



Генеральная Ассамблея

Distr.
LIMITED

A/CN.9/WG.IV/WP.82
29 June 1999

RUSSIAN
Original: ENGLISH

КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ
Рабочая группа по электронной торговле
Тридцать пятая сессия
Вена, 6-17 сентября 1999 года

ПРОЕКТ ЕДИНООБРАЗНЫХ ПРАВИЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

Записка Секретариата

СОДЕРЖАНИЕ

	<u>Пункты</u>	<u>Страница</u>
ВВЕДЕНИЕ	1-12	2
I. ОБЩИЕ ЗАМЕЧАНИЯ	13-20	5
II. ПРОЕКТЫ СТАТЕЙ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ	21-71	6
Статья 1. Сфера применения	21	6
Статья 2. Определения	22-33	7
Статья 3. [Недискриминация] [Технологическая нейтральность]	34	12
Статья 4. Толкование	35	12
Статья 5. Изменение по договоренности	36-40	13
Общие примечания в отношении проектов статей 6-8	41	14
Статья 6. [Соблюдение требований к подписи] [Презумпция подписания]	42-44	14
Статья 7. [Презумпция наличия подлинника]	45	17
Статья 8. Определение [усиленной] электронной подписи	46	17
Общие примечания в отношении проектов статей 9 и 10	47-49	18
Статья 9. [Ответственность] [обязанности] обладателя подписи	50-55	18
Статья 10. Доверие к усиленным электронным подписям		22
Статья 11. Доверие к сертификатам	56-58	23
Статья 12. [Ответственность] [обязанности] сертификатора информации	59-68	25
Статья 13. Признание иностранных сертификатов и подписей	69-71	36

ВВЕДЕНИЕ

1. На своей двадцать девятой сессии (1996 год) Комиссия постановила включить в свою повестку дня вопросы о подписях в цифровой форме и сертификационных органах. Рабочей группе по электронной торговле было предложено рассмотреть целесообразность и возможность подготовки единообразных правил по этим темам. Было достигнуто согласие в отношении того, что единообразные правила, которые следует подготовить, должны охватывать такие вопросы, как: правовая основа, поддерживающая процессы сертификации, включая появляющуюся технологию удостоверения подлинности и сертификации в цифровой форме; применимость процесса сертификации; распределение риска и ответственности пользователей, поставщиков и третьих сторон в контексте использования методов сертификации; конкретные вопросы сертификации через применение регистров; и включение путем ссылки¹.

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"). 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 (далее в тексте - "Типовой закон"). Таким образом, единообразные правила не должны препятствовать использованию других методов удостоверения подлинности. Кроме того, при решении вопросов криптографии публичных ключей в единообразных правилах, возможно, необходимо будет учесть различия в уровнях защиты и признать различные юридические последствия и уровни ответственности, соответствующие различным видам услуг, оказываемых в контексте подписей в цифровой форме. Что касается сертификационных органов, то Комиссия, хотя она и признала ценность стандартов, определяемых рыночными отношениями, в целом согласилась с тем, что Рабочая группа может надлежащим образом предусмотреть разработку минимального свода стандартов, которые должны будут строго соблюдаться сертификационными органами, особенно в случае необходимости трансграничной сертификации².

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

5. На тридцать первой сессии (1998 год) Комиссии был представлен доклад Рабочей группы о работе ее тридцать второй сессии (A/CN.9/446). 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. Комиссия подтвердила принятое на ее тридцатой сессии решение относительно возможности разработки единообразных правил и выразила уверенность в том, что на своей тридцать третьей сессии Рабочая группа сможет добиться дальнейшего прогресса на основе пересмотренного проекта, подготовленного Секретариатом (A/CN.9/WG.IV/WP.76). В контексте этого обсуждения Комиссия с удовлетворением отметила, что по общему признанию Рабочая группа стала особо важным международным форумом для обмена мнениями по правовым вопросам электронной торговли и выработки решений по этим вопросам³.

6. На тридцать второй сессии (1999 год) Комиссии были представлены доклады Рабочей группы о работе ее тридцать третьей (июль 1998 года) и тридцать четвертой (февраль 1999 года) сессий (A/CN.9/454 и 457). Комиссия выразила признательность Рабочей группе за ее усилия по подготовке проекта единообразных правил об электронных подписях. Хотя, по мнению большинства членов Комиссии, на этих сессиях был достигнут значительный прогресс в понимании правовых вопросов, связанных с использованием электронных подписей, было также сочтено, что Рабочая группа столкнулась с рядом трудностей в достижении консенсуса в отношении законодательного принципа, на котором должны основываться единообразные правила.

7. Было также высказано мнение, что подход, применяемый в настоящее время Рабочей группой, недостаточно полно отражает потребность деловых кругов в гибком использовании электронных подписей и других методов удостоверения подлинности. В единообразных правилах, как они рассматриваются в настоящее время Рабочей группой, уделяется чрезмерно большое внимание методам цифровых подписей и - в сфере применения таких подписей - специальной практике сертификации третьей стороной. Соответственно, было предложено либо ограничить работу по вопросам электронных подписей, осуществляемую Рабочей группой, правовыми вопросами трансграничной сертификации, либо отложить ее до тех пор, пока не упрочится соответствующая рыночная практика. В связи с этим было также высказано мнение, что применительно к целям международной торговли большая часть правовых вопросов, возникающих в связи с использованием электронных подписей, уже была решена в Типовом законе ЮНСИТРАЛ об электронной торговле. Хотя некоторые виды использования электронных подписей, возможно, требуют урегулирования за рамками торгового права, Рабочей группе не следует заниматься какими-либо вопросами, связанными с такого рода регулированием.

8. Преобладающее мнение заключалось в том, что Рабочей группе следует выполнять свою задачу, исходя из своего первоначального мандата (см. пункт 3 выше). Что касается необходимости в единообразных правилах об электронных подписях, то, как было разъяснено, правительственные и законодательные органы многих стран, занимающиеся подготовкой законодательства по вопросам электронных подписей, включая создание инфраструктур публичных ключей (ИПК), или другими проектами по тесно связанным с этой областью вопросам (см. A/CN.9/457, пункт 16), ожидают определенных рекомендаций от ЮНСИТРАЛ. Что касается принятого Рабочей группой решения сосредоточить свое внимание на вопросах использования ИПК и терминологии ИПК, то было вновь указано, что комплекс взаимоотношений между тремя отдельными категориями сторон (т.е. обладателями ключей, сертификационными органами и полагающимися сторонами) отвечает одной возможной модели ИПК, но что можно предположить и существование других моделей, например, в тех случаях, когда независимый сертификационный орган не является участником таких отношений. Одно из основных преимуществ, которое можно извлечь из концентрации внимания на вопросах ИПК, состоит в том, что это позволит облегчить составление единообразных правил за счет ссылок на три функции (или роли) применительно к парам ключей, а именно на функцию выдачи ключа (или функцию абонирования), сертификационную функцию и полагающуюся функцию. Было достигнуто общее согласие с тем, что эти три функции являются общими для всех моделей ИПК. Было также принято решение о том, что вопросы, связанные с этими тремя функциями, должны регулироваться независимо от того, выполняют ли их на практике три отдельных субъекта или же одно и то же лицо выполняет две из этих функций (например, в случаях, когда сертификационный орган также является полагающейся стороной). Кроме

того, согласно получившему широкую поддержку мнению, уделение первоочередного внимания функциям, типичным для ИПК, а не какой-либо конкретной модели, может на более позднем этапе облегчить разработку такой нормы, которая являлась бы полностью нейтральной с точки зрения носителя информации (там же, пункт 68).

9. После обсуждения Комиссия вновь подтвердила принятые ею ранее решения относительно возможности подготовки таких единообразных правил (см. пункты 3 и 5 выше) и выразила уверенность, что Рабочая группа сможет добиться дальнейшего прогресса на будущих сессиях.

10. В настоящей записке содержатся пересмотренные проекты положений, подготовленные с учетом обсуждений Рабочей группы, а также обсуждений и решений Комиссии на ее тридцать второй сессии, воспроизведенные выше. Они призваны отразить решения, принятые Рабочей группой на ее тридцать четвертой сессии. Положения в новой редакции подчеркнуты.

11. В соответствии с применимыми инструкциями, касающимися более строго 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.

Справочные национальные законодательные и другие тексты

12. В целях информации и сопоставления в настоящий документ под этим названием применительно к ряду статей включены примеры национальных законодательных и других текстов, выделенные более мелким шрифтом. Примеры национального законодательства включались исходя из тех законодательных актов, которые были известны Секретариату и которые имелись в его распоряжении для справочных целей. Примеры других текстов включались исходя из того, что эти документы были подготовлены международными организациями или являются широко известными и общедоступными. Сокращения указывают на следующие законодательные акты и другие тексты:

- Германия Закон о цифровых подписях 1997 года (статья 3, Закон об информационных и коммуникационных услугах; утвержден 13/6/97; вступил в силу 1/8/97);
- Иллинойс США, Закон о безопасности электронной торговли 1998 года (1997 Illinois House Bill 3180; 5 Ill. Comp. Stat. 175; принят в августе 1998 года);
- Миннесота США, Закон об электронном удостоверении подлинности (Minnesota Statutes §325; принят в мае 1997 года);
- Миссури США, Закон о цифровых подписях 1998 года (1998 SB 680; принят в июле 1998 года);
- Сингапур Закон об электронных сделках 1998 года, Закон № 25 1998 года;
- Р у к о в о д я щ и е п р и н ц и п ы А А А
Американская ассоциация адвокатов, Научно-техническая секция, "Руководящие принципы в отношении цифровых подписей", 1996 год;
- Проект директивы ЕС Проект директивы Европейского парламента и Совета об общих рамках для электронных подписей, 1999 год (7015/99);
- ГУИДЕК Международная торговая палата, "Общая практика для международных торговых операций, заверенных в цифровой форме", 1997 год.

I. ОБЩИЕ ЗАМЕЧАНИЯ

13. 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.

14. 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.

15. 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 предназначены 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 уже существующими договорными нормами и процедурами, подлежащими соблюдению при передаче сообщений с помощью электронных средств).

16. При рассмотрении проектов положений, предлагаемых для включения в единообразные правила, Рабочая группа, возможно, пожелает рассмотреть в более общем плане взаимосвязь между единообразными правилами и Типовым законом. Настоящий проект единообразных правил был подготовлен исходя из той предпосылки, что они будут приняты в качестве отдельного документа. Дополнительно включены две новые статьи, отражающие положения, которые содержатся в Типовом законе: статья 1 (Сфера применения) и статья 4 (Толкование). Сделки с участием потребителей прямо из сферы применения единообразных правил не исключаются, однако в текст проекта статьи 1 была включена сноска из Типового закона с тем, чтобы разъяснить, что единообразные правила не преследуют цели установить преимущественный порядок по отношению к любым положениям национального права, касающимся вопросов защиты потребителей.

17. Рабочая группа, возможно, пожелает 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.

18. На тридцать третьей сессии Рабочей группы были выражены 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". На тридцать четвертой сессии (A/CN.9/457, пункт 39) было высказано мнение о том, что определение "усиленной электронной подписи", возможно, потребует еще раз рассмотреть вместе с вопросом об общей структуре единообразных правил после того, как будет разъяснена цель создания соответствующих режимов для двух категорий электронных подписей, особенно в том, что касается юридических последствий обоих видов электронных подписей. Было высказано предположение о том, что рассмотрение усиленных электронных подписей будет оправданным только

в том случае, если единообразные правила будут устанавливать функциональный эквивалент конкретным видам использования собственноручных подписей. Поскольку эта задача может быть особенно трудной на международном уровне и к тому же будет иметь лишь ограниченное значение для международных коммерческих сделок, те дополнительные выгоды, которые можно ожидать от использования не просто "электронной подписи", а "усиленной электронной подписи", потребуется, возможно более подробно разъяснить.

19. С учетом этого проведенного обсуждения вопроса о необходимости в категории "усиленных электронных подписей" в настоящем пересмотренном проекте единообразных правил использован альтернативный подход, предлагаемый на рассмотрение Рабочей группы. Определение "усиленной электронной подписи" в проекте статьи 2(b) было заключено в квадратные скобки. Примечания, касающиеся возможных изменений этого определения, приведены в связи со статьей 2. В проекты статей 6, 7 и 8 включены соответствующие части этого определения в качестве альтернативных материально-правовых положений. Цель такого альтернативного подхода состоит в том, чтобы оказать содействие Рабочей группе в принятии решения о том, следует ли исключить ссылки как на электронные, так и на усиленные электронные подписи, с тем чтобы в единообразных правилах регулировалась только единая категория электронных подписей. Примечания, касающиеся конкретных предложений, приводятся в разделах, посвященных соответствующим статьям.

