

(3) Положения пункта (2) не применяются в следующих случаях: [...].

Справочные материалы

A/CN.9/446, пункты 37—45 (проект статьи 1); и
A/CN.9/WG.IV/WP.73, пункт 27.

Замечания

27. В отличие от не отвечающих требованиям "электронных подписей", которые рассматриваются в проекте статьи 2, [усиленные] [защищенные] электронные подписи согласно проекту статьи 6 дают преимущество в том, что либо посредством соблюдения применимых положений, либо непосредственно путем заключения договора коммерческие стороны могут достичь определенности в отношении правовых последствий любого данного способа подписания до использования этого способа. Рабочая группа может пожелать обсудить вопрос о том, следует ли предусмотреть ограничения автономии сторон в этом отношении в самих единообразных правилах или же просто оставить это на усмотрение внутреннего права согласно пункту (3) (см. выше, пункт 14).

Статья 7. Ответственность за [усиленную] [защищенную] электронную подпись

Вариант А

Если [усиленная] [защищенная] электронная подпись использовалась без разрешения и предполагаемый подписавшийся не проявил разумной осмотрительности во избежание неразрешенного использования его подписи и для предотвращения того, чтобы адресат доверял такой подписи, предполагаемый подписавшийся обязан [возместить ущерб для компенсации доверяющей стороне причиненного вреда] возместить причиненный вред, за исключением случаев, когда доверяющая сторона знала или должна была знать, что данная подпись не является подписью предполагаемого подписавшегося.

Вариант В

Если [усиленная] [защищенная] электронная подпись использовалась без разрешения и предполагаемый подписавшийся не проявил разумной осмотрительности во избежание неразрешенного использования его подписи и для предотвращения того, чтобы адресат доверял такой подписи, эта подпись, тем не менее, считается подписью предполагаемого подписавшегося, за исключением случаев, когда доверяющая сторона знала или должна была знать, что данная подпись не является подписью предполагаемого подписавшегося.

Справочные материалы

A/CN.9/446, пункты 49—61 (проект статьи 3);
A/CN.9/WG.IV/WP.73, пункты 33—36;
A/CN.9/437, пункты 118—124 (проект статьи E); и
A/CN.9/WG.IV/WP.71, пункты 64—65.

Замечания

28. На своей тридцать второй сессии Рабочая группа обсудила вопрос о том, следует ли в единообразных правилах предусмотреть только атрибуцию защищенных электронных подписей (или подписей в цифровой форме) или же следует также затронуть вопрос об ответственности предполагаемого подписавшегося перед доверяющими сторонами. Было подчеркнуто, что при установлении связи между электронной подписью и предполагаемым подписавшимся единообразные правила должны также создавать стимул для использования подписей в цифровой форме за счет надлежащего распределения ответственности за убытки, причиненные доверяющей стороне в результате неспособности предполагаемого подписавшегося проявить

разумную осмотрительность и не допустить неразрешенного использования его подписи (см. A/CN.9/446, пункт 51).

29. Рабочая группа может пожелать обсудить связь между единообразными правилами и статьей 13 Типового закона. Хотя статья 13 Типового закона касается атрибуции сообщения данных, вопрос об атрибуции электронной подписи рассматривается в определении "[усиленной] [защищенной] электронной подписи" и в проекте статьи 4.

30. Вариант A ограничивает ответственность предполагаемого подписавшегося ущербом, доказанным доверяющей стороной, который может быть исчислен на деликтной или договорной основе, в зависимости от обстоятельств. Вариант B устанавливает ответственность предполагаемого подписавшегося за содержание сообщения данных.

Часть III. Подписи в цифровой форме, подтвержденные сертификатами

Статья 8. Содержание [усиленного] [защищенного] сертификата

Для целей настоящих Правил в [усиленном] [защищенном] сертификате, по меньшей мере:

a) идентифицируется выдавший его сертификационный орган;

b) называются или идентифицируются [подписавшийся] [субъект сертификата] либо соответствующее устройство или электронный агент, находящиеся под контролем [подписавшегося] [субъекта сертификата] [данного лица];

c) содержится публичный ключ, соответствующий частному ключу, находящемуся под контролем [подписавшегося] [субъекта сертификата];

d) указывается срок действия сертификата;

e) имеется подпись в цифровой форме или же обеспечена как-либо иначе его защита выдавшим его сертификационным органом;

[f) указываются ограничения, если таковые установлены, в отношении сферы использования публичного ключа;] [и]

[g) идентифицируется алгоритм, подлежащий применению].

