ОРГАНИЗАЦИЯ
ОБЪЕДИНЕННЫХ НАЦИЙ

A

Генеральная Ассамблея

Distr.
LIMITED

A/CN.9/WG.IV/WP.79
23 November 1998

RUSSIAN
Original: ENGLISH

КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ
Рабочая группа по электронной торговле
Тридцать четвертая сессия
Вена, 8-19 февраля 1999 года

ПРОЕКТ ЕДИНООБРАЗНЫХ ПРАВИЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

Записка Секретариата

СОДЕРЖАНИЕ

	Пункты	Страница
ВВЕДЕНИЕ	1-11	3
I. ОБЩИЕ ПРИМЕЧАНИЯ	12-14	4
II. ПРОЕКТЫ ПОЛОЖЕНИЙ О ЦИФРОВЫХ ПОДПИСЯХ, ДРУГИХ ЭЛЕКТРОННЫХ ПОДПИСЯХ, СЕРТИФИКАЦИОННЫХ ОРГАНАХ И СООТВЕТСТВУЮЩИХ ПРАВОВЫХ ВОПРОСАХ	15-53	5
ГЛАВА I. СФЕРА ПРИМЕНЕНИЯ И ОБЩИЕ ПОЛОЖЕНИЯ	15-20	5
ГЛАВА II. ЭЛЕКТРОННЫЕ ПОДПИСИ	21-48	6
Раздел I. Электронные подписи в целом	21-23	6
Статья 1. Определения	21	6
Статья 2. Соблюдение требований законодательства	22-23	8
Раздел II. [Усиленные] электронные подписи	24-44	9
Статья 3. [ ]	24-30	9
Статья 4. Презумпция атрибуции [усиленной] электронной подписи	31-33	11
Статья 5. Презумпция целостности	34-37	12

СОДЕРЖАНИЕ (продолжение)

		Пункты	Страница
Статья 6.	Предварительное определение [усиленной] электронной подписи	38-41	13
Статья 7.	Ответственность за несанкционированное использование [усиленной] электронной подписи	42-44	14
Раздел III.	Цифровые подписи, подтвержденные сертификатами	45-48	16
Статья 8.	Содержание [усиленных] сертификатов	45-46	16
Статья 9.	Последствия цифровых подписей, подтвержденных сертификатами	47-48	18
ГЛАВА III.	СЕРТИФИКАЦИОННЫЕ ОРГАНЫ И СМЕЖНЫЕ ВОПРОСЫ	49-53	20
Статья 10.	Гарантия при выдаче [усиленного] сертификата	49-50	20
Статья 11.	Договорная ответственность	51	21
Статья 12.	Ответственность сертификационного органа перед сторонами, полагающимися на сертификаты	52	22
Общие примечания в отношении проектов статей 13-15		53	23
Статья 13.	Аннулирование сертификата	--	23
Статья 14.	Приостановление действия сертификата	--	24
Статья 15.	Регистр сертификатов	--	24

ВВЕДЕНИЕ

1. На своей двадцать девятой сессии (1996 год) Комиссия постановила включить в повестку дня вопросы о подписях в цифровой форме и сертификационных органах. Рабочей группе по электронной торговле было предложено рассмотреть целесообразность и возможность подготовки единообразных правил по этим темам. Было достигнуто согласие в отношении того, что единообразные правила, которые следует подготовить, должны охватывать такие вопросы, как: правовая основа, поддерживающая процессы сертификации, включая появляющуюся технологию удостоверения подлинности и сертификации в цифровой форме; применимость процесса сертификации; распределение риска и ответственности пользователей, поставщиков и третьих сторон в контексте использования методов сертификации; конкретные вопросы сертификации через применение регистров; и включение путем ссылки[1].

2. На тридцатой сессии (1997 год) Комиссии был представлен доклад Рабочей группы о работе ее тридцать первой сессии (A/CN.9/437). Рабочая группа сообщила Комиссии, что она достигла консенсуса в отношении важного значения и необходимости работы в направлении согласования норм права в этой области. Хотя она не приняла окончательного решения в отношении формы и содержания такой работы, Рабочая группа пришла к предварительному выводу о том, что 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).

3. Комиссия одобрила заключения Рабочей группы и поручила ей подготовить единообразные правила по юридическим вопросам подписей в цифровой форме и сертификационных органов (далее в тексте - "единообразные правила").

4. В отношении конкретной сферы применения и формы таких единообразных правил было выражено общее мнение, 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 (Типовой закон). Таким образом, единообразные правила не должны препятствовать использованию других методов удостоверения подлинности. Кроме того, при решении вопроса криптографии публичных ключей в единообразных правилах, возможно, необходимо будет учесть различия в уровнях защиты и признать различные юридические последствия и уровни ответственности, соответствующие различным видам услуг, оказываемых в контексте подписей в цифровой форме. Что касается сертификационных органов, то Комиссия, хотя она и признала ценность стандартов, определяемых рыночными отношениями, в целом согласилась с тем, что Рабочая группа может надлежащим образом предусмотреть разработку минимального свода стандартов, которые должны будут строго соблюдаться сертификационными органами, особенно в случае необходимости трансграничной сертификации[2].

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

6. На тридцать первой сессии (1998 год) Комиссии был представлен доклад Рабочей группы о работе ее тридцать второй сессии (A/CN.9/446). Комиссия выразила признательность Рабочей группе за усилия по подготовке проекта единообразных правил об электронных подписях. Было отмечено, что на своих тридцать первой и тридцать второй сессиях Рабочая группа столкнулась с очевидными трудностями в достижении общего понимания новых правовых вопросов, которые возникают в связи с расширением использования подписей в цифровой и другой электронной форме. Было отмечено также, что еще предстоит достичь

консенсуса в отношении того, каким образом эти вопросы можно было бы урегулировать в международно приемлемых правовых рамках. В то же время Комиссия в целом сочла, что достигнутый к настоящему моменту прогресс свидетельствует о том, что проект единообразных правил об электронных подписях постепенно превращается в документ, который можно будет применять на практике.

7. Комиссия подтвердила принятое на ее тридцать первой сессии решение относительно возможности разработки единообразных правил и выразила уверенность в том, что на своей тридцать третьей сессии (Нью-Йорк, 29 июня - 10 июля 1998 года) Рабочая группа сможет добиться дальнейшего прогресса на основе пересмотренного проекта, подготовленного Секретариатом (A/CN.9/WG.IV/WP.76). В контексте этого обсуждения Комиссия с удовлетворением отметила, что по общему признанию Рабочая группа стала особо важным международным форумом для обмена мнениями по правовым вопросам электронной торговли и выработки решений по этим вопросам.