20. В соответствии с настоящим пересмотренным проектом единообразных правил их применение расширяется за пределы ситуации, когда существуют юридические требования к форме или когда законодательство предусматривает наступление соответствующих последствий при несоблюдении некоторых условий, таких, как наличие подписи или подлинника. Сфера действия единообразных правил потенциально является, таким образом, более широкой, чем сфера действия Типового закона, хотя в проект статьи 6 и включено требование к форме, содержащееся в статье 7 Типового закона. Рабочая группа, возможно, пожелает рассмотреть вопрос о такой более широкой сфере применения единообразных правил.

II. ПРОЕКТЫ СТАТЕЙ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

Статья 1. Сфера применения

Настоящие Правила применяются к электронным подписям, используемым в контексте торговых* отношений, и они не имеют преимущественной силы по отношению к любым правовым нормам, предназначенным для защиты потребителей.

*Термин "торговые" следует толковать широко, с тем чтобы он охватывал вопросы, вытекающие из всех отношений торгового характера, как договорных, так и недоговорных. Отношения торгового характера включают следующие сделки, не ограничиваясь ими: любые торговые сделки на поставку товаров или услуг или обмен товарами или услугами; дистрибьюторские соглашения; коммерческое представительство и агентские отношения; факторинг; лизинг; строительство промышленных объектов; предоставление консультативных услуг; инжиниринг; купля/продажа лицензий; инвестирование; финансирование; банковских услуги; страхование; соглашения об эксплуатации или концессии; совместные предприятия и другие формы промышленного или предпринимательского сотрудничества; перевозка товаров и пассажиров воздушным, морским, железнодорожным или автомобильным транспортом.

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 53-64

Примечания

21. Проект статьи 1 был первоначально предложен на тридцать четвертой сессии Рабочей группы в качестве пункта 1 статьи, регулирующей вопросы автономии сторон (проект статьи E, A/CN.9/457, пункты 55, 60). Поскольку это положение - если рассматривать его более корректно - затрагивает вопросы сферы действия единообразных правил, в настоящем проекте оно было включено в отдельную статью под названием "Сфера применения". Как это было решено Рабочей группой (A/CN.9/457, пункт 64), в проект статьи 1 включена сноска, в которой повторяется определение термина "торговый", содержащееся в статье 1 Типового закона об электронной торговле, а в текст этого проекта включена формулировка сноски** Типового закона, касающейся вопроса о потребителях. Слова "электронные подписи, используемые в контексте", были добавлены в эту статью для более точного определения предмета регулирования единообразных правил.

Статья 2. Определения

Для целей настоящих Правил:

а) "электронная подпись" означает [данные в электронной форме, которые содержатся в сообщении данных, приложены к нему или логически ассоциируются с ним и которые могут быть использованы] [любой способ, который может быть использован в отношении сообщения данных] для идентификации обладателя подписи в связи с сообщением данных и указания на то, что обладатель подписи согласен с информацией, содержащейся в сообщении данных;

[b) "усиленная электронная подпись" означает электронную подпись, в отношении которой может быть продемонстрировано с помощью использования [какой-либо процедуры защиты] [какого-либо метода], что эта подпись:

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

ii) была создана и приложена к сообщению данных обладателем подписи или с использованием средства, находящегося под исключительным контролем обладателя подписи [, а не каким-либо другим лицом];

[iii) была создана и связана с сообщением данных, к которому она относится, таким образом, который обеспечивает надежные доказательства целостности сообщения";]

с) "сертификат" означает сообщение данных или иную запись, которые выдаются сертифицированным информацией и которые предназначены для удостоверения личности лица или организации, являющихся обладателями [определенной пары ключей] [определенного подписывающего устройства];

d) "сообщение данных" означает информацию, подготовленную, отправленную, полученную или хранимую с помощью электронных, оптических или аналогичных средств, включая электронный обмен данными (ЭДИ), электронную почту, телеграмму, телекс или телефакс, но не ограничиваясь ими;

e) "обладатель подписи" [обладатель устройства] [обладатель ключа] [абонент] [обладатель подписывающего устройства] [подписавшийся] [подписавший] означает лицо, которым или от имени которого усиленная электронная подпись может быть создана и приложена к сообщению данных;

f) "сертификатор информации" означает лицо или организацию, которые в рамках своей деятельности занимаются [предоставлением идентификационных услуг, которые используются]

[сертификацией информации, которая используется] для поддержки использования [усиленных] электронных подписей.

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 22-47, 66-67, 89, 109;
A/CN.9/WG.IV/WP.80, пункты 7-10;
A/CN.9/WG.IV/WP.79, пункт 21;
A/CN.9/454, 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 А, В и С); и
A/CN.9/WG.IV/WP.71, пункты 52-60.

Примечания

Определение "электронной подписи"

22. Определение электронной подписи было пересмотрено в соответствии с решением, принятым Рабочей группой на ее тридцать четвертой сессии (A/CN.9/457, пункты 23-32). Слова в квадратных скобках "[любой способ, который может быть использован в отношении сообщения о данных]" включены для приведения формулировки определения в единообразных правилах в соответствие с формулировками статьи 7 Типового закона.

Определение "усиленной электронной подписи"

23. В соответствии с решением, принятым Рабочей группой на ее тридцать четвертой сессии (A/CN.9/457, пункт 39), определение "усиленной электронной подписи" было пересмотрено: в него в квадратных скобках в качестве необходимой привязки электронной подписи на сообщении данных к информации, содержащейся в сообщении данных, была включена формулировка подпункта (b)(iii), в которой содержится ссылка на функцию целостности. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли понятие целостности включить в качестве составной части определения усиленной электронной подписи или же это понятие, взятое в качестве концепции, более тесно связано с понятием подлинника, как оно рассматривается в статье 8 Типового закона и проекте статьи 7 единообразных правил. Ранее содержавшаяся в подпункте (ii) формулировка "может использоваться для объективной идентификации обладателя подписи в связи с сообщением данных" была исключена из пересмотренного текста на том основании, что она уже является частью определения "электронной подписи" в подпункте (a).

24. Во вступительную формулировку подпункта (b) в качестве альтернативы применению "процедуры защиты" была включена ссылка на применение "способа" с тем, чтобы обеспечить более тесное соответствие с терминологией, используемой в Типовом законе.

25. В подпункте (b)(ii) слова "а не каким-либо другим лицом" были помещены в квадратные скобки, поскольку их включение ставит ряд вопросов. Во-первых, включение этих слов в определение усиленной электронной подписи может послужить основанием для предположения о том, что подпись, которая не создана и не приложена обладателем подписи (и, таким образом, потенциально является несанкционированной), не представляет собой усиленной электронной подписи. В результате такого толкования подобные подписи могут быть исключены из сферы действия некоторых статей единообразных правил, включая, например, проекты статей 8, 9 и 10. В частности, могут возникнуть сомнения относительно применимости тех частей проекта статьи 9, которые касаются ответственности за компрометацию подписывающих устройств.

26. Во-вторых, включение этих слов будет равнозначно установлению требования о том, что для того, чтобы какая-либо процедура защиты или какой-либо способ считались усиленной электронной подписью, эта процедура или способ должны создавать возможность продемонстрировать, что подпись была действительно создана и приложена владельцем подписи. Поскольку некоторые технологии могут не предусматривать такой возможности, включение такого требования может предполагать необходимость в использовании - в сочетании с применением подписывающего устройства - какого-либо метода идентификации личности, например, использования биометрики или какого-либо другого аналогичного метода.

27. Еще одним вопросом, который Рабочая группа, возможно, пожелает рассмотреть в контексте подпункта (b)(ii), является взаимосвязь между требованием "исключительного контроля" и пунктом 2 проекта статьи 9, в котором предусматривается совместный контроль. Этот вопрос также возникает в связи с определением "владельца подписи", которое рассматривается ниже.

28. В подпункте (b)(iii) слова "разумные доказательства" были заменены на "надежные доказательства" с тем, чтобы обеспечить соответствие с терминологией статьи 8 Типового закона.

Определение "сертификата"

29. Определение термина "сертификат" было включено в единообразные правила по причине необходимости обеспечения их как можно более полного характера. Это определение основывается на определении термина "сертификат личности", содержащемся в документе A/CN.9/WG.IV/WP.79, хотя в настоящем проекте единообразных правил описательная формулировка "сертификат личности" более не используется. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, могут ли быть исключены слова "или другой существенной характеристики", которые в документе A/CN.9/WG.IV/WP.79 заключены в квадратные скобки. Причина этого предложения заключается в следующем: концепция "личности" может представлять собой более объемное понятие, чем просто ссылку на имя владельца подписи и может охватывать также и другие существенные характеристики, такие как занимаемая должность или выполняемые функции, как в сочетании с указанием имени, так и без ссылки на него. Исходя из этого, в проведении различия между личностью и другими существенными характеристиками или в ограничении применимости единообразных правил только теми ситуациями, когда используются только сертификаты личности, указывающие имя владельца подписи, возможно, не имеется. Альтернативную точку зрения назначения понятия "личность" см. "Background Paper on Electronic Authentication Technologies and Issues", Joint OECD-Private Sector Workshop on Electronic Authentication, California. 2-4 June 1999, pp.6-9.

30. Рабочая группа, возможно, пожелает рассмотреть вопрос об уместности использования слов "подтверждение личности", поскольку сертификат в действительности может не подтверждать личность владельца подписи, а идентифицировать владельца подписи в результате применения ряда процедур и удостоверить наличие связи между этой личностью и подписывающим устройством или публичным ключом, указанным в сертификате. Для обеспечения нейтральности единообразных правил с технологической точки зрения Рабочая группа, возможно, также пожелает рассмотреть вопрос об использовании такой, например, технологически нейтральной формулировки, как "подписывающее устройство", в качестве альтернативы словам "пара ключей", поскольку слова "пара ключей" непосредственно связаны с цифровыми подписями. Использование словосочетания "пара ключей" в связи с определением "сертификата" может быть уместно в тех ситуациях, когда сертификаты используются только в контексте цифровых подписей.

Определение "сообщения данных"

31. Определение "сообщения данных" было включено в проект единообразных правил по причине необходимости в обеспечении их как можно более полного характера. Рабочая группа, возможно, пожелает рассмотреть вопрос о необходимости включения этого определения в контексте взаимосвязи единообразных правил и Типового закона.

Определение "обладателя подписи"

32. На своей тридцать четвертой сессии Рабочая группа не завершила обсуждения определения термина "обладатель подписи" (A/CN.9/457, пункт 47). Пересмотренный текст этого определения в настоящее время включает в квадратных скобках ряд терминов, которые, как это было сочтено Рабочей группой, будут, возможно, более уместными, чем словосочетание "обладатель подписи". Это определение, возможно, потребуется пересмотреть в контексте подпункта (b)(ii) определения "усиленной электронной подписи", приведенного выше, и проекта статьи 9(2), как на это указывается в пункте 27.

Определение "сертификатора информации"

33. Это определение Рабочей группой на ее предыдущей сессии не рассматривалось и приведено без изменений. Однако с учетом предыдущих обсуждений (A/CN.9/457, пункт 109) Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли толковать слова "в рамках своей деятельности", содержащиеся в определении "сертификатора информации", как подразумевающие, что деятельность, связанная с сертификацией, должна быть единственным видом деловых операций сертификатора информации или же - с тем чтобы охватить такие ситуации, при которых, например, сертификаты будут выдаваться компаниями, занимающимися расчетами по кредитным картам - следует также охватить и вопрос о сертификатах в качестве второстепенной части деятельности.

Справочные национальные законодательные и другие тексты

Руководящие принципы ААА

Часть 1: Определения

1.5 Сертификат

Сообщение, которое, по меньшей мере,

- 1) идентифицирует выдавший его сертификационный орган,
- 2) именует или идентифицирует абонента,
- 3) содержит публичный ключ абонента,
- 4) указывает срок действия, и
- 5) в цифровой форме подписано выдавшим его сертификационным органом.