Справочные материалы

A/CN.9/446, пункты 113—131 (проект статьи 8);
A/CN.9/WG.IV/WP.73, пункты 50—57;
A/CN.9/437, пункты 98—113 (проект статьи C); и
A/CN.9/WG.IV/WP.71, пункты 18—45 и 59—60.

Замечания

31. На своей тридцать второй сессии Рабочая группа не решила вопрос о том, должны ли единообразные правила содержать в порядке редактирования ссылку на "субъект сертификата" или же конкретно указывать, что таким субъектом должно быть какое-либо "лицо". Для облегчения работы с текстом единообразных правил неизменно использовался термин "подписавшийся", тогда как термин "субъект" был также сохранен для сопоставления. Хотя единообразные правила вполне могут включать ссылку на понятие "лица", в таком случае потребовалось бы существенное изменение формулировок во избежание

двусмысленности в том, какое лицо предполагается охватить. В определении "подписавшегося" согласно проекту статьи 1(h) указывается, что подписавшийся должен быть "лицом".

Статья 9. Правовые последствия подписей в цифровой форме, подтвержденных сертификатами

(1) В отношении всего сообщения данных или какой-либо его части в случае, когда составитель идентифицирован подписью в цифровой форме, эта подпись в цифровой форме [является [усиленной] [защищенной] электронной подписью] [удовлетворяет условиям, установленным в статье 7 Типового закона ЮНСИТРАЛ об электронной торговле], если:

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

b) сертификат устанавливает связь между публичным ключом и личностью [подписавшегося] [соответствующего лица] в силу того факта, что:

i) сертификат был выдан сертификационным органом, получившим лицензию от ... [принимающее государство указывает орган или ведомство, компетентное выдавать лицензии сертификационным органам и принимать правила, регулирующие функционирование получивших лицензию сертификационных органов]; или

ii) сертификат был выдан сертификационным органом, аккредитованным ответственным аккредитационным органом, применяющим коммерчески обоснованные и международно признанные стандарты, относящиеся к вопросам надежности технологии, практики и других соответствующих характеристик функционирования сертификационного органа. Неисчерпывающий перечень таких аккредитационных органов или стандартов, удовлетворяющих условиям настоящего пункта, может быть опубликован ... [принимающее государство указывает орган или ведомство, компетентное устанавливать признанные стандарты функционирования получивших лицензию сертификационных органов]; или

iii) сертификат был иным образом выдан в соответствии с коммерчески обоснованными и международно признанными стандартами [.] [; или]

[iv) достаточные доказательства показывают, что сертификат устанавливает [четкую] связь между публичным ключом и личностью [подписавшегося] [субъекта].]

[(2) В случае, когда сообщение данных подписано с использованием подписи в цифровой форме [проставленной в течение срока действия сертификата], не удовлетворяющей требованиям, изложенным в пункте (1), эта подпись в цифровой форме считается [усиленной] [защищенной] электронной подписью , если имеются достаточные доказательства того, что [данный сертификат] устанавливает четкую связь между публичным ключом и личностью [подписавшегося] [субъекта сертификата].]

(3) Положения настоящей статьи не применяются в следующих случаях: [...].

Справочные материалы

A/CN.9/446, пункты 71—84 (проект статьи 5);
A/CN.9/WG.IV/WP.73, пункты 39—44; и
A/CN.9/437, пункты 43, 48 и 92.

Замечания

32. Вступительная формулировка пункта (1) отражает решение, принятое Рабочей группой на ее тридцать второй сессии (см. A/CN.9/446, пункт 76).

33. 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 ссылки на сертификат, являются защищенными, особенно если нет уверенности в точности идентификации подписавшегося или удостоверения подлинности публичного ключа. К числу важнейших факторов, определяющих защищенность подписи в цифровой форме, относятся следующие: 1) должным ли образом сертификационный орган идентифицировал подписавшегося; 2) должным ли образом сертификационный орган удостоверил подлинность публичного ключа подписавшегося; 3) не скомпрометирован ли частный ключ подписавшегося; и 4) заслуживает ли доверия процесс проверки (например, отвечают ли необходимым требованиям алгоритм публичного ключа и длина ключа).