8. На своей тридцать третьей сессии (1998 год) Рабочая группа продолжила рассмотрение единообразных правил на основе записки, подготовленной Секретариатом (A/CN.9/WG.IV/WP.76). Доклад о работе этой сессии содержится в документе A/CN.9/454.

9. В настоящей записке содержатся пересмотренные проекты положений, подготовленные с учетом обсуждений и решений Рабочей группы, а также обсуждений и решений Комиссии на ее тридцать первой сессии, воспроизведенных выше. Они призваны отразить решения, принятые Рабочей группой на ее тридцать третьей сессии.

10. 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.

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

I. ОБЩИЕ ПРИМЕЧАНИЯ

12. 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, эти проекты положений направлены на предупреждение несогласованности правовых норм, применимых к электронной торговле, путем установления совокупности стандартов, на основе которых могут быть признаны правовые последствия цифровых и других электронных подписей, с возможной помощью сертификационных органов, для которых также предусматривается ряд основных правил.

13. В единообразных правилах, в которых основное внимание сосредоточено на частноправовых аспектах торговых сделок, не предпринимается попытки 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.

14. Единообразные правила основываются на Типовом законе и призваны, в частности, отразить: принцип нейтральности с точки зрения носителей информации; недискриминационный подход в отношении функциональных эквивалентов 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 ЦИФРОВЫХ ПОДПИСЯХ, ДРУГИХ ЭЛЕКТРОННЫХ ПОДПИСЯХ, СЕРТИФИКАЦИОННЫХ ОРГАНАХ И СООТВЕТСТВУЮЩИХ ПРАВОВЫХ ВОПРОСАХ

ГЛАВА I. СФЕРА ПРИМЕНЕНИЯ И ОБЩИЕ ПОЛОЖЕНИЯ

15. 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 цифровых подписях быть приняты в качестве отдельного правового документа или же их следует включить в расширенный вариант Типового закона, например, в качестве новой части III Типового закона.

16. Если единообразные правила будут подготовлены в качестве отдельного документа, то, как представляется, они должны будут включать положения, аналогичные статье 1 (Сфера применения), статье 2 (необходимые определения), статье 3 (Толкование) и статье 4 (Изменение по договоренности) 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 будут включены в единообразные правила. В отношении сферы применения единообразных правил следует иметь в виду, что если будет включена статья, аналогичная статье 1 Типового закона, то сделки, касающиеся потребителей, не будут исключаться из сферы применения, если только законодательство, применимое к потребительским сделкам в принимающем государстве, не противоречит единообразным правилам.

17. Что касается вопроса об автономии сторон, то простой ссылки на статью 4 (Изменение по договоренности) может быть недостаточно для удовлетворительного решения. В статье 4 проводится различие между теми положениями Типового закона, которые можно свободно изменить по договоренности, и теми положениями, которые должны считаться императивными, 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 законодательством, 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, проверенные путем ссылки на сертификат, достаточно надежными для той или иной конкретной цели, во внимание должны приниматься все соответствующие соглашения, в которых участвуют стороны, любая установившаяся в их отношениях практика и любой соответствующий торговый обычай.

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

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

19. На своей тридцать третьей сессии Рабочая группа выразила сомнения в отношении приемлемости использования слов "усиленная" или "защищенная" для указания на методы подписания, которые могут обеспечить более высокую степень надежности, чем "электронные подписи" в целом (A/CN.9/454, пункт 29). Рабочая группа сделала вывод о том, что в отсутствие более подходящего термина следует сохранить слово "усиленная". Исходя из этих причин, в настоящем пересмотренном варианте единообразных правил в квадратных скобках используется слово "усиленная".

20. При обсуждении взаимосвязи между рассматриваемыми единообразными правилами и статьей 7 Типового закона Рабочая группа, возможно, пожелает изучить вопрос о том, следует ли ограничить применение рассматриваемых правил теми ситуациями, когда существуют юридические требования к форме или когда законодательство предусматривает определенные последствия, если какие-либо условия, такие как письменная форма или наличие подписи, не соблюдены. Следует напомнить о том, что в ходе подготовки Типового закона вопрос о содержании понятия требований в отношении формы уже рассматривался. В пункте 68 Руководства по принятию Типового закона отмечается, что слово "законодательство" ("the law"), использованное в Типовом законе, следует понимать как охватывающее не только статутное право или подзаконные акты, но также и нормы, создаваемые судами, и другие процессуальные нормы. Таким образом, слово "законодательство" охватывает также и правила доказывания. В тех случаях, когда в законодательстве не оговорено требование о соблюдении какого-либо конкретного условия, но предусмотрены последствия для случая несоблюдения условия, например для отсутствия письменной формы или наличия подписи, такие случаи также охватываются концепцией "законодательство", как она использована в Типовом законе.

ГЛАВА II. ЭЛЕКТРОННЫЕ ПОДПИСИ

Раздел I. Электронные подписи в целом

Статья 1. Определения

Для целей настоящих Правил:

a) "Электронная подпись" означает данные в электронной форме, содержащиеся в сообщении данных, приложенные к нему или логически ассоциируемые с ним и [которые могут использоваться] используемые с целью [идентификации лица, подписавшего 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] электронная подпись" означает электронную подпись, которая [создана и] [со времени ее создания] может быть проверена с помощью применения какой-либо процедуры защиты или комбинации процедур защиты, которая 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 создана и проставлена на сообщении данных подписавшимся или с использованием средства, находящегося под исключительным контролем подписавшегося; [или]

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

c) Вариант A

"Цифровая подпись" означает такую электронную подпись, созданную путем преобразования сообщения данных с использованием резюмирующей функции сообщения и кодирования полученного преобразования при помощи 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

"Цифровая подпись" 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 цифровых подписей. [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] 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, пункт 20;
A/CN.9/WG.IV/WP.76, пункты 16—20;
A/CN.9/446, пункты 27—46 (проект статьи 1), 62—70 (проект статьи 4), 113—131 (проект статьи 8), 132—133 (проект статьи 9);
A/CN.9/WG.IV/WP.73, пункты 16—27, 37—38, 50—57 и 58—60;
A/CN.9/437, пункты 29—50 и 90—113 (проекты статей A, B и C); и
A/CN.9/WG.IV/WP.71, пункты 52—60.