1.6 Сертификационный орган

Лицо, которое выдает сертификат.

1.27 Полагающаяся сторона

Лицо, которое получило сертификат и цифровую подпись, которая может быть проверена при использовании публичного ключа, указанного в сертификате, и которое в состоянии положиться на них.

1.30 Подписавшийся

Лицо, которое создает цифровую подпись для сообщения.

1.31 Абонент

Лицо, которое

- 1) поименовано и идентифицировано в сертификате, выданном такому лицу, и
- 2) обладает частным ключом, соответствующим публичному ключу, указанному в этом сертификате.

Проект директивы ЕС

Статья 2

Определения

Для целей настоящей Директивы:

1. "электронная подпись" означает данные в электронной форме, которые приложены к другим электронным данным или логически ассоциируются с ним и которые служат способом удостоверения подлинности;
 - 1а. "продвинутая электронная подпись" означает электронную подпись, которая отвечает следующим требованиям:
 - a) она обладает уникальной связью с подписавшим;
 - b) она может идентифицировать подписавшего;
 - c) она создана при использовании средствами, над которыми подписавший может поддерживать свой исключительный контроль; и
 - d) она связана с данными, к которым она относится, таким образом, что любое последующее изменение в данных могло бы быть выявлено;
2. "подписавший" означает лицо, которое обладает устройством для создания подписи и действует от своего собственного имени или от имени лица или организации, которых оно представляет;
3. "данные для создания подписи" означает уникальные данные, такие, как коды или частные криптографические ключи, которые используются подписавшим при создании электронной подписи;
 - 3а. "устройство для создания подписи" означает конфигурированное программное или аппаратное обеспечение для подготовки данных для создания подписи;
 - 3б. "защищенное устройство для создания подписи" означает устройство для создания подписи, которое отвечает требованиям, изложенным в приложении III;

4. "данные для проверки подписи" означает данные, такие, как коды или публичные криптографические ключи, которые используются при проверке электронной подписи;
- 4a. "устройство для проверки подписи" означает конфигурированное программное или аппаратное обеспечение для подготовки данных для проверки подписи;
- 4b. "сертификат" означает электронную аттестацию, которая позволяет установить связь между данными для проверки подписи и каким-либо лицом и которая подтверждает личность этого лица;
5. [...];
6. "поставщик сертификационных услуг" означает лицо или организацию, которые выдают сертификаты или предоставляют другие услуги, связанные с электронными подписями.

Германия

§ 2 Определения

- 1) Цифровая подпись по смыслу настоящего закона представляет собой знак на цифровых данных, который создан с помощью частного подписывающего ключа и который позволяет при помощи использования соответствующего публичного ключа, к которому приложен сертификат подписывающего ключа, выданный сертификатом или органом согласно § 3, установить владельца ключа подписи и нефальсифицированный характер данных.
- 2) Сертификатором по смыслу настоящего закона является физическое или юридическое лицо, которое аттестует атрибуцию публичных подписывающих ключей физическим лицам и обладает лицензией на такую деятельность согласно § 4.
- 3) Сертификат по смыслу настоящего закона является цифровой аттестацией, которая касается атрибуции публичного подписывающего ключа физическому лицу и к которой приложена цифровая подпись (сертификат подписывающего ключа), или специальной цифровой аттестацией, которая безошибочно указывает на сертификат подписывающего ключа и содержит дальнейшую информацию (сертификат атрибуции).

ГИУДЕК

VI. Глоссарий терминов

2. Сертификат

Заверенное каким-либо лицом сообщение, которое аттестует точность фактов, имеющих существенное значение для юридической действительности акта какого-либо иного лица.

4. Сертификатор

Лицо, которое выдает сертификат и тем самым аттестует точность факта, имеющего существенное значение для юридической действительности акта какого-либо иного лица.

12. Сертификат публичного ключа

Сертификат, в котором указывается публичный ключ, присвоенный абоненту и соответствующий частному ключу, которым обладает этот абонент.

14. Абонент

Лицо, указанное в сертификате.

Иллинойс

5. Электронные записи и подписи в целом

Раздел 5-105. Определения

"Сертификат" означает запись, в которой, как минимум: а) идентифицируется выдавший его сертификационный орган; б) именуется или иным образом идентифицируется абонент, или устройство, или электронный агент под контролем абонента; с) содержится публичный ключ, соответствующий частному ключу, находящемуся под контролем абонента; d) указывается срок действия; и е) имеется цифровая подпись выдавшего его сертификационного органа.

"Сертификационный орган" означает лицо, которое разрешает и обеспечивает выдачу сертификата.

"Электронная подпись" означает подпись в электронной форме, приложенную к электронной записи или логически ассоциируемую с ней.

"Подписывающее устройство" означает уникальную информацию, такую, как коды, алгоритмы, буквы, цифры, частные ключи или личные идентификационные номера (PIN), или материальные устройства с уникальной конфигурацией, которые необходимы - отдельно или в сочетании с другой информацией или устройствами - для создания электронной подписи, атрибуруемой какому-либо конкретному лицу.

Сингапур

Часть 1. Раздел 2. Толкование

"Сертификат" означает выданную для цели поддержки цифровых подписей запись, которая предназначена для подтверждения личности или других существенных характеристик лица, обладающего соответствующей парой ключей;

"сертификационный орган" означает лицо или организацию, которые выдают сертификат;

"электронная подпись" означает любые буквы, знаки, цифры или другие символы в цифровой форме, которые приложены к электронной записи или логически ассоциируются с ней и которые были созданы или приняты с целью удостоверения подлинности электронной записи или выражения согласия с ней;

"пара ключей" - в асимметричной криптосистеме - означает частный ключ и математически связанный с ним публичный ключ, которые обладают свойством, позволяющим с помощью публичного ключа проверить цифровую подпись, созданную с помощью частного ключа;

"частный ключ" означает тот ключ из пары ключей, который используется для создания цифровой подписи;

"публичный ключ" означает тот ключ из пары ключей, который используется для проверки цифровой подписи;

"абонент" означает лицо, которое поименовано или идентифицировано в выданном ему сертификате и которое обладает частным ключом, соответствующим публичному ключу, указанному в этом сертификате.

Статья 3. [Недискриминация] [Технологическая нейтральность]

[Ни одно из положений настоящих Правил не применяется] [Положения настоящих Правил не применяются] таким образом, чтобы исключать, ограничивать или лишать юридической силы любой способ [подписания], который отвечает требованиям [статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле].

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 53-64.

Примечания

34. Проект статьи 2 был первоначально предложен на тридцать четвертой сессии Рабочей группы в качестве пункта 3 статьи, касающейся автономии сторон (проект статьи E, A/CN.9/457, пункты 55, 60). Поскольку пункт 3 в первую очередь касался вопросов недискриминации и технологической нейтральности, а не автономии сторон, он был включен в настоящий проект в качестве отдельной статьи под альтернативными названиями "Недискриминация" или "Технологическая нейтральность". Первоначальная формулировка "исключать, ограничивать или устанавливать дискриминационный режим в отношении" была заменена формулировкой "исключать, ограничивать или лишать юридической силы", с тем чтобы более точно описать цель и предмет этого положения. Ссылка на статью 7 Типового закона об электронной торговле будет представлять собой ссылку на этот Типовой закон, как он принят в национальном законодательстве.

Статья 4. Толкование

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

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

Примечания

35. В проекте статьи 4 воспроизводится статья 3 Типового закона об электронной торговле за исключением добавления слов "в электронной торговле", которое было произведено для обеспечения полноты изложения. Рабочая группа, возможно, пожелает рассмотреть вопрос о целесообразности составления окончательного текста единообразных правил в качестве документа, не являющегося частью Типового закона, хотя и сохраняющего с ним очевидную связь. Если Рабочая группа примет такое решение, то в статью 4 могут быть включены руководящие положения для толкования единообразных правил судами или другими национальными или местными органами. Применение статьи 4, как ожидается, будет способствовать тому, чтобы унифицированный текст после его включения в местное законодательство толковался со ссылками на его международный характер и происхождение, а не только со ссылками на концепции местного права.

Статья 5. Изменение по договоренности

Вариант А

[Стороны по договоренности - будь то прямой или подразумеваемой - свободны отходить от настоящих Правил или изменять любые их аспекты.] [Допускается отход от любых аспектов настоящих Правил или их изменение на основании договоренности - будь то прямой или подразумеваемой, -] кроме как в той степени, в которой такой отход или изменение окажут неблагоприятное воздействие на права третьих сторон.

Вариант В

- 1) Настоящие Правила не затрагивают каких-либо прав, которые могут существовать в отношении изменения по договоренности любой нормы права, упомянутой в статьях 6 и 7.
- 2) Допускается отход от любых аспектов статей 9-12 настоящих Правил или их изменение по договоренности - будь то прямой или подразумеваемой, - кроме как в той степени, в которой такой отход или изменение окажут неблагоприятное воздействие на права третьих сторон.

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 53-64.

Примечания

36. В варианте А проекта статьи 5 отражено принятое Рабочей группой на ее тридцать четвертой сессии решение о том, чтобы включить для цели будущего обсуждения положение, обеспечивающее свободу сторон договариваться в отношениях между собой о возможности отхода от положений правил или их изменения только для целей сделок между договаривающимися сторонами. Такая договоренность не может, однако, затрагивать права сторон, не являющихся ее сторонами, т.е. третьих сторон. Это положение об автономии относится только к рассматриваемым правилам и не преследует цели затронуть публичный порядок или императивные положения законодательства, применимые к контрактам, такие как положения, касающиеся несправедливых контрактов.

37. В варианте В признается, что положения проектов статей 6 и 7 единообразных правил, которые основываются на статьях 7 и 8 Типового закона, содержат ссылки на законодательные требования, которые могут являться императивными требованиями национального законодательства и не подлежат изменению по договоренности. Согласно пункту 1 допускается изменение по договоренности в тех случаях, когда подобные императивные требования национального законодательства могут быть изменены

таким образом. В его нынешнем виде этот пункт воспроизводит формулировку статьи 4(2) Типового закона, в которой регулируется этот же вопрос.

38. В соответствии с пунктом 2 варианта В сохраняется полная автономия сторон в отношении проектов статей 9-12. Это положение составлено на том основании, что проекты статей 9-12 будут представлять собой материально-правовые нормы, которые будут применяться в отсутствие договоренности об отходе от них или об изменении их применения в отношениях между договаривающимися сторонами. Стороны будут свободны изменять эти положения или исключать их применение. Цель пункта 2 состоит в обеспечении того, чтобы любая такая договоренность не наносила ущерба третьим сторонам, однако он не предназначен для того, чтобы лишать юридической силы какую-либо часть договоренности между сторонами.

39. Положения, касающиеся трансграничного признания, не будут подлежать изменению на основании договоренности, кроме как если это конкретно предусматривается такими положениями.

40. Рабочая группа, возможно, пожелает рассмотреть формулировку проекта статьи 5 и поднимаемые ею вопросы в отношении удовлетворения законодательных требований, которые упоминаются в проектах статей 6 и 7 и которые будут, возможно, носить императивный характер. Рабочая группа также, возможно, пожелает рассмотреть вопрос о порядке применения принципа автономии сторон к проектам статей 9-12. В соответствующем положении могут быть, например, установлены субсидиарные нормы, которые будут применяться в отсутствие заключенного между договаривающимися сторонами соглашения о противном ("договоренность об исключении действия"), или могут устанавливаться правила, о применении которых стороны могут договориться ("договоренность о применении").

Общие примечания в отношении проектов статей 6-8

41. В контексте обсуждения сферы действия единообразных правил на своей тридцать четвертой сессии (A/CN.9/457, пункты 48-52) Рабочая группа постановила сконцентрировать внимание на разработке правил для тех технологий, которые в настоящее время используются в коммерческих операциях, например для цифровых методов, применяемых в рамках инфраструктуры публичных ключей (ИПК). Соответственно, было принято решение о том, что Рабочей группе следует сконцентрировать обсуждения на проектах статей F-H (в данном проекте - статьи 9-12) в контексте ИПК. Обсуждение проектов статей A-D (в данном проекте - статьи 2, 6, 7 и 8) было отложено до завершения обсуждения статей F-H. Было указано, что, в частности, проект статьи В (в данном пересмотренном варианте - статья 6 "Соблюдение требований к подписи") может выполнять важную функцию в том, что касается определения сферы применения статей F-H. Кроме того, было высказано мнение о том, что статья Е (в данном проекте - статья 5 "Изменение по договоренности"), которая касается принципа автономии сторон, будет иметь важное значение для рассмотрения любых обязательств сторон в статьях F-H.