34. В пункте 1) устанавливаются два базовых критерия для 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 аннулировния или приостановления действия сертификата.

35. Ко второму этапу относится установление гарантий того, что сам сертификат точно идентифицирует соответствующее лицо в качестве подписавшегося по отношению к частному ключу, соответствующему публичному ключу, указанному в сертификате. Степень достоверности сертификата может быть оценена путем ссылки на стандарты, процедуры и прочие требования, устанавливаемые признанными органами принимающего государства. Такие стандарты могут устанавливаться посредством аккредитации сертификационных органов третьими сторонами, добровольного лицензирования сертификационных органов, в иных же случаях требуется соответствие нормам, введенным в принимающем государстве.

36. 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 подписавшегося и удостоверившим подлинность публичного ключа подписавшегося.

37. В соответствии с "двойственным подходом", принятым Рабочей группой, проект статьи 9 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.

38. Важно также отметить, что в то время как один из вариантов поекта статьи 9 содержит установление точности сертификатов судебными органами, другой предполагает точность сертификата в случае его выдачи сертификационным органом, аккредитованным принимающим 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, может ли любой их акт, совершаемый с доверием к соответствующему сообщению, быть исполнен в принудительном порядке.

Однако презумпция точности сертификата может быть опровергнута доказательством того, что сертификат, выданный таким аккредитованным сертификационным органом, на самом деле не является точным или надежным (см. A/CN.9/WG.IV/WP.73, пункты 39—44).

РАЗДЕЛ III. СЕРТИФИКАЦИОННЫЕ ОРГАНЫ И СМЕЖНЫЕ ВОПРОСЫ

Статья 10. Гарантия, предоставляемая при выдаче сертификата

(1) Выдавая сертификат, сертификационный орган гарантирует [любому лицу, разумно полагающемуся на сертификат], что:

3 a) сертификационный орган выполнил все применимые требования [настоящих Правил];

b) вся содержащаяся в сертификате информация является точной на момент его выдачи, [если только сертификационный орган не указал в сертификате, что точность определенной информации не подтверждена];

c) насколько известно сертификационному органу, в сертификате не упущены никакие существенные факты, которые могли бы отрицательно сказаться на достоверности информации, содержащейся в сертификате; и

[d) если сертификационный орган опубликовал заявление о практике сертификации, сертификат был выдан сертификационным органом в соответствии с этим заявлением о практике сертификации.]

(2) Выдавая [усиленный] [защищенный] сертификат, сертификационный орган предоставляет в отношении [подписавшегося] [субъекта], идентифицируемого в сертификате, [любому лицу, разумно полагающемуся на сертификат,] следующие дополнительные гарантии:

a) что публичный и частный ключи [подписавшегося] [субъекта], идентифицируемого в сертификате, составляют действующую пару ключей; и

b) что во время выдачи сертификата частный ключ:

i) является ключом [подписавшегося] [субъекта], идентифицируемого в сертификате; и

ii) соответствует публичному ключу, указанному в сертификате.

Справочные материалы

A/CN.9/446, пункты 134—145 (проект статьи 10);
A/CN.9/WG.IV/WP.73, пункты 61—63;
A/CN.9/437, пункты 51—73 (проект статьи H); и
A/CN.9/WG.IV/WP.71, пункты 70—72.

Замечания

39. Проект статьи 10 основывается на различии между [усиленными] [защищенными] сертификатами и более широкой категорией сертификатов. В зависимости от решения, которое будет принято Рабочей группой в отношении степени, в которой единообразные правила должны затрагивать подписи в цифровой форме, используемые в иных целях, чем для установления заранее определенной эквивалентности собственноручным подписям, это различие, возможно, и не потребуется проводить (см. выше, пункт 20).

Статья 11. Договорная ответственность

Вариант A

(1) Во взаимоотношениях между сертификационным органом, выдавшим сертификат, и держателем этого сертификата [или какой-либо иной доверяющей стороной, находящейся в договорных отношениях с сертификационным органом] права и обязательства сторон [и их любое ограничение] определяются достигнутым между ними соглашением [при условии соблюдения применимого права].