Примечания

21. На предыдущей сессии по причине нехватки времени Рабочая группа отложила рассмотрение проекта статьи 1 до одной из будущих сессий (см. A/CN.9/454, пункт 19). Если не считать исключения слова "защищенная", использовавшегося в связи с электронными подписями, текст проекта статьи 1 в настоящей записке идентичен тексту этого проекта статьи, содержащемуся в документе A/CN.9/WG.IV/WP.76.

Статья 2. Соблюдение требований законодательства

1) Применительно к сообщению данных, подлинность которого удостоверяется при помощи электронной подписи [иной, чем [усиленная] электронная подпись], электронная подпись отвечает любому требованию законодательства в отношении подписи, если способ, использованный для проставления электронной подписи, является как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано с учетом всех обстоятельств, включая любые соответствующие договоренности.

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

3) Если это прямо не предусматривается другими положениями [настоящего Закона], на электронные подписи, которые не являются [усиленными] электронными подписями, не распространяется действие положений, стандартов или же процедур лицензирования, установленных ... [указанными государством органами или ведомствами, упомянутыми в проекте статьи 6], или презумпций, созданных в силу статей 3, 4 и 5.

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

Справочные материалы

A/CN.9/454, пункты 21-27;
A/CN.9/WG.IV/WP.76, пункт 21; и
A/CN.9/446, пункты 27-46 (проект статьи 1).

Примечания

22. Цель проекта статьи 2 состоит в том, чтобы подтвердить связь между статьей 7 Типового закона и единообразными правилами. В проекте статьи 2(1) должным образом признается автономия сторон. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли сохранить в проекте статьи 2(1) заключенные в квадратные скобки слова ["иной, чем усиленная электронная почта"], поскольку они предполагают, что усиленная электронная подпись не отвечает требованиям статьи 7 Типового закона. Как представляется, это противоречит последствиям, создаваемым в силу варианта B проекта статьи 3.

23. Проект статьи 2(2) включен для обеспечения соответствия со статьей 7 Типового закона и по причинам, упомянутым выше в связи со значением слова "законодательство". В проекте статьи 2(3) четко устанавливается, что правила, применяемые к более высоким уровням "усиленных" или "защищенных" электронных подписей, например, правила, касающиеся возможных систем лицензирования сертификационных органов, или другие возможные нормы, регулирующие, в частности, цифровые подписи, в отношении всех видов "электронных подписей" в целом не применяются.

Раздел II. [Усиленные] электронные подписи

Статья 3.

Вариант A

Статья 3. Выполнение [усиленной] электронной подписью требований законодательства

1) В тех случаях, когда законодательство требует наличия подписи, это требование считается выполненным с помощью [усиленной] электронной подписи [, если не доказано, что [усиленная] электронная подпись не отвечает требованиям статьи 7 Типового закона].

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

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

Вариант B

Статья 3. Презумпция подписания

1) Сообщение данных презюмируется подписанным, если [усиленная] электронная подпись проставлена на сообщении данных или логически связана с ним.

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

Вариант C

Статья 3. Последствия, возникающие из использования [усиленной] электронной подписи

1) В случаях, когда в результате [использования] подписи возникли бы предусмотренные законом последствия, эти последствия возникают из [усиленной] электронной подписи.

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

Справочные материалы

A/CN.9/454, пункты 28-39;
A/CN.9/WG.IV/WP.76, пункты 22-23;
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.

Примечания

Вариант A

24. В варианте A применительно к усиленным электронным подписям устанавливается содержащее привязку правило, позволяющее обеспечить выполнение требований статьи 7 Типового закона. Этот вариант проекта статьи 3 и проект статьи 2 закладывают основу единообразных правил. Во-первых, в проекте статьи 2 еще раз закрепляется принцип статьи 7 Типового закона, состоящий в том, что электронная подпись может удовлетворять установленному законодательством требованию в отношении наличия подписи в том случае, если она отвечает определенным условиям. Во-вторых, вариант A проекта статьи 3 предусматривает, что [усиленная] электронная подпись удовлетворяет этим условиям, и устанавливается привязка, обеспечивающая соблюдение требований статьи 7.

25. Положение, подтверждающее, что слово "законодательство" применяется независимо от того, выражено ли соответствующее требование в форме обязательства или же законодательство просто предусматривает наступление определенных последствий, если какое-либо конкретное условие не соблюдено, было повторено в пункте 2 варианта A, с тем чтобы обеспечить единообразное значение слова "законодательство" в проекте единообразных правил и Типовом законе.

26. Если формулировка, заключенная в проекте варианта A в квадратные скобки, будет сохранена, то проект варианта A будет устанавливать привязку, обеспечивающую удовлетворение требований статьи 7 Типового закона; ее действие может быть приостановлено в случаях, когда представляются доказательства, свидетельствующие о том, что требования статьи 7 не удовлетворены. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли сохранить эту формулировку в проекте статьи 3.

Вариант B

27. Цель варианта B состоит в создании презумпции того, что сообщение данных может рассматриваться в качестве "подписанного", если его подлинность удостоверена усиленной электронной подписью. Собственно в рамках этой презумпции "подписание" сообщения рассматривается отдельно от вопроса об идентификации подписавшегося. Такая презумпция может быть важной в тех случаях, когда формальных требований в отношении подписи, как это предусматривается в статье 7 Типового закона, не имеется, однако наличие подписи на сообщении данных может быть важным для какой-либо другой цели, или в случаях, когда законодательство требует, чтобы сообщение было подписанным, не оговаривая вопрос о личности подписавшегося, или в случаях, когда вопрос о личности подписавшегося значения не имеет.

28. Вариант B в его настоящей редакции может применяться в ситуациях, являющихся дополнительными к случаям, предусмотренным в статье 7. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, охватывает ли двойной подход, используемый в статье 7 (т.е. случаи, когда законодательство требует наличия подписи, и случаи, когда устанавливаются последствия, если подпись отсутствует), все ситуации, когда может использоваться подпись и когда она может повлечь за собой юридические последствия. Если все такие ситуации не охватываются, то включение положения, аналогичного варианту B, может быть целесообразным. В подобных обстоятельствах могут быть одновременно сохранены вариант B и вариант A, поскольку вариант B будет касаться дополнительных обстоятельств.

29. Содержавшаяся в предыдущем проекте статьи 3 ссылка на момент проставления подписи была исключена, однако Рабочая группа, возможно, пожелает рассмотреть вопрос о возможной необходимости включения этой концепции в какое-либо другое положение проекта единообразных правил.