Статья 6. [Соблюдение требований к подписи] [Презумпция подписания]

Вариант А

1) В тех случаях, когда в связи с сообщением данных используется усиленная электронная подпись, сообщение данных считается подписанным.

2) В тех случаях, когда законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если использованная электронная подпись, которая является как надежной, так и соответствующей цели, для которой сообщение данных было подготовлено или передано с учетом всех обстоятельств, включая любые соответствующие договоренности.

- [3) В тех случаях, когда законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если использована усиленная электронная подпись.]
- 4) Пункты 2 и 3 применяются как в случаях, когда упомянутое в них требование выражено в форме обязательства, так и в случаях, когда законодательство просто предусматривает наступление определенных последствий, если подпись отсутствует.
- 5) Положения настоящей статьи не применяются в следующих случаях: [...].

Вариант В

1) В тех случаях, когда в связи с сообщением данных, [использован какой-либо способ, который] [использована какая-либо электронная подпись, которая]:

- а) [присущ] [присуща] исключительно владельцу подписи [для цели, с которой] [в контексте, в котором] [он] [она] используется;
- [b) может использоваться для объективной идентификации владельца подписи в связи с сообщением данных; и]
- с) [был создан и приложен] [была создана и приложена] к сообщению данных владельцем подписи или с использованием средства, находящегося под исключительным контролем владельца подписи [, а не каким-либо другим лицом];

считается, что сообщение данных подписано.

- 2) В тех случаях, когда законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если использована электронная подпись, которая является как надежной, так и соответствующей цели, для которой сообщение данных было подготовлено или передано с учетом всех обстоятельств, включая любые соответствующие договоренности.
- 3) Пункт 2 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.
- 4) Положения настоящей статьи не применяются в следующих случаях: [...].

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 48-52;
A/CN.9/WG.IV/WP.80, пункты 11-12.

Примечания

Вариант А

42. Согласно варианту А устанавливается, что в случаях, когда в связи с сообщением данных использована усиленная электронная подпись, сообщение данных может считаться подписанным. В пункте 2 воспроизводится принцип статьи 7 Типового закона, состоящий в том, что электронная подпись может выполнить требования законодательства о наличии подписи при условии, что она отвечает определенным критериям надежности. Рабочая группа, возможно, обратит внимание на тот факт, что факторы, которые могут учитываться при определении надлежащего уровня надежности, перечисляются в пункте 58 Руководства по принятию Типового закона. Пункт 3, в котором предусматривается, что

усиленная электронная подпись отвечает таким условиям, и в котором содержится сжатое правило, позволяющее обеспечить выполнение требований статьи 7 Типового закона, был включен в настоящий проект в квадратных скобках. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, сохраняется ли необходимость в этом положении с учетом пункта 1.

Вариант В

43. Цель варианта В состоит в установлении презумпции подписания и выполнения каких-либо законодательных требований в отношении наличия подписи в контексте единой категории электронных подписей. Соответственно понятие "усиленной электронной подписи" в нем не упоминается. В пункте 1 варианта В устанавливается, что в случаях, когда в связи с сообщением данных использован какой-либо способ и когда такой способ удовлетворяет ряду требований, сообщение данных может считаться подписанным. Такой способ должен удовлетворять условиям, установленным в определении "усиленной электронной подписи" в проекте статьи 2(b), за исключением ссылки на целостность, содержащейся в подпункте (b)(iii). Пункт 1(b) приводится в квадратных скобках, поскольку он потребуется только в том случае, если во вступительной формулировке пункта 1 будет говориться "о способе", а не об "электронной подписи".

44. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли ограничить применение рассматриваемых правил теми ситуациями, когда существуют юридические требования к форме или когда законодательство предусматривает наступление определенных последствий, 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 требования в отношении формы уже рассматривался. В пункте 68 Руководства по принятию Типового закона отмечается, что слово "законодательство" ("the law"), используемое 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.

Справочные национальные законодательные и другие тексты

Сингапур

Часть V. Защищенные электронные записи и подписи

Защищенные электронные подписи

17. Если в результате применения предписанной процедуры защиты или коммерчески обоснованной процедуры защиты, согласованной соответствующими сторонами, может быть проверено, что электронная подпись в момент, когда она была сделана

- a) была присуща исключительно использующему ее лицу;
- b) создавала возможность для идентификации такого лица;
- c) была создана таким образом или при использовании таких средств, которые находились под исключительным контролем использующего ее лица; и
- d) была связана с электронной записью, к которой она относится, таким образом, что при изменении этой записи электронная подпись была бы скомпрометирована,

такая подпись рассматривается в качестве защищенной электронной подписи.

Презумпции, касающиеся защищенных электронных записей и подписей

18. [...]

2) При любых процедурах, связанных с защищенными электронными подписями, если не предоставлены доказательства противного, считается, что

- a) защищенная электронная подпись является подписью лица, к которому она имеет отношение; и
- b) защищенная электронная подпись была приложена этим лицом с намерением подписать электронную запись или выразить согласие с ней.

Статья 7. [Презумпция наличия подлинника]

1) В тех случаях, когда в связи с сообщением данных [использована усиленная электронная подпись] [[использована электронная подпись, которая] [использован способ, который] обеспечивает надежные доказательства целостности информации с момента, когда она была впервые подготовлена в ее окончательной форме в виде сообщения данных или в каком-либо ином виде], считается, что сообщение данных является подлинником.

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

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 48-52;

A/CN.9/WG.IV/WP.80, пункты 13-14.

Примечания

45. Цель проекта статьи 7 состоит в подтверждении связи со статьей 8 Типового закона и в установлении требования целостности. В пункте 1 содержатся две альтернативы. Согласно первой из них предусматривается, что использование усиленной электронной подписи, как она определена в проекте статьи 2(b), будет создавать презумпцию того, что сообщение данных является подлинником. Согласно второму альтернативному варианту в тех случаях, когда использованы какая-либо электронная подпись или какой-либо способ, которые обеспечивают надежные доказательства целостности, сообщение данных может быть сочтено подлинником. Хотя подлинная форма не всегда требует наличия подписи, применение электронной подписи в той или иной форме, будь то усиленной или нет, может быть использовано для проверки целостности сообщения данных или записи.

Статья 8. Определение [усиленной] электронной подписи

1) [Орган или ведомство, указанное принимающим государством в качестве компетентного] может определить, [что электронная подпись является усиленной электронной подписью] [[какие] [методы] [электронные подписи]] удовлетворяют требованиям статей 6 и 7].

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

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 48-52;

A/CN.9/WG.IV/WP.80, пункт 15.

Примечания

46. Цель проекта статьи 8 состоит в том, чтобы четко установить, что принимающее государство может назначить орган или ведомство, которые будут обладать полномочиями, выносить определения относительно того, какие конкретные технологии могут отвечать квалификационным требованиям к усиленной электронной подписи. Альтернативная формулировка включена в пункт 1 с тем, чтобы привести проект статьи 8 в соответствие с альтернативными вариантами, содержащимися в пересмотренных статьях 6 и 7. Цель пункта 2 состоит в том, чтобы побудить государства к обеспечению того, чтобы определения, выносимые в силу пункта 1, отвечали применимым международным стандартам, что будет способствовать унификации практики в отношении усиленных электронных подписей и трансграничному использованию и признанию подписей.

Статья 9. [Ответственность] [обязанности] обладателя подписи

1) Обладатель подписи [обязан]:

а) [проявлять] [проявляет] надлежащую осмотрительность для обеспечения точности и полноты всех сделанных обладателем подписи материальных заверений, которые имеют отношение к выдаче, приостановлению действия или аннулированию сертификата или которые включены в сертификат;

б) [уведомлять] [уведомляет] соответствующих лиц без ненадлежащих задержек в случае, когда [ему известно, что его подпись была скомпрометирована] [его подпись была или могла быть скомпрометирована];

с) [проявлять] [проявляет] надлежащую заботливость для сохранения контроля и недопущения несанкционированного использования его подписи по состоянию с момента, когда обладатель подписи получает исключительный контроль над подписывающим устройством.

2) Если [имеются совместные обладатели [ключа] [подписывающего устройства]] [имеется более одного лица, осуществляющего контроль над [ключом] [подписывающим устройством]] [обязательства] [обязанности] по пункту 1 являются солидарными.

3) Обладатель подписи несет [ответственность] [финансовую ответственность] за [неисполнение [обязательств] [обязанностей]] [невыполнение требований], предусмотренных в пункте 1.

4) [Финансовая ответственность обладателя подписи не может превышать ущерба, который обладатель подписи предвидел или должен был предвидеть в момент неисполнения как возможное последствие неисполнения обладателем подписи [обязательств] [обязанностей] [требований], предусмотренных в пункте 1, учитывая обстоятельства, о которых обладатель ключа в то время знал или должен был знать.]

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 65-98;

A/CN.9/WG.IV/WP.80, пункты 18-19.

Общие примечания в отношении проектов статей 9 и 10

47. Рабочая группа, возможно, пожелает рассмотреть вопрос о практической взаимосвязи между проектами статей 9 и 10. Имеется ряд возможных комбинаций обязанностей, предусматриваемых в проекте статьи 9, и последствий неисполнения этих обязанностей в соответствии с проектом статьи 10. Проиллюстрировать некоторые из вопросов, которые необходимо рассмотреть, можно с помощью двух таких комбинаций.

48. Во-первых, ситуация, когда обладатель подписи не нарушает обязанности проявлять разумную заботливость согласно проекту статьи 9(1)(с), но тем не менее подпись тем или иным образом скомпрометирована. Обладатель подписи не знает о компрометации и, таким образом, не уведомляет сертификатора информации, но в то же время его вряд ли можно считать нарушившим обязанность по проекту статьи 9(1)(b). Согласно проекту статьи 10, полагающаяся сторона, проверяющая информацию, которая была представлена сертификатором информации, не может узнать о компрометации подписей и может положиться на подпись. В этой ситуации возникает ряд вопросов: является ли доверие к информации полагающейся стороны разумным в такой ситуации; лежит ли риск доверия на полагающейся стороне; каковы последствия такого доверия для обладателя подписи; связан ли обладатель подписи любой информацией, подписанной при использовании скомпрометированной подписи?

49. Во-вторых, может иметь место ситуация, когда обладатель подписи нарушает обязанность проявлять разумную заботливость согласно проекту статьи 9(1)(с) и когда подпись является скомпрометированной. Обладателю подписи известно о компрометации, и он уведомляет сертифициатора информации. Согласно проекту статьи 10 полагающаяся сторона, проверяющая информацию, которая была предоставлена сертифициатором информации, может узнать о компрометации подписи и не сможет, таким образом, положиться на эту подпись. Обладатель подписи будет, таким образом, нести ответственность согласно проекту статьи 9(3) за неисполнение обязанностей, предусмотренных в пункте 2 и будет нести финансовую ответственность за убытки согласно пункту 4. В этой ситуации результат является намного более ясным, чем в ситуации, рассмотренной в пункте 48.

Примечания

Статья 9, пункт 1

50. Пункт 1 проекта статьи 9 был пересмотрен в соответствии с решениями, принятыми Рабочей группой на ее тридцать четвертой сессии (A/CN.9/457, пункты 73-92). Рабочая группа выразила обеспокоенность тем, что обязанность, предусматриваемая в подпункте (а), должна быть ограничена контекстом процесса сертификации (A/CN.9/457, пункт 92), поскольку в противном случае эта обязанность может быть широко истолкована как охватывающая заверения и заявления, сделанные обладателем подписи полагающейся стороне. Поскольку заверения или заявления, сделанные в контексте этих отношений, должны регулироваться правом основного контракта, подпункт (а) был составлен в более узкой редакции, с тем чтобы ограничить эту обязанность контекстом процесса выдачи, приостановления действия или аннулирования сертификата.