[(2) При условии соблюдения статьи 10 сертификационный орган может, по соглашению между сторонами, снять с себя ответственность за любой ущерб, [возникший в результате доверия к сертификату], [вызванный дефектами информации, указанный 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.]

Вариант B

В соответствии с применимым правом права и обязательства сертификационного органа, [подписавшегося] [субъекта], идентифицированного в сертификате, и любой другой стороны регулируются соглашением или соглашениями, заключенными между этими сторонами, в той мере, в какой такое соглашение или соглашения касаются таких прав и обязательств, а также их любых ограничений.

Вариант C

В случае, когда соглашения заключаются сертификационным органом, [подписавшимся] [субъектом], идентифицированным в сертификате, и любой другой стороной, права и обязательства этих сторон и их любое ограничение, которые предусмотрены этими соглашениями, регулируются этими соглашениями в соответствии с применимым правом и в той мере, в какой это допускается применимым правом.

Справочные материалы

A/CN.9/446, пункты 146—154 (проект статьи 11);
A/CN.9/WG.IV/WP.73, пункты 64—65;
A/CN.9/437, пункты 51—73 (проект статьи H); и
A/CN.9/WG.IV/WP.71, пункты 70—72.

Замечания

40. До рассмотрения предлагаемых вариантов проекта статьи 11 Рабочая группа может пожелать обсудить вопрос о том, следует ли сохранить проект статьи 11 в качестве части единообразных правил. На тридцать второй сессии Рабочей группы было указано, что данный проект статьи касается вопросов, которые целесообразно решать на основе договора и применимого права. В частности, было отмечено, что, возможно, и нет необходимости вновь излагать принцип автономии сторон, который охватывается статьей 4 Типового закона, и что другие положения этого проекта статьи вступают в коллизию с национальным правом по вопросам, возможность унификации которых проблематична. Хотя решение оставить вопросы договорной ответственности на урегулирование на основе договора и права, применимого за пределами сферы действия единообразных правил, было признано приемлемой альтернативой, возобладало мнение о том, что имеет смысл попытаться достигнуть определенной степени единообразия в урегулировании этого важного предмета (см. A/CN.9/446, пункт 148).

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

(1) При условии соблюдения пункта (2), если сертификационный орган выдает сертификат, он несет ответственность перед любым лицом, разумно полагающимся на этот сертификат, за:

a) ошибки в сертификате, если только сертификационный орган не докажет, что он или его агенты приняли [все разумные] [коммерчески обоснованные] меры [, которые соответствовали цели, для которой был выдан сертификат, с учетом всех обстоятельств] для избежания ошибок в сертификате;

b) непринятие мер по регистрации аннулирования сертификата, если только сертификационный орган не докажет, что он или его агенты приняли [все разумные] [коммерчески обоснованные] меры [, которые соответствовали цели, для которой был выдан сертификат, с учетом всех обстоятельств] для регистрации аннулирования сразу же после получения уведомления о его аннулировании [; и

c) последствия неприменения следующего:

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

ii) любой процедуры, предусмотренной применимым правом].

(2) Доверие к сертификату не является разумным в той мере, в которой оно противоречит информации, содержащейся в сертификате [или включенной в него путем ссылки] [или в перечне аннулирования] [или в информации об аннулировании]. [Доверие не является разумным, в частности, если:

a) оно противоречит цели, для которой выдан сертификат;

b) оно оказано в превышение стоимости, в отношении которой сертификат является действительным; или

c) [...].]

Справочные материалы

A/CN.9/446, пункты 155—173 (проект статьи 12);
A/CN.9/WG.IV/WP.73, пункты 66—67;
A/CN.9/437, пункты 51—73 (проект статьи H); и
A/CN.9/WG.IV/WP.71, пункты 70—72.

Замечания

41. Проект статьи 12 отражает решение, принятое Рабочей группой на ее тридцать второй сессии (A/CN.9/446, пункт 173). На той же сессии было высказано мнение о том, что проект статьи 12 должен применяться только в отношении сертификационных органов, выдающих сертификаты личности.