Вариант C

30. Цель этого варианта состоит в том, чтобы четко установить в единообразных правилах принцип недискриминации, как он отражен в статье 5 Типового закона. Это положение направлено на обеспечение того, чтобы в случаях, когда использование подписи ведет к возникновению юридических последствий, эти

последствия - независимо от формального требования к наличию подписи - были бы одинаковыми как для собственноручных, так и для электронных подписей. Действие этого варианта в значительной степени аналогично действию варианта B, поскольку для определения последствий в случаях, когда сообщение подписано (вариант B) или когда использована подпись (вариант C), они оба отсылают к внутреннему праву.

Статья 4. Презумпция атрибуции [усиленной] электронной подписи

1) [Усиленная] электронная подпись презюмируется подписью лица, которым или от имени которого она, как предполагается, была подготовлена, если только не установлено, что [усиленная] электронная подпись не была поставлена ни предполагаемым подписавшимся, ни лицом, уполномоченным действовать от его имени.

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

Справочные материалы

A/CN.9/454, пункты 40-53;
A/CN.9/WG.IV/WP.76, пункт 24;
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.

Примечания

31. В проекте статьи 4 устанавливается презумпция атрибуции применительно к [усиленным] электронным подписям, а также оговариваются два случая, когда эта презумпция не применяется. Собственно, в этом проекте статьи регулируются вопросы, рассматриваемые в статье 13 Типового закона, хотя в редакционном плане имеются определенные различия. Например, проект статьи 4 составлен в форме опровержимой презумпции атрибуции. С другой стороны, статья 13(2) Типового закона представляет собой положение, устанавливающее предположение, а в статье 13(3) закрепляется правило, которое предоставляет адресату право действовать исходя из атрибуции сообщения данных. Проект статьи 4 регулирует вопрос об атрибуции подписи, в то время как статья 13 Типового закона касается атрибуции сообщения данных. Критерии атрибуции подписи в проекте статьи 4 несколько отличаются от критериев, использованных в статье 13 Типового закона применительно к атрибуции сообщения данных.

32. Рабочая группа, возможно, пожелает рассмотреть взаимосвязь между проектом статьи 4 и статьей 13 Типового закона и, в частности, вопрос о том, имеется ли какая-либо юридическая необходимость в проведении разграничения между атрибуцией сообщения и атрибуцией подписи на этом сообщении. Здесь следует учитывать тот факт, что в силу технических причин проведение такого разграничения может быть невозможным. Можно предположить, что атрибуция подписи должна вытекать из атрибуции сообщения данных - или наоборот, - и в этом случае необходимо только одно правило об атрибуции.

33. Другой аспект проекта статьи 4 состоит в том, что в нем затрагивается вопрос о несанкционированном использовании электронной подписи. В этом отношении имеет место частичное дублирование вопросов, охваченных статьей 13 Типового закона. Например, в проекте статьи 4 предусматривается, что презумпция атрибуции не применяется в двух случаях: когда подпись не была поставлена ни предполагаемым подписавшимся, ни лицом, уполномоченным предполагаемым подписавшимся. С другой стороны, в статье 13 предусматривается, что независимо от того, являлось ли сообщение санкционированным, адресат может рассматривать сообщение данных как сообщение предполагаемого составителя. Рабочая группа, возможно, пожелает изучить вопрос о необходимости включения в рассматриваемые единообразные правила новой нормы о несанкционированном использовании подписей и о взаимосвязи такой нормы и проекта статьи 7 об ответственности.

Статья 5. Презумпция целостности

1) Вариант A

В случае, когда [надежная процедура защиты] [усиленная электронная подпись] надлежащим образом применяется к обозначенной части сообщения данных и указывает, что обозначенная часть сообщения данных не подвергалась изменениям с определенного момента, обозначенная часть сообщения данных презюмируется не изменявшейся с этого момента.

Вариант B

В случае, когда процедура защиты способна [надежно] [со значительной степенью определенности] продемонстрировать, что обозначенная часть сообщения данных не подвергалась изменениям с определенного момента, и надлежащее применение этой процедуры указывает на то, что сообщение данных не подвергалось изменениям, презюмируется, что [целостность сообщения данных была сохранена] [сообщение данных не подвергалось изменениям] с этого момента.

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

Справочные материалы

A/CN.9/454, пункты 54-63;
A/CN.9/WG.IV/WP.76, пункт 25-26;
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.

Примечания

34. Проект статьи 5 был пересмотрен в соответствии с решением Рабочей группы, принятым на ее тридцать третьей сессии (A/CN.9/454, пункты 54-63). Цель пересмотренного проекта состоит в том, чтобы установить презумпцию относительно целостности сообщения данных. Как представляется, оба варианта этого проекта статьи для создания такой презумпции требуют, чтобы процедуры защиты или подпись были фактически применены с результатом, показывающим, что сообщение не подвергалось изменениям. При наличии подобных доказательств презумпция, приводящая к тому же результату, не будет иметь практического значения. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли сформулировать этот проект статьи в качестве презумпции или в качестве материально-правовой нормы.

35. Одна из альтернатив, предусматриваемая в варианте A, основывается на том, что постановка подписи указывает на целостность. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли включить как постановку, так и проверку такой подписи (и использование функции хеширования или резюме сообщения), или же следует отдать предпочтение формулировке, предусматривающей применение процедуры защиты.

36. Как вариант A, так и вариант B проекта статьи 5(1) устанавливают прямую связь между подписанием сообщения и целостностью этого сообщения, однако условие наличия такой связи может быть не всегда полезным или необходимым. В ряде случаев функция целостности является неотъемлемой составной частью использованного вида технологии электронной подписи (как это может иметь место применительно к некоторым конкретным видам [усиленных] электронных подписей), и презумпция относительно целостности просто описывает прямой результат использования такой технологии. В других случаях использованная технология подписи может и не удовлетворять требованию о целостности, несмотря на то, что во всех других отношениях такая подпись может рассматриваться в качестве [усиленной] электронной подписи. Кроме того, имеются случаи, когда может возникнуть необходимость в доказывании целостности неподписанного

сообщения. В подобных случаях правило, устанавливающее прямую связь между целостностью и подписью, может оказаться нецелесообразным.

37. В тех случаях, когда целостность требуется для того, чтобы продемонстрировать, что сообщение является подлинником, применяется статья 8 Типового закона. Рабочая группа, возможно, пожелает изучить вопрос о том, следует ли включить в рассматриваемые правила презумпцию относительно целостности в качестве материально-правовой нормы, следует ли включить функцию целостности в определение [усиленной] электронной подписи, а также вопрос о взаимосвязи между этим проектом статьи и статьей 8 Типового закона.