51. Подпункт (b) был пересмотрен, с тем чтобы включить два альтернативных текста, согласованные Рабочей группой (A/CN.9/457, пункт 83). Слова "знал или должен был знать" не были включены в этот пересмотренный вариант на том основании, что обладателю подписи будет трудно исполнить обязанность по уведомлению, которая основывается на чем-то, что ему должно было быть известно, но что ему в действительности неизвестно.

52. В подпункте (с) упоминается не только обязательство не допускать несанкционированного использования подписи, но также и обязательство сохранять контроль над ключом. В этом пересмотренном положении также упоминается о моменте, с которого возникает обязанность проявлять разумную заботливость. Это отражает возобладавшее в Рабочей группе мнение о том, что, хотя обязанность держателя ключа защищать ключ должна возникать только в отношении тех пар ключей, которые фактически защищены сертификатом, обязанность держателя ключа защищать сертифицированные ключи от злоупотребления, должна применяться ретроактивно до момента, когда обладатель подписи получил исключительный контроль над парой ключей (A/CN.9/457, пункт 67).

Пункт 2

53. Пункт 2 был добавлен в проект статьи 9 с тем, чтобы прояснить обязательства проявлять должную заботливость в ситуации, когда существует несколько обладателей одного и того же ключа. Рабочая группа, возможно, пожелает рассмотреть это положение и его взаимосвязь с требованиями исключительного контроля, предусмотренными в статье 2.

Пункт 3

54. Этот пункт был пересмотрен в соответствии с решениями, принятыми Рабочей группой на ее сорок четвертой сессии (A/CN.9/457, пункты 93-98). Ссылка на "последствия неисполнения [обладателем подписи] обязательств, предусмотренных в пункте 1", была исключена с тем, чтобы i) избежать вопроса о том, являлось ли нарушенное обязательство договорным по своему характеру и ii) избежать любой неопределенности, которая может возникнуть в результате использования в тексте на английском языке слова "последствия" с определенным артиклем, что может предположительно означать, что имеются в

виду все возможные последствия, и не передает идею об отдаленности таких возможных последствий от момента неисполнения обязательства.

Пункт 4

55. Данный пункт основывается на статье 74 Конвенции Организации Объединенных Наций о договорах международной купли-продажи товаров и был включен для дальнейшего рассмотрения Рабочей группой. В нем устанавливается правило, основывающееся на критерии предсказуемости убытков, однако сфера его действия ограничивается нарушением обязательств обладателя подписи, устанавливаемых в пункте 1. На тридцать четвертой сессии Рабочей группой высказывалась определенная обеспокоенность (A/CN.9/457, пункты 93-98) в связи с тем, что ответственность, которая может возникнуть в контексте договора купли-продажи товаров, не равнозначна ответственности, которая может возникнуть из использования подписи, и что эти виды ответственности в количественном отношении не могут быть выражены одинаково. Было также указано, что критерий предсказуемости может быть неуместным в контексте договорных отношений между обладателем подписи и сертификатом информации, хотя такой критерий, возможно, и подходит к контексту отношений между обладателем подписи и полагающей стороной. Рабочая группа, возможно, пожелает изучить эти вопросы в ходе дальнейшего рассмотрения данного проекта статьи, а также дополнительно взаимосвязь проекта статьи 9 и проекта статьи 10.

Справочные национальные законодательные и другие тексты

Пункт 1(а) - материальные заверения

Руководящие принципы ААА

4.2 Обязательства абонента

Все материальные заверения, сделанные абонентом сертификационному органу, включая любую информацию, известную абоненту и изложенную в сертификате, должны быть наиболее точными, как это может быть известно обладателю подписи или как он это может предполагать, независимо от того, подтверждены ли такие заверения сертификационным органом.

ГУИДЕК

VII. Заверение сообщения

7. Заверения сертификатору

Абонент должен точно представить сертификатору все факты, имеющие существенное значение для сертификата.

Иллинойс

Статья 20. Обязанности абонентов

Раздел 20-101. Получение сертификата

Все материальные заверения, осознанно сделанные каким-либо лицом сертификационному органу для целей получения сертификата, в котором такое лицо именуется в качестве абонента, должны быть наиболее точными и полными, как это может быть известно такому лицу или как оно это может предполагать.

Раздел 20-105. Акцепт сертификата

[...]

b) В результате акцепта сертификата абонент, указанный в сертификате, заверяет любое лицо, которое, действуя добросовестно и в течение срока действия сертификата, разумно полагается на содержащуюся в нем информацию, в том, что:

- 1) абонент правомерно обладает частным ключом, соответствующим публичному ключу, указанному в сертификате;
- 2) все заверения, сделанные абонентом сертификационному органу и имеющие существенное значение для информации, указанной в сертификате, являются верными; и
- 3) вся указанная в сертификате информация, известная абоненту, является верной.

Сингапур

Часть IX. Обязанности абонентов

Получение сертификата

37. Все материальные заверения, сделанные абонентом сертификационному органу для целей получения сертификата, включая всю информацию, известную абоненту и изложенную в сертификате, должны быть наиболее точными и полными, как это может быть известно абоненту или как он это может предполагать, независимо от того, подтверждаются ли такие заверения сертификационным органом.

Пункт 1(b) - уведомление

Руководящие принципы ААА

4.4 Начало процесса приостановления действия или аннулирования

Абонент, который акцептовал сертификат, должен обратиться к выдавшему его сертификационному органу с просьбой о приостановлении действия или аннулировании сертификата, если частный ключ, соответствующий публичному ключу, указанному в сертификате, был скомпрометирован.

Иллинойс

Статья 20. Обязанности абонентов

Раздел 20-110. Аннулирование сертификата

Если иное не предусмотрено другой применимой нормой права, в случае, если частный ключ, соответствующий публичному ключу, указанному в действующем сертификате, утерян, украден, становится доступным для неуполномоченного лица или иным образом скомпрометирован в течение срока действия сертификата, абонент, которому стало известно о компрометации, должен незамедлительно обратиться к выдавшему сертификат сертификационному органу с просьбой об аннулировании сертификата и опубликовать уведомление об аннулировании во всех местах, в которых абонент ранее разрешил опубликование сертификата, или иным образом представить разумное уведомление об аннулировании.

Раздел 10-125. Создание подписывающих устройств и контроль над ними

Если иное не предусмотрено другой применимой нормой права, во всех случаях, когда создание, действительность или надежность электронной подписи, созданной с помощью процедуры защиты, отвечающей критериям, установленным [...], зависит от сохранения в тайне подписывающего устройства подписавшегося или от контроля над таким устройством:

- 1) лицо, обеспечивающее или создающее подписывающее устройство, должно осуществлять это надежным образом;
- 2) подписавшийся и все другие лица, которые правомерно обладают доступом к такому подписывающему устройству, должны проявлять разумную осмотрительность для сохранения контроля над подписывающим устройством и сохранения его в тайне, а также для защиты его от любого несанкционированного доступа, разглашения или использования в течение срока, когда доверие к подписи, созданной с помощью такого устройства, является разумным;
- 3) в случае, если подписавшемуся или какому-либо другому лицу, правомерно обладающему доступом к такому подписывающему устройству, известно - или у них имеются основания полагать, - что тайный характер такого подписывающего устройства или контроль над ним были скомпрометированы, такое лицо должно предпринять разумные усилия для незамедлительного уведомления всех лиц, которые, как это известно такому лицу, могут предсказуемо понести убытки в результате такой компрометации, или - в случаях, если имеется [...] надлежащий механизм публикации - опубликовать уведомление о компрометации и о дезавуировании любых подписей, созданных впоследствии.

Сингапур

Начало процесса приостановления действия или аннулирования

40. Абонент, акцептовавший сертификат, в кратчайшие возможные сроки обращается к выдавшему сертификат сертификационному органу с просьбой о приостановлении действия или аннулировании сертификата, если частный ключ, соответствующий публичному ключу, указанному в сертификате, скомпрометирован.

Пункт 1(c) - несанкционированное использование

Руководящие принципы ААА

4.3 Охрана частного ключа

В течение срока действия действительного сертификата абонент не компрометирует частный ключ, соответствующий публичному ключу, указанному в таком сертификате, а также должен избегать компрометации в течение любого периода приостановления действия.

ГУИДЕК

VII. Заверение сообщения

6. Охрана заверяющего устройства

Если лицо заверяет сообщение с помощью какого-либо устройства, это лицо, как минимум, должно проявлять разумную осмотрительность для недопущения несанкционированного использования этого устройства.

Иллинойс

Раздел 10-125. Создание подписывающих устройств и контроль над ними

Если иное не предусмотрено другой применимой нормой права, во всех случаях, когда создание, действительность или надежность электронной подписи, созданной с помощью процедуры защиты, отвечающей критериям, установленным [...], зависит от сохранения в тайне подписывающего устройства подписавшегося или от контроля над таким устройством:

- 1) лицо, обеспечивающее или создающее подписывающее устройство, должно осуществлять это надежным образом;
- 2) подписавшийся и все другие лица, которые правомерно обладают доступом к такому подписывающему устройству, должны проявлять разумную осмотрительность для сохранения контроля над подписывающим устройством и сохранения его в тайне, а также для защиты его от любого несанкционированного доступа, разглашения или использования в течение срока, когда доверие к подписи, созданной с помощью такого устройства, является разумным;
- 3) в случае, если подписавшемся или какому-либо другому лицу, правомерно обладающему доступом к такому подписывающему устройству, известно - или у них имеются основания полагать, - что тайный характер такого подписывающего устройства или контроль над ним были скомпрометированы, такое лицо должно предпринять разумные усилия для незамедлительного уведомления всех лиц, которые, как это известно такому лицу, могут предсказуемо понести убытки в результате такой компрометации, или - в случаях, если имеется [...] надлежащий механизм публикации - опубликовать уведомление о компрометации и о дезавуировании любых подписей, созданных впоследствии.

Пункты 3 и 4 - ответственность

Миннесота

325K.12 Заверения и обязанности после акцепта сертификатов

Подраздел 4. Возмещение абонентом

Акцептом сертификата абонент принимает на себя обязательство возмещать сертификационному органу ущерб или убытки, причиненные выдачей или опубликованием сертификата на основании доверия к:

- 1) ложному и существенно важному представлению факта абонентом;
- 2) несообщению абонентом существенно важного факта, если заверения или несообщения были сделаны либо с намерением ввести в заблуждение сертификационный орган или лицо, полагающееся на сертификат, или в результате грубой небрежности. Отказ от предоставления возмещения, предусматриваемого в настоящем разделе, или ограничение его объема на основании договорных положений не допускаются. В договоре могут быть предусмотрены, однако, отвечающие настоящему разделу дополнительные условия, касающиеся возмещения.

Сингапур

Часть IX. Обязанности абонентов

Контроль над частным ключом

39. 1) Акцептом сертификата, выданного сертификационным органом, абонент, указанный в сертификате, принимает на себя обязанность осуществлять разумную осмотрительность для сохранения контроля над частным ключом, соответствующим публичному ключу, указанному в таком сертификате, и для недопущения разглашения его лицу, не уполномоченному на создание цифровой подписи абонента.
- 2) Такая обязанность сохраняется в течение срока действия сертификата и в течение любого периода приостановления действия сертификата.

Статья 10. Доверие к усиленным электронным подписям

1) Лицо [имеет право] [не имеет права] полагаться на усиленную электронную подпись в той мере, в которой такое поведение [является] [не является] разумным.

2) При определении того, является ли доверие [не]разумным, учитывается, если это уместно, следующее:

- a) характер основной сделки, подтвердить которую предполагается с помощью подписи;
- b) предприняла ли полагающаяся сторона надлежащие шаги для определения надежности подписи;

- c) было ли полагающейся стороне известно или должно было быть известно, что подпись была скомпрометирована или аннулирована;
- d) любое соглашение или практика в отношениях между полагающейся стороной и абонентом или любой торговый обычай, который может быть применимым;
- e) любой другой соответствующий фактор.

Статья 11. Доверие к сертификатам

- 1) Лицо [имеет право] [не имеет права] полагаться на сертификат в той мере, в которой такое поведение [является] [не является] разумным.
- 2) При определении того, является ли доверие [не]разумным, учитывается, если это уместно, следующее:
 - a) любые ограничения, установленные для сертификата;
 - b) предприняла ли полагающаяся сторона надлежащие шаги для определения надежности сертификата, включая ознакомление с перечнем аннулированных сертификатов, когда это уместно;
 - c) любое соглашение или практика в отношениях между полагающейся стороной и сертификатом информации или абонентом или любой торговый обычай, который может быть применимым;
 - d) [любой другой соответствующий фактор] [все другие соответствующие факторы].