Общее замечание относительно проектов статей 13—16

42. На своей предыдущей сессии по причине нехватки времени Рабочая группа отложила рассмотрение проектов статей 13—16 до своей будущей сессии (см. A/CN.9/446, пункт 174). За исключением редакционной правки, направленной в основном на обеспечение согласованности различных положений, включенных в пересмотренный текст единообразных правил, тексты проектов статей 13—16, содержащиеся в настоящей записке, в целом идентичны текстам этих статей, изложенным в документе A/CN.9/WG.IV/WP.73.

Статья 13. Аннулирование сертификата

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

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

b) достоверных доказательств наступления смерти [подписавшегося][субъекта], если таковым является физическое лицо; или

c) достоверных доказательств ликвидации или прекращения существования [подписавшегося][субъекта], если таковым является юридическое лицо.

(2) [Подписавшийся][субъект] в отношении сертифицированной пары ключей обязан аннулировать соответствующий сертификат или потребовать его аннулирования, если [подписавшийся][субъект] узнает, что частный ключ был утерян или скомпрометирован или подвергается опасности неправильного использования в других отношениях. Если [подписавшийся][субъект] не аннулирует сертификат или не потребует его аннулирования в такой ситуации, то этот [подписавшийся][субъект] несет ответственность перед любой стороной, полагавшейся на содержание сообщения, за ущерб в результате того, что этот [подписавшийся][субъект] не произвел такого аннулирования.

(3) Независимо от того, дает ли свое согласие на аннулирование [подписавшийся][субъект], идентифицированный в сертификате, сертификационный орган, выдавший сертификат, должен аннулировать сертификат сразу же после того, как ему станет известно, что:

a) изложенные в сертификате существенные 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 [подписавшегося[[субъекта] сертификата.

(3) После аннулирования сертификата согласно пункту (3) сертификационный орган должен уведомить [подписавшегося[[субъекта] сертификата и полагающиеся на сертификат стороны в соответствии с политикой и процедурами, регулирующими порядок уведомления об аннулировании сертификата и предусмотренными применимым заявлением о практике сертификации, либо в отсутствие такой политики и процедур, незамедлительно уведомить [подписавшегося[[субъекта] сертификата и незамедлительно 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 [подписавшимся[[субъектом] 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 [регистрации][опубликования] сертификационным органом.]

Справочные материалы

A/CN.9/446, пункт 174 (проект статьи 13);
A/CN.9/WG.IV/WP.73, пункт 68;
A/CN.9/437, пункты 125—139 (проект статьи F); и
A/CN.9/WG.IV/WP.71, пункты 66—67.

Замечания

43. Проект статьи 13 призван отразить различные точки зрения, высказанные на тридцать первой сессии Рабочей группы, путем установления субсидиарного стандарта, регулирующего порядок аннулирования сертификатов. Однако сертификационный орган может всегда избежать этого субсидиарного 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 том, следует ли проводить различие между положением подписавшего сертификат 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 такой политики и процедур, незамедлительно по получении требования об этом от лица, которого сертификационный орган разумно считает [подписавшимся][субъектом], идентифицированным в сертификате, либо лицом, уполномоченным действовать от имени такого [подписавшегося][субъекта].

Справочные материалы

A/CN.9/446, пункт 174 (проект статьи 14);
A/CN.9/WG.IV/WP.73, пункт 69; и
A/CN.9/437, пункты 133—135 (проект статьи F).

Замечания

44. На своей тридцать первой 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 том, следует ли добавлять к правилам положения, аналогичные принципам, изложеннным в пунктах (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 — в течение ... [принимающее государство указывает срок хранения в регистре соответствующей информации]

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

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

Справочные материалы

A/CN.9/446, пункт 174 (проект статьи 15);
A/CN.9/WG.IV/WP.73, пункты 70—71;
A/CN.9/437, пункты 140—148 (проект статьи G); и
A/CN.9/WG.IV/WP.71, пункты 68—69.

Замечания

45. На тридцать первой сессии Рабочей группы 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 сертификационными органами 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.

46. 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 [подписавшегося][субъекта сертификата].

(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 [подписавшийся][субъект] имеет право устанавливать ограничения в отношении использования сертификата.