Статья 6. Предварительное определение [усиленной] электронной подписи

1) [Орган или ведомство, указанное принимающим государством в качестве компетентного,] может определять:

a) что электронная подпись [является [усиленной] электронной подписью] [удовлетворяет требованиям статьи 7 Типового закона];

[b) что процедура защиты удовлетворяет требованиям статьи 5].

2) Любое определение, вынесенное в силу пункта 1, должно соответствовать признанным международным техническим стандартам.

3) [С учетом [настоящих Правил и] применимого законодательства] стороны могут договориться о том, что электронная подпись в отношениях между ними должна рассматриваться:

[a) в качестве [усиленной] электронной подписи];

[b) в качестве удовлетворяющей требованиям статьи 7 Типового закона].

Справочные материалы

A/CN.9/454, пункты 64-75;
A/CN.9/WG.IV/WP.76, пункт 27;
A/CN.9/446, пункты 37-45 (проект статьи 1); и
A/CN.9/WG.IV/WP.73, пункт 27.

Примечания

38. В предыдущем варианте проекта статьи 6(1) говорилось о подписи, удовлетворяющей требованиям проекта статьи 1(b) (определение [усиленной] электронной подписи). Изменение формулировки статьи 6 позволяет выносить определения о том, что электронная подпись является [усиленной] электронной подписью или - альтернативная возможность - что электронная подпись удовлетворяет требованиям статьи 7, т.е. этот вопрос решается с помощью непосредственной привязки. Если электронная подпись является [усиленной] электронной подписью в соответствии с вариантом A проекта статьи 3, то необходимости указывать, что она удовлетворяет требованиям статьи 7, не имеется, поскольку это ясно вытекает из ее [усиленного] статуса.

39. Пересмотренный вариант проекта статьи 6(1)(b), согласованный на тридцать третьей сессии Рабочей группы (A/CN.9/454, пункт 73), содержит ссылку на "требования статьи 5". Проект статьи 5, как он был пересмотрен на этой же сессии (A/CN.9/454, пункт 61), более не устанавливает требований в отношении целостности. Рабочая группа, возможно, пожелает вернуться к вопросу о включении в проект статьи 6(1)(b) ссылки на проект статьи 5.

40. В проекте статьи 6(2) слова "в тех случаях, когда они существуют" были исключены на том основании, что в контексте типового закона они не являются необходимыми. В тех случаях, когда подобные стандарты существуют, государства, принимающие единообразные правила, должны поощряться к их соблюдению, и соответствующее примечание могло бы быть включено, например, в руководство по принятию.

41. Формулировка проекта статьи 6(3) была пересмотрена, с тем чтобы отразить обеспокоенность, высказанную на тридцать третьей сессии Рабочей группы (A/CN.9/454, пункт 71) и состоящую в том, что, хотя необходимо обеспечить уважение автономии сторон, любое соглашение между сторонами в отношении использования электронной подписи не должно иметь последствий для третьих сторон. В пересмотренном варианте также учтена обеспокоенность (A/CN.9/454, пункт 75) относительно использования формулировки "определять последствия подписи" (подчеркивание добавлено) и относительно возможного толкования этой формулировки в различных правовых системах. В проекте пункта 3 воспроизводятся формулировки пункта 1 и предусматривается определение [усиленного] статуса в качестве альтернативы определению того, что подпись отвечает требованиям статьи 7 Типового закона.

Статья 7. Ответственность за несанкционированное использование [усиленной] электронной подписи

Вариант A

В случае, когда использование [усиленной] электронной подписи являлось несанкционированным и предполагаемый подписавшийся не проявил разумной осмотрительности для избежания несанкционированного использования его подписи и для предотвращения того, чтобы адресат положился на такую подпись,

Вариант X эта подпись тем не менее считается санкционированной, за исключением случая, когда полагающейся стороне стало известно или должно было стать известно, что данная подпись является несанкционированной.

Вариант Y предполагаемый подписавшийся может нести ответственность лишь за покрытие расходов по восстановлению положения сторон, существовавшего до несанкционированного использования подписи, за исключением случая, когда полагающейся стороне стало известно или должно было стать известно, что данная подпись не является подписью предполагаемого подписавшегося.

Вариант Z предполагаемый подписавшийся несет ответственность [за уплату убытков для компенсации полагающейся стороне] за нанесенный ущерб, за исключением случая, когда полагающейся стороне стало известно или должно было стать известно, что данная подпись не является подписью предполагаемого подписавшегося.

Вариант B

1) В случае, когда:

a) использование [усиленной] электронной подписи являлось несанкционированным;

b) предполагаемый подписавшийся не проявил разумной осмотрительности для избежания несанкционированного использования его подписи и для предотвращения того, чтобы адресат положился на такую подпись; и

c) адресат добросовестно разумно положился на подпись себе в ущерб

[производится] [может быть произведена] атрибуция подписи предполагаемому подписавшемуся для целей распределения ответственности за покрытие расходов по восстановлению положения сторон, существовавшего до несанкционированного использования подписи.

2) Пункт 1 не применяется в той мере, в которой адресату стало известно или должно было стать известно, что использование подписи являлось несанкционированным.

Вариант С

1) В случае, когда [усиленная] электронная подпись проставляется на сообщении данных и:

a) использование [усиленной] электронной подписи являлось несанкционированным;

b) предполагаемый подписавшийся не проявил разумной осмотрительности для избежания несанкционированного использования его подписи; и

c) адресат добросовестно разумно положился на подпись себе в ущерб,

производится атрибуция сообщения данных предполагаемому подписавшемуся, за исключением случаев, когда это [является необоснованным и несправедливым] [будет явно несправедливым] с учетом целей, для которых было использовано сообщение данных, и других соответствующих обстоятельств.

2) [В случае, когда применяются подпункты (a), (b) и (c) пункта 1 и атрибуции сообщения данных предполагаемому подписавшемуся согласно пункту 1 не производится] [В случае, когда атрибуции сообщения данных предполагаемому подписавшемуся согласно пункту 1 не производится на основании явной несправедливости], предполагаемый подписавшийся тем не менее несет ответственность за покрытие расходов по восстановлению положения адресата, существовавшего до использования несанкционированной подписи.