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 99-107;

A/CN.9/WG.IV/WP.80, пункты 20-21.

Примечания

56. Проекты статей 10 и 11, которые касаются, соответственно, разумности доверия к усиленным электронным подписям и сертификатам, были пересмотрены в соответствии с мнениями в отношении содержания этих статей, возобладавшими на тридцать четвертой сессии Рабочей группы (A/CN.9/457, пункт 107). Хотя первоначальное предложение состояло в том, чтобы урегулировать как доверие к подписям, так и доверие к подписям, подтвержденным сертификатом, в одной единой статье, в нынешнем проекте эти две концепции были разделены на том основании, что в каждой ситуации применимы различные соображения. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, имеется ли необходимость во включении правила относительно доверия к сертификатам в дополнение к правилу относительно доверия к подписям и какие соображения применительно к установлению разумного характера доверия в каждом конкретном случае следует предусмотреть.

57. Рабочая группа выразила определенную обеспокоенность тем, что составление проектов статей 10 и 11 в качестве положений, устанавливающих право полагаться на подписи и сертификаты, может предполагать определенные юридические последствия, в то время, как положение, устанавливающее те факторы, которые должны приниматься во внимание при определении того, может ли доверие рассматриваться в качестве разумного, может позволить избежать рассмотрения вопроса о возможных юридических последствиях подписи или сертификата. Противоположная точка зрения состояла в том, что редакция этих проектов статей в качестве положений, устанавливающих право полагаться на сертификат или подпись, создает дополнительные преимущества, не предусмотренные в Типовом законе,

и не устанавливает никаких юридических последствий с точки зрения действительности подписи. Как это было согласовано Рабочей группой, в пересмотренные проекты статей должны быть включены формулировки как в положительной, так и в отрицательной форме, и в них следует предусмотреть факторы, которые должны приниматься во внимание в случае подписей и в случае сертификатов.

58. Определенная обеспокоенность была выражена также в отношении взаимосвязи между проектами статей 10 и 11 и статьей 13 Типового закона, а также в отношении вопроса о том, будут ли статьи 9, 10 и 11, если их читать вместе, устанавливать правило атрибуции. Рабочая группа, возможно, пожелает рассмотреть взаимосвязь проектов статей 10 и 11 с проектом статьи 9, а также со статьей 13 Типового закона.

Справочные национальные законодательные и другие тексты

Руководящие принципы ААА

5.3 Ненадежные цифровые подписи

1) [...]

2) Если иное не предусмотрено законом или договором, полагающаяся сторона принимает на себя риск того, что цифровая подпись является недействительной в качестве подписи или удостоверения подлинности подписанного сообщения, если доверие к этой цифровой подписи является неразумным в данных обстоятельствах в соответствии с факторами, перечисленными в Руководящем принципе 5.4 (разумность доверия).

5.4 Разумность доверия

Нижеперечисленные факторы, в том числе, имеют существенное значение при оценке разумности доверия получателя к сертификату и к цифровым подписям, которые могут быть проверены при использовании публичного ключа, указанного в сертификате:

- 1) факты, которые полагающейся стороне известны или о которых полагающаяся сторона была уведомлена, включая все факты, указанные в сертификате или включенные в него посредством ссылки;
- 2) ценность или важность подписанного в цифровой форме сообщения, если она известна;
- 3) практика в отношениях между полагающимся лицом и абонентом, а также имеющиеся признаки надежности или ненадежности, помимо цифровой подписи;
- 4) торговый обычай, особенно в том, что касается сделок, заключаемых с помощью надежных систем или других компьютерных средств.

2.3 Предсказуемость доверия к сертификатам

Поведение, при котором лица, полагающиеся на цифровую подпись, будут также полагаться на действующий сертификат, содержащий публичный ключ, с помощью которого может быть проверена цифровая подпись, является предсказуемым.

ГУИДЕК

VIII. Сертификация

1. Последствия действительного сертификата

Лицо может положиться на действующий сертификат как на точно заверяющий факт или факты, указанные в нем, если это лицо не получало уведомления о том, что сертифициатор не выполнил какого-либо материального требования к практике заверенных сообщений.

Сингапур

Часть VI. Последствия цифровых подписей

Ненадежные цифровые подписи

22. Если иное не предусмотрено законом или договором, лицо, полагающееся на электронную запись, подписанную в цифровой форме, принимает на себя риск того, что эта цифровая подпись является недействительной в качестве подписи или удостоверения подлинности подписанного электронного сообщения, если доверие к этой цифровой подписи является неразумным в данных обстоятельствах с учетом следующих факторов:

- a) факты, которые известны лицу, полагающемуся на электронное сообщение, подписанное в цифровой форме, или о которых оно было уведомлено, включая все факты, указанные в сертификате или включенные в него посредством ссылки;
- b) ценность или важность электронной записи, подписанной в цифровой форме, если она известна;
- c) практика в отношениях между лицом, полагающимся на электронную запись, подписанную в цифровой форме, и абонентом и имеющиеся признаки надежности или ненадежности, помимо цифровой подписи; и

d) любой торговый обычай, особенно в том, что касается сделок, совершаемых с помощью надежных систем или других электронных средств.

Статья 12. [Ответственность] [обязанности] сертификатора информации

- 1) [Сертификатор информации [обязан] [, в том числе,]:
- a) [действовать] [действует] в соответствии с заверениями, сделанными им в отношении его практики;
 - b) [предпринимать] [предпринимает] разумные шаги для определения точности любых фактов или информации, которые сертификатор информации сертифицирует в сертификате [, включая личность обладателя подписи];
 - c) [обеспечивать] [обеспечивает] разумно доступные средства, которые позволяют полагающейся стороне установить:
 - i) личность сертификатора информации;
 - ii) что лицо, которое [поименовано] [идентифицировано] в сертификате, [обладает] [обладало в соответствующий момент] [частным ключом, соответствующим публичному ключу, указанному] [подписывающим устройством, указанным], в сертификате;
 - iii) что ключи представляют собой функционирующую пару ключей;
 - iv) способ, использованный для идентификации обладателя подписи;
 - v) любые ограничения в отношении цели или стоимостного объема, в связи с которыми может использоваться подпись; и
 - vi) является ли подписывающее устройство действительным и не было ли оно скомпрометировано;
 - d) [обеспечивать] [обеспечивает] обладателей подписей средствами для направления уведомлений о том, что усиленная электронная подпись была скомпрометирована, и [обеспечивать] [обеспечивает] своевременное функционирование службы аннулирования;
 - e) [проявлять] [проявляет] надлежащую осмотрительность для обеспечения точности и полноты всех сделанных сертификатором информации материальных заверений, которые имеют отношение к выдаче, приостановлению действия или аннулированию сертификата или которые включены в сертификат;
 - f) [использовать] [использует] надежные системы, процедуры и людские ресурсы при предоставлении своих услуг.

Вариант X

- 2) Сертификатор информации несет [ответственность] [финансовую ответственность] за [неисполнение [обязательств] [обязанностей]] [невыполнение требований], предусмотренных в пункте 1.
- 3) Финансовая ответственность сертификатора информации не может превышать ущерба, который сертификатор информации предвидел или должен был предвидеть в момент неисполнения как возможное последствие неисполнения сертификатором информации [обязательств] [обязанностей] [требований], предусмотренных в пункте 1, учитывая обстоятельства, о которых сертификатор информации в то время знал или должен был знать.

Вариант Y

2) С учетом положений пункта 3, если ущерб был причинен в результате неправильности или дефекта в сертификате, сертифициator информации несет финансовую ответственность за убытки, понесенные, либо:

a) стороной, вступившей в договорные отношения с сертифициatorом информации для цели выдачи сертификата; или

b) любым лицом, которое разумно полагается на сертификат, выданный сертифициatorом информации.

3) Сертификатор информации не несет финансовой ответственности согласно пункту 2:

a) если - и в той мере, в которой - в которой он включил в сертификат заявление, ограничивающее объем или пределы своей финансовой ответственности перед любым лицом; или

b) если он докажет, что он [не проявил небрежности] [принял все разумные меры для недопущения ущерба].

Справочные документы ЮНСИТРАЛ

A/CN.9/457, пункты 108-119;

A/CN.9/WG.IV/WP.80, пункты 22-24.

Примечания

59. Проект статьи 12 был пересмотрен в соответствии с решениями, принятыми Рабочей группой на ее сорок четвертой сессии (A/CN.9/457, пункты 108-119).

Пункт 1

60. В тексте пункта 1 отражены несколько альтернативных вариантов. Первый из них связан с вопросом о том, следует ли редакцию этого положения составить при использовании формулировки "обязан" сделать то-то и то-то, или же формулировки с использованием глагола в настоящем времени. Второй альтернативный вариант связан с использованием слов "в том числе" во вступительной формулировке. Если эти слова будут использованы, то в проекте статьи 12 будет излагаться открытый, иллюстративный перечень обязанностей. Хотя сертифициatorам информации подобная формулировка будет, возможно, представляться обременительной, она, по мнению Рабочей группы, не будет противоречить общему правилу, применимому в настоящее время к сертифициatorам информации во многих правовых системах. Если слова "в том числе" будут исключены, то в проекте статьи 12 будет излагаться исчерпывающий перечень обязанностей сертифициатора информации, что позволит определять точный объем финансовой ответственности сертифициатора информации и избежать трудностей, которые могут возникнуть в результате использования различных формулировок в странах, в которых может и не предусматриваться общая обязанность сертифициатора информации проявлять надлежащую осмотрительность.

61. Что касается конкретных обязанностей, включенных в пункт 1, то этот перечень был расширен с тем, чтобы учесть мнения, высказанные в Рабочей группе (A/CN.9/457, пункты 112-114). Что касается подпункта (с), то информация, которая должна быть представлена с помощью "разумно доступных средств", включает определенную информацию, включения которой в сертификат может разумно ожидать полагающаяся сторона, и иную информацию, которая может быть получена только путем отсылки к какому-либо другому источнику, например к перечню аннулированных сертификатов. Рабочая группа, возможно, пожелает рассмотреть вопросы о том, следует ли конкретно оговорить необходимость

включения в сертификат некоторой такой информации и следует ли включить в единообразные правила дополнительную норму, устанавливающую минимальное содержание сертификата.

62. В пункте 1(с)(ii) содержатся ссылки как на "пару ключей", так и на "подписывающее устройство". Для обеспечения нейтральности единообразных правил, с технологической точки зрения, Рабочая группа, возможно, пожелает рассмотреть вопрос об использовании такой, например, технологически нейтральной формулировки, как "подписывающее устройство", в качестве альтернативы словам "пара ключей", поскольку слова "пара ключей" непосредственно связаны с технологией цифровых подписей. Использование словосочетания "пара ключей" в связи с определением "сертификата" может быть уместным в ситуациях, когда сертификаты используются только в контексте цифровых подписей.

63. Пункт 1(с)(iii) был включен в соответствии с внесенным на предыдущей сессии предложением, однако Рабочая группа, возможно, пожелает рассмотреть вопрос о том, является ли предусматриваемое требование уместным. Если публичный ключ, указанный в сертификате, соответствует частному ключу, находящемуся в распоряжении обладателя подписи, и между двумя ключами имеется, таким образом, математическое соответствие, то непонятно, какой дополнительный функциональный элемент будет привноситься требованием о том, чтобы пара ключей представляла собой "функционирующую пару ключей". Кроме того, имеются сомнения в вопросе о том, сможет ли сертифициатор информации представить - в дополнение к требуемому согласно пункту 1(с)(ii) - какую-либо информацию, которая будет указывать на этот дополнительный функциональный элемент.

Пункты 2 и 3

64. Вариант X устанавливает правило, согласно которому сертифициатор информации несет ответственность за неисполнение обязательств или обязанностей, предусмотренных в пункте 1, однако определение конкретных возможных последствий такого неисполнения оставляется на усмотрение национального законодательства. В пересмотренном варианте проекта статьи 12 слово "последствия" было исключено по тем же причинам, которые приводились в связи с исключением этого слова из пункта 3 проекта статьи 9. Это было сделано в следующих целях: i) необходимость избежать изучения вопроса о том, являлось ли нарушенное обязательство договорным по своему характеру и ii) необходимость избежать неопределенности, которая может возникнуть в результате использования в тексте на английском языке слова "последствия" с определенным артиклем, что может предположительно означать, что имеются в виду все возможные последствия, и не передает идеи об отдаленности таких возможных последствий от момента неисполнения обязательства.