(3) Информация, указанная в пункте (1), предоставляется [потенциальному] [подписавшемуся][субъекту] 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] [подписавшийся][субъект] 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.]

Справочные материалы

A/CN.9/446, пункт 174 (проект статьи 16);
A/CN.9/WG.IV/WP.73, пункт 72;
A/CN.9/437, пункты 149—150 (проект статьи J); и
A/CN.9/WG.IV/WP.71, пункт 76.

Замечания

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

РАЗДЕЛ IV. ИНОСТРАННЫЕ ЭЛЕКТРОННЫЕ ПОДПИСИ

Статья 17. Предоставление услуг иностранными сертификационными органами

(1) Вариант A Иностранные [лица] [организации] могут получить местную регистрацию в качестве сертификационных органов либо могут предоставлять 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.

Вариант B В соответствии с законодательством принимающего государства иностранное [лицо] [организация] может:

a) получить местную регистрацию в качестве сертификационного органа; или

b) предоставлять сертификационные услуги без получения местной регистрации, если [оно] [она] удовлетворяет тем же объективным стандартам и следует тем же процедурам, что и местные организации и лица, имеющие право стать сертификационными органами.

Вариант C Иностранным [лицам] [организациям] не может быть отказано в праве на получение местной регистрации или на предоставление сертификационных услуг лишь

на том основании, что они являются иностранными, 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 в следующих случаях:

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

Справочные материалы

A/CN.9/446, пункты 175—188 (проект статьи 17);
A/CN.9/WG.IV/WP.73, пункт 73;
A/CN.9/437, пункты 74—89 (проект статьи I); и
A/CN.9/WG.IV/WP.71, пункты 73—75.

Замечания

48. Разрешая иностранным организациям получать регистрацию в качестве сертификационных органов, проект статьи 17 всего лишь излагает принцип, согласно которому иностранные организации не должны подвергаться дискриминации при условии, что они удовлетворяют стандартам, установленным для местных сертификационных органов. Хотя этот принцип, возможно, является общепризнанным, особенно важно изложить его в отношении сертификационных органов, поскольку сертификационные органы, как предполагается, могут функционировать, не создавая при этом физических отделений или другого коммерческого предприятия в той стране, в которой они действуют.

Статья 18. Подтверждение иностранных сертификатов местными сертификационными органами

Вариант A 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 ... [закон 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.

Вариант B 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 в их отношении сертификационным органом, функционирующим на основании ... [закон принимающего государства], выдана соответствующая гарантия.

Справочные материалы

A/CN.9/446, пункт 189—195 (проект статьи 18);
A/CN.9/WG.IV/WP.73, пункт 74;
A/CN.9/437, пункты 74—89 (проект статьи I); и
A/CN.9/WG.IV/WP.71, пункт 73—75.

Замечания

49. Проект статьи 18 позволяет внутреннему 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 касается вопросов, которые

были названы вопросами "перекрестной сертификации" на тридцать первой сессии Рабочей группы. Проект статьи 18 по существу содержит 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

Вариант A

(1) Вариант X Сертификаты, выданные иностранными сертификационными органами, не могут быть лишены такого же признания, как и сертификаты, выданные внутренними сертификационными органами, на том основании, что они были выданы иностранными сертификационными органами.

Вариант Y Сертификаты, выданные иностранным сертификационным органом, признаются юридически эквивалентными сертификатам, выданным сертификационными органами, функционирующими на основании ... [закон 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, касающимся подписей в цифровой форме или других электронных подписей, признаются юридически эквивалентными подписям и записям, соответствующим настоящим Правилам, если законы этого другого государства требуют степени надежности, по меньшей мере эквивалентной той, которая требуется от подобных записей и подписей согласно ... [закон принимающего государства]. [Такое признание может быть осуществлено путем опубликования соответствующего государственного решения либо путем заключения двустороннего или многостороннего соглашения с другими государствами.]

(2)[3] Подписи в цифровой форме, проверяемые путем ссылки на сертификат, выданный иностранным сертификационным органом, [не могут быть лишены юридической силы] [наделяются юридической силой] [судами и другими органами, занимающимися установлением фактов,], если этот сертификат является как надежным, так и соответствующим цели, для которой он был выдан, с учетом всех обстоятельств.