3) Пункт 1 не применяется:

a) в той мере, в которой адресату стало известно или должно было стать известно, если бы он проявил разумную осмотрительность, что данная подпись не является подписью предполагаемого подписавшегося;

b) в случае, когда адресат получил от предполагаемого подписавшегося уведомление о том, что данная подпись не является подписью предполагаемого подписавшегося, и в распоряжении адресата имелось разумное время для принятия соответствующих мер.

4) Атрибуция несанкционированной подписи предполагаемому подписавшемуся согласно пункту 1 будет явно несправедливой, если:

a) это возложит на предполагаемого подписавшегося бремя, не пропорциональное убыткам, понесенным адресатом,

b) [...]

Справочные материалы

A/CN.9/454, пункты 76-88;
A/CN.9/WG.IV/WP.76, пункты 28-30;
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.

Примечания

42. Проект статьи 7 был пересмотрен с тем, чтобы учесть ряд различных вариантов, обсужденных Рабочей группой на ее тридцать третьей сессии (A/CN.9/454, пункты 76-88). И вариант A, и вариант B в их нынешней редакции поднимут вопросы, которые уже охвачены статьей 13 Типового закона, в частности статьей 13(3). Следует, однако, отметить, что статья 13 Типового закона касается атрибуции сообщения данных, в то время как в проекте статьи 7 рассматривается несанкционированное использование подписи.

43. Вопрос об атрибуции в проекте статьи 7 рассматривается несколько по-иному, чем это делается согласно статье 13. Например, согласно статье 13(4)(a) и (b) в тех случаях, когда имеется несанкционированное сообщение по смыслу статьи 13(3)(b), получающая сторона может полагаться на сообщение при условии, что она не получила уведомления об отсутствии санкций, или за исключением случаев, когда ей должно было стать известно о том, что сообщение является несанкционированным. В статье 13 не оговаривается, что предполагаемый подписавшийся может выдвинуть возражение о том, что он принял разумные меры для защиты подписи (например, путем предотвращения доступа к методу, используемому подписавшимся для идентификации сообщения данных в качестве его собственного), а согласно варианту B(1)(b) проекта статьи 7 такая возможность предусматривается. Кроме того, в статье 13 не рассматривается вопрос о полагающейся стороне, действующей добросовестно себе в ущерб; в отличие от этого вариант B(1)(c) проекта статьи 7 единообразных правил четко исходит из ущерба, понесенного адресатом, и идеи реституции.

44. В центре внимания статьи 13 Типового закона и проекта статьи 7 единообразных правил стоят различные вопросы. Статья 13 посвящена атрибуции сообщений, а в проекте статьи 7 устанавливается правило ответственности в связи с атрибуцией подписи. Рабочая группа, возможно, пожелает принять во внимание решение, которое предстоит принять применительно к статье 4 и которое связано с юридической необходимостью в проведении разграничения между атрибуцией сообщения и атрибуцией подписи (см. пункт 32 выше). Возможно, потребуется рассмотреть взаимосвязь между этими двумя проектами статей, с тем чтобы не было недопониманий в вопросе о том, какое из положений следует применять для атрибуции сообщения данных в случае подписанного сообщения данных. Один из путей, позволяющих избежать возможных недоразумений, состоит в принятии специального правила, применимого к случаям, когда сообщение данных подписано [усиленной] электронной подписью. Именно эту цель преследует включение варианта C в проект статьи 7. В проекте пункта 3 варианта C, помимо оснований явной несправедливости, повторяются два предусмотренных статьей 13 случая, когда атрибуция сообщения предполагаемому подписавшемуся не может быть произведена, а в проекте пункта 4 варианта C содержатся определенные указания на то, что можно считать явной несправедливостью. Рабочая группа, возможно, пожелает рассмотреть другие ситуации, которые могут представлять собой явную несправедливость в контексте атрибуции.

Раздел III. Цифровые подписи, подтвержденные сертификатами

Статья 8. Содержание [усиленных] сертификатов

Вариант A

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

a) идентифицируется выдавший его сертификационный орган;

b) именуется или идентифицируется [подписавшийся] [субъект сертификата] либо устройство или электронный агент, находящийся под контролем [подписавшегося] [субъекта сертификата] [этого лица];

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

d) указывается срок действия сертификата;

e) имеется цифровая подпись или же обеспечена иная защита выдавшим его сертификационным органом;

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

[g) идентифицируется алгоритм, подлежащий применению].

Вариант B

1) При раскрытии какой-либо стороне содержащейся в сертификате информации сертификационный орган [или субъект сертификата] обеспечивает включение в такую информацию по меньшей мере сведений, указанных в пункте 2, за исключением случаев, когда сертификационный орган [или, в соответствующих случаях, субъект] и такая сторона прямо договорились об ином.

Вариант X 2) Указанная в пункте 1 информация включает:

a) для всех сертификатов

i) идентификацию выдавшего сертификационного органа;

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

iii) цифровую или иную подпись сертификационного органа, выдавшего сертификат [информацию];

b) для [...] сертификатов

i) срок действия сертификата;

[ii) ограничения, если таковые имеются, применимые в отношении сферы использования публичного ключа;]

[iii) идентификацию алгоритма, подлежащего применению].

Вариант Y 2) Указанная в пункте 1 информация включает:

a) идентификацию сертификационного органа, выдавшего [сертификат] [информацию];

b) наименование или идентификацию [подписавшегося] [субъекта сертификата] или устройства или электронного агента, находящегося под контролем [подписавшегося] [субъекта сертификата] [этого лица];

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

d) цифровая или иная подпись сертификационного органа, выдавшего сертификат [информацию].

3) Сертификаты могут также включать другую информацию, в том числе следующую:

a) срок действия сертификата;

[b) ограничения, если таковые имеются, применимые в отношении сферы использования публичного ключа;]

[c) идентификацию алгоритма, подлежащего применению].

Справочные материалы

A/CN.9/454, пункты 89-116;
A/CN.9/WG.IV/WP.76, пункт 31;
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.

Примечания

45. С учетом быстрого изменения соответствующих технологий и развития новых форм сертификации, не основывающихся на трехсторонней модели (подписавшийся, полагающаяся сторона и сертификационный орган), на тридцать третьей сессии Рабочей группы было высказано сомнение относительно уместности включения в рассматриваемые правила единого положения, касающегося содержания сертификатов (A/CN.9/454, пункты 90-97). Данная пересмотренная редакция проекта статьи 8, которая включает два согласованных Рабочей группой варианта (A/CN.9/454, пункт 116), будет являться основой для дальнейшего обсуждения.