65. После решения вопроса о включении в пересмотренный пункт 1 одного из двух вариантов: исчерпывающего перечня обязательств или открытого, иллюстративного перечня обязательств - Рабочая группа, возможно, пожелает рассмотреть вопрос о том, не будет ли вариант X более уместным в том случае, если пункт 1 будет составлен в виде исчерпывающего, а не открытого перечня.

66. В пункте 3 варианта X устанавливается правило предсказуемости ущерба, основывающееся на статье 74 Конвенции Организации Объединенных Наций о договорах международной купли-продажи товаров. В результате этого пункта объем финансовой ответственности сертифициатора информации, которая может возникнуть на основании пунктов 1 и 2, в количественном выражении ограничивается.

Вариант Y

67. В рамках Рабочей группы широкое распространение получило мнение (A/CN.9/457, пункт 115) о том, что было бы целесообразным подготовить унифицированное правило, выходящее за рамки простой ссылки на применимое право, и установить общее правило финансовой ответственности за небрежность при условии возможных договорных исключений (если подобное ограничение не будет явно несправедливым) и при условии возможности сертифициатора информации освободиться от ответственности, если он докажет, что исполнил обязательства по пункту 1. Пункт 2 варианта Y касается вопроса о том, перед кем сертифициатор информации может нести финансовую ответственность. В

пункте 3 устанавливается правило, позволяющее сертификатору информации полагаться на любое ограничение финансовой ответственности, установленное в сертификате, или доказать, что он не проявил небрежности или принял все разумные меры для недопущения ущерба.

68. Как и в случае варианта X, Рабочая группа, возможно, пожелает рассмотреть вопрос о том, не является ли положение, подобное предлагаемому в варианте Y, более уместным в контексте исчерпывающего перечня обязанностей по пункту 1, чем в случае, когда перечень обязательств будет открытым. Она также, возможно, пожелает рассмотреть вопрос о необходимости четко оговорить в проекте пункта 2 варианта Y, что финансовая ответственность сертификатора информации ограничивается случаями неисполнения обязательств, установленных в пункте 1.

Справочные национальные законодательные и другие тексты

Статья 12, пункт 1 - общие обязанности

Руководящие принципы ААА

3. Сертификационные органы

3.1 Сертификационные органы должны использовать надежные системы

Сертификационные органы при предоставлении своих услуг должны использовать надежные системы.

3.2 Раскрытие информации

- 1) Сертификационный орган должен раскрывать любые существенно важные заявления о практике сертификации, а также информацию об уведомлении об аннулировании и приостановлении действия сертификата сертификаторного органа.
- 2) Сертификационный орган должен прилагать разумные усилия для уведомления любых лиц, которые, как это известно, затронуты или будут предсказуемо затронуты аннулированием или приостановлением действия его сертификата сертификаторного органа.
- 3) [...]
- 4) В случае события, имеющего существенные и негативные последствия для надежной системы сертификаторного органа или его сертификата сертификаторного органа, сертификаторный орган должен приложить разумные усилия для уведомления любых лиц, которые, как это известно, затронуты или будут предсказуемо затронуты этим событием, или предпринять действия в соответствии с процедурами, указанными в его заявлении о практике сертификации.

3.7 Заверения сертификаторного органа в сертификате

Выдавая сертификат, сертификаторный орган заверяет любое лицо, которое разумно полагается на сертификат или цифровую подпись, которую можно проверить с помощью указанного в сертификате публичного ключа, что сертификаторный орган в соответствии с любым применимым заявлением о практике сертификации, о котором уведомлено полагающееся лицо, подтверждает, что:

- 1) сертификаторный орган при выдаче сертификата выполнил все применимые требования настоящих Руководящих принципов и, если сертификаторный орган опубликовал сертификат или иным образом предоставил его в распоряжение такого разумно полагающегося лица, что абонент, указанный в сертификате, акцептовал его;
- 2) абонент, идентифицированный в сертификате, обладает частным ключом, соответствующим публичному ключу, указанному в сертификате;
- 3) [...]
- 4) публичный ключ и частный ключ абонента представляют собой функционирующую пару ключей; и
- 5) вся информация в сертификате является точной, если только сертификаторный орган не заявил в сертификате, что точность конкретно оговоренной информации не подтверждается, или не указал на это с помощью включения в сертификат соответствующей ссылки.

Кроме того, сертификаторный орган заверяет, что в сертификате не опущены никакие известные имеющие существенное значение факты, которые в случае, если бы они были известны, оказали бы неблагоприятное воздействие на надежность его заверений согласно настоящему руководящему принципу.

3.9 Приостановление действия сертификата по просьбе абонента

Если иное не предусмотрено договором между сертификаторным органом и абонентом, сертификаторный орган должен приостановить действие сертификата в кратчайший возможный срок после получения просьбы от лица, которое, как это может разумно полагать сертификаторный орган, является:

- 1) абонентом, указанным в сертификате;
- 2) лицом, должным образом уполномоченным действовать от имени этого абонента; или
- 3) лицом, действующим от имени этого абонента, который не может выйти на связь.

3.10 Аннулирование сертификата по просьбе абонента

Сертификационный орган, который выдал сертификат, должен аннулировать его по просьбе указанного в нем абонента, если сертификационный орган подтвердил

- 1) что лицо, обращающееся с просьбой об аннулировании, является абонентом, указанным в сертификате, подлежащем аннулированию; или
- 2) если проситель действует в качестве агента, что этот проситель имеет достаточные полномочия на осуществление аннулирования.

3.11 Аннулирование или приостановление действия без согласия абонента

Сертификационный орган должен приостановить действие сертификата или аннулировать его независимо от согласия на это абонента, указанного в сертификате, если сертификационный орган подтверждает, что

- 1) какой-либо существенный факт, заверенный в сертификате, является ложным,
- 2) какое-либо существенное предварительное условие для выдачи сертификата не было выполнено, или
- 3) частный ключ или надежная система сертификационного органа были скомпрометированы таким образом, который существенно затрагивает надежность сертификата.

По осуществлении такого приостановления действия или аннулирования сертификационный орган должен незамедлительно уведомить об этом абонента, указанного в сертификате, который был аннулирован или действие которого было приостановлено.

3.12 Уведомление о приостановлении действия или аннулировании

Незамедлительно по приостановлении действия или аннулировании сертификата сертификационный орган должен опубликовать уведомление о приостановлении действия или аннулировании, если сертификат был опубликован, и должен по запросу полагающейся стороны иным образом раскрыть информацию о факте приостановления действия или аннулирования.

Проект директивы ЕС

Приложение II Требования к поставщикам сертификационных услуг, выдающим сертификаты, отвечающие установленным требованиям

Поставщики сертификационных услуг должны:

- a) продемонстрировать надежность, необходимую для предложения сертификационных услуг;
- b) обеспечить функционирование оперативной и надежной директории и надежной и безотлагательной службы аннулирования;
- b(a) обеспечить возможность установления даты и времени выдачи или аннулирования сертификата;
- c) проверять с помощью надлежащих средств в соответствии с национальным правом личность и, если это применимо, любые конкретные характеристики лица, которому выдается отвечающий установленным требованиям сертификат;
- d) нанимать на службу сотрудников, обладающих специальными знаниями, опытом и квалификацией, необходимыми для предоставления предлагаемых услуг, в частности, компетенцией на управленческом уровне, опытом в применении технологии электронных подписей и знакомством с надлежащими процедурами защиты; они также должны применять административные и управленческие процедуры и процессы, которые являются достаточными и которые отвечают признанным стандартам;
- e) использовать надежные системы и продукты, которые защищены от модификации и которые должны обеспечивать техническую и криптографическую безопасность поддерживаемых ими процессов;
- f) принимать меры против подделки сертификатов и в тех случаях, когда поставщик сертификационных услуг готовит данные для создания подписи, гарантировать конфиденциальность в ходе процесса подготовки таких данных;
- g) поддерживать финансовые ресурсы на достаточном уровне для обеспечения функционирования в соответствии с требованиями, установленными в настоящей Директиве, в частности, покрывать риск финансовой ответственности за убытки, например, посредством заключения соответствующего страхования;
- h) вести запись всей соответствующей информации, касающейся сертификата, отвечающего установленным требованиям, в течение надлежащего срока, в частности, для представления доказательств сертификации для целей юридических процедур. Такие записи могут вестись электронным способом;
- i) не хранить или не копировать данных для создания подписи лица, которому поставщик сертификационных услуг предлагает услуги по управлению использованием ключа;
- j) до заключения договорных отношений с лицом, обращающимся за выдачей сертификата для подтверждения его электронной подписи, проинформировать это лицо с помощью средств связи, обеспечивающих возможность длительного хранения информации, о конкретных условиях использования сертификата, включая любые ограничения на использование сертификата, о наличии добровольной аккредитации и о процедурах для подачи жалоб и урегулирования споров. Такая информация должна представляться в письменной форме и может передаваться электронным способом на доступном языке.

По просьбе третьих сторон, полагающихся на сертификат, также должен предоставляться доступ к соответствующим частям такой информации;

- k) использовать надежные системы для хранения сертификатов в поддающейся проверке форме с тем, чтобы
- вносить записи и изменения могли только уполномоченные лица,
 - информация могла быть проверена на аутентичность,
 - публичный доступ к поиску сертификатов был открыт только в тех случаях, когда получено согласие обладателя сертификата; и
 - любые технические изменения, компрометирующие эти требования безопасности, были очевидны для оператора.

Германия

§ 5 Выдача сертификатов

- 1) Сертификатор надежно идентифицирует лиц, обращающихся за выдачей сертификата. Он подтверждает атрибуцию публичного подписывающего ключа идентифицированному лицу посредством сертификата подписывающего ключа и обеспечивает доступ к таковому, а также к атрибутивным сертификатам, в любой момент и для любых лиц по публично доступным телекоммуникационным каналам поддающимся проверке образом и с согласия владельца подписывающего ключа.
- 2) По просьбе заявителя сертификат регистрирует информацию, касающуюся полномочий заявителя на представление третьей стороны или касающуюся его профессиональной или другой лицензии, в сертификате подписывающего ключа или в атрибутивном сертификате в той мере, в которой такая лицензия или согласие третьей стороны на регистрацию полномочий на представительство будут достоверно продемонстрированы.
- 3) По просьбе заявителя сертификат регистрирует в сертификате вместо имени заявителя его псевдоним.
- 4) Сертификатор принимает меры с тем, чтобы данные для сертификатов не могли быть подделаны или фальсифицированы каким-либо незаметным образом. Кроме того, он предпринимает шаги для гарантирования конфиденциальности частных подписывающих ключей. Хранение частных подписывающих ключей сертификатом не допускается.
- 5) Для сертификационной деятельности он использует надежный персонал и в соответствии с §14 использует технические компоненты для обеспечения доступа к подписывающим ключам и создания сертификатов. Это также применяется к техническим компонентам, позволяющим осуществить проверку сертификатов согласно второму предложению пункта 1.

§ 6 Обязанности инструктировать

Сертификатор инструктирует заявителя согласно пункту 1 § 5 относительно мер, необходимых для содействия защите цифровых подписей и их достоверной проверки. Он инструктирует заявителя относительно технических компонентов, которые необходимы для выполнения требований пунктов 1 и 2 § 14, а также относительно атрибуции цифровых подписей, созданных с помощью частного подписывающего ключа. Он информирует заявителя о том, что данные относительно цифровых подписей, возможно, потребуются вновь подписать до того, как степень защиты имеющейся подписи с течением времени ослабится.

§ 8 Блокирование сертификатов

- 1) Сертификатор блокирует сертификат, если с просьбой об этом обращается владелец подписывающего ключа или его представитель, если сертификат был выдан на основе ложной информации согласно § 7, если сертификат прекращает свои операции и их осуществление не продолжается каким-либо другим сертификатом, или если Орган отдает приказ о блокировании согласно второму предложению пункта 5 § 13. При блокировании указывается время, с которого начинается его действие. Ретроактивное блокирование не допускается.