(3)[4] Независимо от положений предыдущего пункта правительственные ведомства и стороны коммерческих и иных сделок могут указать, что в оформлении представляемых им сообщений или подписей должны участвовать какой-либо конкретный сертификационный орган, определенная категория сертификационных органов или категория сертификатов.

Вариант B

(1) Сертификаты, выданные иностранным сертификационным органом, признаются юридически эквивалентными сертификатам, выданным сертификационными органами, функционирующими на основании ... [закон 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.

[(2) Определение эквивалентности, упоминаемое в пункте (1), может быть произведено путем опубликования соответствующего государственного решения либо путем заключения двустороннего или многостороннего соглашения с другими государствами.]

(3) При определении эквивалентности необходимо учитывать следующие факторы:

a) финансовые и людские ресурсы, включая наличие активов в пределах юрисдикции;

b) надежность систем аппаратного и программного обеспечения;

c) процедуры оформления сертификатов и рассмотрения заявок на сертификаты, а также хранения записей;

d) наличие информации для [подписавшихся] [субъектов], идентифицированных в сертификатах, и для потенциальных сторон, полагающихся на сертификаты;

e) регулярность и масштабы аудита, проводимого каким-либо независимым органом;

f) наличие заявления государства, аккредитационного органа или сертификационного органа относительно соблюдения или наличия вышеизложенного;

g) подсудность судам принимающего государства; и

h) степень расхождений между законодательством, применимым к ответственности сертификационного органа, и законодательством принимающего государства.

Вариант C

Иностранный сертификационный орган считается надежным [в принимающем государстве] для цели сертификата, выдаваемого им в подтверждение подписей в отношении сообщений данных, если при выдаче такого сертификата этот сертификационный орган соблюдает или, по меньшей мере, несет такие же обязательства, как обязательства, возлагаемые настоящими Правилами и любым внутренним режимом лицензирования, применимым к сертификату такого типа.

Вариант D

(1) Иностранный сертификационный орган считается надежным [в принимающем государстве] для цели сертификата, выдаваемого им в подтверждение подписей в отношении сообщений данных, если при выдаче такого сертификата этот сертификационный орган обеспечивает степень надежности, [по меньшей мере] эквивалентную той, [которая требуется от] которой обладают внутренние сертификационные органы, выдающие такие сертификаты.

(2) При оценке степени надежности сертификационного органа необходимо учитывать следующие факторы:

a) финансовые и людские ресурсы, включая наличие активов в пределах юрисдикции;

b) надежность систем аппаратного и программного обеспечения;

c) процедуры оформления сертификатов и рассмотрения заявок на сертификаты, а также хранения записей;

d) наличие информации для [подписавшихся] [субъектов], идентифицированных в сертификатах, и для потенциальных сторон, полагающихся на сертификаты;

e) регулярность и масштабы аудита, проводимого каким-либо независимым органом;

f) наличие заявления государства, аккредитационного органа или сертификационного органа относительно соблюдения или наличия вышеизложенного;

g) подсудность судам принимающего государства; и

h) степень расхождений между законодательством, применимым к ответственности сертификационного органа, и законодательством принимающего государства.

Справочные материалы

A/CN.9/446, пункты 196—207 (проект статьи 19);
A/CN.9/WG.IV/WP.73, пункт 75;
A/CN.9/437, пункты 74—89 (проект статьи I); и
A/CN.9/WG.IV/WP.71, пункты 73—75.

Замечания

50. Проект статьи 19 касается вопросов, которые были названы вопросами "трансграничного признания" на тридцать первой сессии Рабочей группы (см. A/CN.9/437, пункты 77—78). Вариант A основывается на предложении об объединении пунктов (1) и (2), внесенном на тридцать второй сессии Рабочей группы (см. A/CN.9/446, пункты 197—204). Вариант B содержит примерный перечень критериев, которые следует учитывать при оценке надежности иностранных сертификатов. Варианты C и D сосредоточиваются на признании иностранных сертификационных органов. Можно отметить, что если Рабочая группа решит включить в единообразные правила критерии, которым должны отвечать внутренние сертификационные органы (см. выше, пункт 19), то, возможно, и не будет необходимости устанавливать такие критерии в проекте статьи 19.

* * *

Примечания

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

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