46. В варианте B отражена обеспокоенность тем, что понятие выдачи сертификата может охватывать только физическую выдачу сертификата субъекту сертификата, связанную с договорными отношениями, в отличие от раскрытия содержащейся в сертификате информации любой полагающейся третьей стороне. В варианте B устанавливается обязательство раскрывать определенную содержащуюся в сертификате информацию, однако оно не связывается с каким-либо обязательством включать эту информацию в сертификат в качестве предварительного условия раскрытия. В тех случаях, когда какая-либо информация в сертификат не включена, могут возникнуть проблемы в вопросе о том, существует ли, тем не менее, обязательство раскрывать такую информацию. Рабочая группа, возможно, пожелает изучить вопрос о возможной предпочтительности выработки положения, которое будет устанавливать минимальную информацию, подлежащую включению в сертификат, и отдельного положения, касающегося обязательства раскрывать информацию.

Статья 9. Последствия цифровых подписей, подтвержденных сертификатами

1) В отношении всего сообщения данных или какой-либо его части в случае, когда составитель идентифицирован цифровой подписью, эта цифровая подпись является [усиленной] электронной подписью, если:

Вариант A a) цифровая подпись была создана в течение срока действия действительного сертификата и [надлежащим образом] проверена [в течение срока действия действительного сертификата] с помощью публичного ключа, указанного в сертификате;

b) сертификат имеет целью установление связи между публичным ключом и личностью [подписавшегося] [соответствующего лица] [составителя];

c) сертификат был выдан для целей удостоверения цифровых подписей, которые являются [усиленными] электронными подписями; и

d) сертификат был выдан:

i) 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) сертификационным органом, аккредитованным ответственным аккреди-тационным органом, применяющим коммерчески обоснованные и международно признанные стандарты, относящиеся к вопросам надежности технологии, практики и других соответствующих характеристик функционирования сертификационного органа. Неисчерпывающий перечень органов и стандартов, отвечающих положениям настоящего пункта, может быть опубликован ... [принимающее государство указывает орган или ведомство, компетентное устанавливать признанные стандарты функционирования получивших лицензию сертификационных органов]; или

[iii) в соответствии с коммерчески обоснованными и международно признанными стандартами.]

Вариант B a) цифровая подпись была [надежно] создана в течение срока действия действительного сертификата и [надлежащим образом] проверена [в течение срока действия действительного сертификата] с помощью публичного ключа, указанного в сертификате; и

b) сертификат устанавливает связь между публичным ключом и личностью [соответствующего лица] [составителя] [...] согласно процедурам, установленным:

i) [принимающее государство указывает орган или ведомство, компетентное выдавать лицензии сертификационным органам и принимать правила, регулирующие функционирование получивших лицензию сертификационных органов]; или

ii) ответственным аккредитационным органом, применяющим коммерчески обоснованные и международно признанные стандарты, относящиеся к вопросам надежности технологии, практики и других соответствующих характеристик функционирования сертификационного органа; или

iii) [международными стандартами и коммерческой практикой или обычаями, широко известными и регулярно применяемыми в области, с которой связана сделка].

2) Цифровая подпись, не удовлетворяющая требованиям, изложенным в пункте 1, считается [усиленной] электронной подписью, если:

a) имеются достаточные доказательства того, что:

i) сертификат устанавливает четкую связь между публичным ключом и личностью [субъекта сертификата] [...]; и

ii) цифровая подпись надлежащим образом создана и [в течение срока действия сертификата] проверена с применением надежной защищенной процедуры; или

b) она квалифицируется в качестве [усиленной] электронной подписи согласно другим положениям настоящих Правил.

Справочные материалы

A/CN.9/454, пункты 117-138;
A/CN.9/WG.IV/WP.76, пункты 32-38;
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.

Примечания

47. Редакция проекта статьи 9 была пересмотрена с тем, чтобы отразить принятое Рабочей группой на ее тридцать третьей сессии (A/CN.9/454, пункт 136) решение включить в текст варианты A и B для будущего обсуждения. В проекте статьи 9 устанавливаются условия, которые должны быть соблюдены для того, чтобы цифровая подпись рассматривалась в качестве [усиленной] электронной подписи. [Усиленная] электронная подпись в общем виде определяется в проекте статьи 1(b) в качестве подписи, удовлетворяющей определенным условиям. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, являются ли условия, содержащиеся в проекте статьи 9, дополнительными по отношению к общим условиям определения или же их цель состоит в разъяснении и развитии этих условий. В то же время проект статьи 9(2)(b) в его нынешней редакции устанавливает, что цифровая подпись может рассматриваться в качестве [усиленной] электронной подписи, даже если она не отвечает требованиям проекта статьи 9(1), при условии, что она квалифицируется в качестве [усиленной] электронной подписи согласно другим положениям правил. Это включает соответствующую квалификацию согласно определению в проекте статьи 1. Если проект статьи 9 не будет четко сформулирован в качестве развития условий, оговоренных в проекте статьи 1, то правила будут устанавливать два различных стандарта для определения того, что следует рассматривать в качестве [усиленной] электронной подписи.

48. Рабочая группа, возможно, пожелает рассмотреть проект статьи 9 в контексте проекта статьи 1 при уделении особого внимания технологии цифровых подписей. Этот проект статьи может, например, специально регулировать вопрос о том, как цифровая подпись может удовлетворить требования проекта статьи 1(b)(i)-(iii).

ГЛАВА III. СЕРТИФИКАЦИОННЫЕ ОРГАНЫ И СМЕЖНЫЕ ВОПРОСЫ

Статья 10. Гарантия при выдаче [усиленного] сертификата

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

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

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

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

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

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

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

b) что в момент выдачи [усиленного] сертификата частный ключ:

i) соответствует [подписавшемуся] [субъекту], идентифицированному в [усиленном] сертификате; и

ii) соответствуют публичному ключу, указанному в [усиленном] сертификате".

Справочные материалы

A/CN.9/454, пункты 139-144;
A/CN.9/WG.IV/WP.76, пункт 39;
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.

Примечания

49. Проект статьи 10 отражает решение, принятое Рабочей группой на ее тридцать третьей сессии (A/CN.9/454, пункты 140-144), хотя Рабочая группа согласилась с тем, что эту статью, возможно, потребуется рассмотреть в будущем с учетом проектов статей 11 и 12.

50. Применение пересмотренного проекта статьи 10 ограничено [усиленными] электронными подписями по той причине, что установление обязательного стандарта для всех видов сертификатов может быть нецелесообразным с учетом разнообразных типов сертификатов и видов их использования, которые могут появиться в будущем.

Статья 11. Договорная ответственность

1) В отношениях между сертификационным органом, выдавшим сертификат, и держателем этого сертификата [или какой-либо иной полагающейся стороной, находящейся в договорных отношениях с сертификационным органом] права и обязательства сторон [и их любое ограничение] определяются их соглашением [с учетом положений применимого законодательства].

2) [С учетом положений статьи 10] сертификационный орган может, по соглашению, исключить свою ответственность за любые убытки, понесенные в результате доверия к сертификату. Однако на оговорку, ограничивающую или исключающую ответственность сертификационного органа, нельзя ссылаться в той мере, в которой такое исключение или ограничение договорной ответственности [будет явно несправедливым] [будет по своей сути несправедливым и приведет к очевидной несбалансированности в положении сторон] [неоправданно предоставит одной стороне чрезмерное преимущество] с учетом цели договора и других соответствующих обстоятельств.

Справочные материалы

A/CN.9/454, пункты 145-157;
A/CN.9/WG.IV/WP.76, пункт 40;
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.

Примечания

51. Проект статьи 11 отражает принятое Рабочей группой на ее тридцать третьей сессии решение (A/CN.9/154, пункт 149) сохранить в единообразных правилах статью, аналогичную проекту статьи 11. На этой сессии была высказана обеспокоенность в связи с тем, что термин "явно несправедливый" может и не быть понятным для всех правовых систем (A/CN.9/454, пункт 152). Рабочей группе было напомнено о том, что пункт 2 построен на основе Принципов международных коммерческих контрактов МИУЧП (статья 7.1.6) и представляет собой попытку установить единообразный стандарт для оценки общей приемлемости оговорок об исключении ответственности. Ссылка на "явно несправедливые" ограничения или исключения ответственности предполагает гибкий подход к оговоркам об исключении ответственности и преследует цель содействовать более широкому признанию оговорок об ограничении и исключении ответственности, чем это было бы возможно, если бы в единообразных правилах упоминался лишь закон, применимый за пределами единообразных правил (A/CN.9/WG.IV/WP.73, пункт 64). Для лучшего разъяснения термина "явно несправедливый" были включены дополнительные формулировки в квадратных скобках. Эти формулировки заимствованы из разъяснительных материалов к статье 7.1.6 Принципов МИУЧП.

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

1) С учетом положений пункта 2 в случае, когда сертификационный орган выдает сертификат, он несет ответственность перед любым лицом, разумно полагающимся на этот сертификат, за:

a) ошибки или упущения в сертификате, если только сертификационный орган не докажет, что он или его агенты приняли все разумные меры для избежания ошибок или упущений в сертификате;

b) непринятие мер по регистрации аннулирования сертификата, если только сертификационный орган не докажет, что он или его агенты приняли все разумные меры для регистрации аннулирования сразу же после получения уведомления о его аннулировании; и

c) последствия несоблюдения любой процедуры, указанной в заявлении о практике сертификации, опубликованном сертификационным органом.

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] [в той мере, в которой]:

a) оно оказано с целью, противоречащей цели, для которой выдан сертификат;

b) оно оказано в связи с операцией, стоимостной объем которой превышает стоимость, в отношении которой сертификат является действительным; или

c) [...]].

Справочные материалы

A/CN.9/454, пункты 158-163;
A/CN.9/WG.IV/WP.76, пункт 41;

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.

Примечания

52. На своей тридцать третьей сессии Рабочая группа согласилась с тем, что проекты статей 10, 11 и 12 необходимо совместно рассмотреть на одном из будущих заседаний для обеспечения того, чтобы обязательства, налагаемые на сертификационные органы, соответствовали нормам об ответственности, устанавливаемым единообразными правилами (A/CN.9/454, пункт 159), но что, однако, проект статьи 12 следует сохранить и пересмотреть на предмет внесения ряда редакционных изменений. Эти редакционные изменения были внесены в данный пересмотренный вариант проекта статьи 12.

Общие примечания в отношении проектов статей 13-15

53. Ввиду отсутствия времени Рабочая группа провела лишь предварительное обсуждение проектов статей 13, 14 и 15 (A/CN.9/454, пункты 164-169). Был высказан ряд замечаний по поводу подробности этих проектов статей и технических предпосылок, на которых они основываются. Рабочей группе было предложено, чтобы применение этих проектов статей ограничивалось только цифровыми подписями и чтобы, поскольку они касаются основных обязательств сертификационного органа, вопрос о существе этих обязательств был решен до возможного рассмотрения вопросов об ответственности. Эти проекты статей было решено сохранить в квадратных скобках для будущего рассмотрения.

[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 в применимом заявлении 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] либо агентом [подписавшегося] [субъекта], обладающим полномочиями требовать такого аннулирования;

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

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

2) [Подписавшийся] [субъект] в отношении сертифицированной пары ключей обязан аннулировать соответствующий сертификат или потребовать его аннулирования в случае, когда [подписавшемуся] [субъекту] стало известно, что частный ключ был утерян или скомпрометирован или подвергается опасности неправомерного 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, полагающейся на сообщение, 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].

4) После аннулирования сертификата согласно пункту 3 сертификационный орган должен уведомить [подписавшегося] [субъекта] и полагающиеся стороны в соответствии с политикой и процедурами, регулирующими порядок уведомления об аннулировании и предусмотренными в применимом заявлении о практике сертификации, либо в отсутствие такой политики и процедур, незамедлительно уведомить [подписавшегося] [субъекта] 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 полагающейся стороны.

5) [В отношениях между [подписавшимся] [субъектом] и сертификационным органом] аннулирование вступает в силу с момента его [получения] [регистрации] сертификационным органом.

[6) В отношениях между сертификационным органом и любой другой полагающейся стороной, аннулирование вступает в силу с момента его [регистрации] [опубликования] сертификационным органом]].

[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 в применимом заявлении 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 от лица, уполномоченного действовать от имени такого [подписавшегося] [субъекта]].

[Статья 15. Регистр сертификатов

1) Сертификационные органы ведут общедоступный электронный реестр выданных сертификатов, содержащий указания на то, когда истекает срок действия того или иного сертификата либо когда его действие было приостановлено или он был аннулирован.

2) Записи в реестре хранятся 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 C в соответствии с политикой и процедурами, установленными сертификационным органом в применимом заявлении о практике сертификации.]

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.