ГУИДЕК

VIII Сертификация

2. Точность заверений в сертификате

Сертификатор должен подтвердить точность всех фактов, указанных в действующем сертификате, только если из самого сертификата очевидно не следует, что некоторая информация не была проверена.

3. Надежность сертификатора

Сертификатор должен:

- a) использовать только технологически надежные информационные системы и процессы и надежный персонал при выдаче сертификата и при приостановлении действия или аннулировании сертификата публичного ключа и при охране своего частного ключа, если таковой имеется;
- b) избегать коллизий интересов, которые обусловят ненадежность сертификатора применительно к выдаче, приостановлению действия и аннулированию сертификата;
- c) воздерживаться от участия в нарушении обязанностей абонента;
- d) воздерживаться от действий или бездействия, которые могут нанести существенный ущерб разумному и предсказуемому доверию к действующему сертификату;
- e) действовать надежным образом в отношении абонента и лиц, полагающихся на действующий сертификат.

4. Уведомление о практике и проблемах

Сертификатор должен предпринимать разумные усилия для уведомления предсказуемо затронутых лиц о:

- a) любом существенном заявлении о практике сертификации, и
- b) любом факте, имеющем существенное значение либо для надежности сертификата, который был им выдан, или для его способности предоставлять свои услуги.

8. Приостановление действия сертификата публичного ключа по просьбе

Сертификатор, который выдал сертификат, должен незамедлительно приостановить его действие по просьбе лица, идентифицировавшего себя в качестве абонента, поименованного в сертификате публичного ключа, или в качестве лица, положение которого, по всей видимости, дают ему возможность узнать о компрометации защиты частного ключа абонента, например, его агента, служащего, компаньона или члена непосредственной семьи абонента.

9. Аннулирование сертификата публичного ключа по просьбе

Сертификат, который выдал сертификат публичного ключа, должен незамедлительно аннулировать его после:

- a) получения просьбы об аннулировании от абонента, поименованного в сертификате, или уполномоченного агента этого абонента, и
- b) подтверждения того, что лицо, обратившееся с просьбой об аннулировании, является таким абонентом или является агентом этого абонента, уполномоченным просить об аннулировании.

10. Приостановление действия или аннулирование сертификата публичного ключа без согласия

Сертификатор, который выдал сертификат публичного ключа, должен аннулировать его, если:

- a) сертификат подтверждает, что существенный факт, заверенный в сертификате, является ложным;
- b) сертификат подтверждает, что надежность информационной системы сертификатора была скомпрометирована таким образом, который может существенно затронуть надежность сертификатов.

Сертификатор может приостановить действие разумно сомнительного сертификата на срок, необходимый для проведения расследования, в достаточной степени подтверждающего основания для аннулирования согласно настоящей статье.

11. Уведомление об аннулировании или приостановлении действия сертификата публичного ключа

Незамедлительно по приостановлении действия или аннулировании сертификата публичного ключа сертификатом сертификат должен сделать надлежащее уведомление об аннулировании или приостановлении действия.

Иллинойс

Статья 15. Последствия цифровой подписи

Раздел 15-301. Надежные услуги

За исключением ясно указанного в заявлении о практике сертификации сертификационный орган и лицо, обеспечивающее функционирование хранилища информации, должны поддерживать функционирование и предоставлять свои услуги надежным образом.

Раздел 15-305. Раскрытие информации

a) Применительно к каждому сертификату, выдаваемому сертификационным органом с той целью, что на него будут полагаться третьи стороны для проверки цифровых подписей, созданных абонентами, сертификационный орган должен публиковать или иным образом предоставлять в распоряжение абонента и всех таких полагающихся сторон:

- 1) свое заявление о практике сертификации, если таковое имеется, применимое к такому сертификату; и
- 2) свой сертификат, в котором указывается сертификационный орган в качестве абонента и в котором содержится публичный ключ, соответствующий частному ключу, используемому сертификационным органом для цифрового подписания сертификата (свой "сертификат сертификационного органа").

b) В случае события, которое существенным образом и негативно затрагивает операции или систему сертификационного органа, его сертификат сертификационного органа или какой-либо иной аспект его способности функционировать надежным образом, сертификационный орган должен действовать в соответствии с указанными в его заявлении о практике сертификации процедурами, регулирующими действия в случае таких событий, или, в отсутствие таких процедур, должен предпринять разумные усилия для уведомления любых лиц, которые, как это известно сертификационному органу, могут предсказуемо понести ущерб в результате такого события.

Раздел 15-310. Выдача сертификата

Сертификационный орган может выдать сертификат будущему абоненту для целей создания возможности для третьих сторон проверять цифровые подписи, созданные абонентом, только после того как:

- 1) сертификационный орган получит просьбу о выдаче от будущего абонента; и
- 2) сертификационный орган:
 - A) выполнит требования всех соответствующих видов практики и процедур, установленные в применимом заявлении о практике сертификации, если таковое имеется; или

В) в отсутствие заявления о практике сертификации, регулирующей такие вопросы, подтвердит надежным образом, что:

- i) будущий абонент является лицом, которое будет указано в сертификате, который будет выдан;
- ii) информация в сертификате, который будет выдан, является точной; и
- iii) будущий абонент правомерно обладает частным ключом, способным создавать цифровую подпись, и что публичный ключ, который будет указан в сертификате, может быть использован для проверки цифровой подписи, приложенной с помощью такого частного ключа.

Раздел 15-315. Заверения по выдаче сертификата

а) Выдавая сертификат с той целью, что на него будут полагаться третьи стороны для проверки цифровых подписей, созданных абонентом, сертификационный орган добросовестно и в течение срока действия сертификата заверяет абонента и любое лицо, которое разумно полагается на информацию, содержащуюся в сертификате, что:

- 1) сертификационный орган обработал, одобрил и выдал - и будет заниматься поддержкой и, в случае необходимости, аннулирует сертификат в соответствии с применимым заявлением о практике сертификации, которое указано в сертификате или включено в него с помощью ссылки или о котором было уведомлено такое лицо, или, вместо такого заявления, в соответствии с настоящим Законом или законодательством правовой системы, регулирующей вопросы выдачи сертификата;
- 2) сертификационный орган проверил личность абонента в той степени, в которой это указано в сертификате или в применимом заявлении о практике сертификации, или, вместо этого, что сертификационный орган проверил личность абонента надежным образом;
- 3) сертификационный орган проверил, что лицо, обратившееся с просьбой о выдаче сертификата, обладает частным ключом, соответствующим публичному ключу, указанному в сертификате; и
- 4) за исключением ясно указанного в сертификате или в применимом заявлении о практике сертификации, насколько это известно сертификационному органу на дату выдачи сертификата, вся другая информация о сертификате является точной и не вводящей по существу в заблуждение.

б) Если сертификационный орган выдал сертификат в соответствии с законодательством другой правовой системы, сертификационный орган также, если это уместно, дает все гарантии и заверения, которые иным образом применимы в соответствии с правом, регулирующим вопросы выдачи.

Раздел 15-320. Аннулирование сертификата

а) В течение срока действия сертификата сертификационный орган, выдавший сертификат, должен аннулировать сертификат в соответствии с принципами и процедурами, регулирующими аннулирование и указанными в применимом заявлении о практике сертификации, или, в отсутствие таких принципов и процедур, в кратчайшие возможные сроки после:

- 1) получения просьбы об аннулировании от абонента, поименованного в сертификате, и подтверждения того, что лицо, обратившееся с просьбой об аннулировании, является абонентом или агентом абонента, уполномоченным просить об аннулировании;
- 2) получения заверенной копии свидетельства о смерти абонента-физического лица или по подтверждении смерти абонента на основании других надежных доказательств;
- 3) представления в его распоряжение документов, на основании которых осуществляется расформирование абонента-юридического лица, или подтверждения на основании других доказательств того, что абонент был расформирован или прекратил существование;
- 4) вручения требующего приказа, выданного судом компетентной правовой системы; или
- 5) подтверждения сертификационным органом того, что:
 - A) существенно важный факт, заверенный в сертификате, является ложным,
 - B) существенное предварительное условие для выдачи сертификата не было выполнено,
 - C) частный ключ или операционная система сертификационного органа были скомпрометированы таким образом, который существенно затрагивает надежность сертификата, или
 - D) частный ключ абонента был скомпрометирован.

б) По осуществлении такого аннулирования сертификационный орган должен уведомить абонента и полагающиеся стороны в соответствии с принципами и процедурами, регулирующими уведомление об аннулировании и указанными в применимом заявлении о практике сертификации, или, в отсутствие таких принципов и процедур, незамедлительно уведомить абонента, незамедлительно опубликовать уведомление об аннулировании во всех местах, в которых сертификационный орган ранее обеспечил опубликование сертификата, или иным образом раскрыть информацию о факте аннулирования по запросу полагающейся стороны.

Сингапур

Часть VIII

Обязанности сертификационных органов

Надежная система

27. Сертификационный орган должен использовать надежные системы при предоставлении своих услуг.

Раскрытие информации

28. 1) Сертификационный орган раскрывает следующую информацию:
- a) свой сертификат, в котором указывается публичный ключ, соответствующий частному ключу, используемому этим сертификационным органом для цифрового подписания других сертификатов (в настоящем разделе - "сертификат сертификационного органа");
 - b) любое соответствующее заявление о практике сертификации;
 - c) уведомление об аннулировании или приостановлении действия сертификата сертификационного органа; и
 - d) любой другой факт, который существенным образом и негативно затрагивает либо надежность сертификата, выданного этим органом, либо способность этого органа предоставлять свои услуги.
- 2) В случае события, которое существенным образом и негативно затрагивает надежную систему сертификационного органа или сертификат сертификационного органа, сертификационный орган:
- a) предпринимает разумные усилия для уведомления любых лиц, которые, как это известно, затронуты или предсказуемо будут затронуты этим событием; или
 - b) действует в соответствии с указанными в его заявлении о практике сертификации процедурами, регулирующими действия в случае таких событий.

Выдача сертификата

29. 1) Сертификационный орган может выдать сертификат будущему абоненту только после того, как сертификационный орган:
- a) получит просьбу о выдаче от будущего абонента; и
 - b) выполнит
 - i) если имеется заявление о практике сертификации - все виды практики и процедуры, изложенные в таком заявлении о практике сертификации, включая процедуры, касающиеся идентификации будущего абонента; или
 - ii) в отсутствие заявления о практике сертификации - условия, указанные в подразделе 2.
- 2) В отсутствие заявления о практике сертификации сертификационный орган подтверждает самостоятельно или через уполномоченного агента, что:
- a) будущий абонент является лицом, которое будет указано в сертификате, который будет выдан;
 - b) если будущий абонент действует через одного или нескольких агентов - абонент уполномочил агента хранить частный ключ абонента и обращаться с просьбой о выдаче сертификата, в котором указывается соответствующий публичный ключ;
 - c) информация в сертификате, который будет выдан, является точной;
 - d) будущий абонент правомерно обладает частным ключом, соответствующим публичному ключу, который будет указан в сертификате;
 - e) будущий абонент обладает частным ключом, способным создавать цифровую подпись; и
 - f) публичный ключ, который будет указан в сертификате, может быть использован для проверки цифровой подписи, приложенной с помощью частного ключа, которым обладает будущий абонент.

Заверения по выдаче сертификата

30. 1) Выдавая сертификат, сертификационный орган заверяет любое лицо, которое разумно полагается на сертификат или цифровую подпись, которую можно проверить с помощью публичного ключа, указанного в сертификате, что сертификационный орган выдал сертификат в соответствии с любым применимым заявлением о практике сертификации, которое включено с помощью ссылки в сертификат или о котором было уведомлено полагающееся лицо.
- 2) В отсутствие такого заявления о практике сертификации сертификационный орган заверяет, что он подтвердил, что:
- a) сертификационный орган выполнил все применимые требования настоящего Закона при выдаче сертификата и, если сертификационный орган опубликовал сертификат или иным образом предоставил его в распоряжение такого доверяющего лица, что абонент, указанный в сертификате, акцептовал его;
 - b) абонент, идентифицированный в сертификате, обладает частным ключом, соответствующим публичному ключу, указанному в сертификате;
 - c) публичный ключ и частный ключ абонента представляют собой функционирующую пару ключей;
 - d) вся информация в сертификате является точной, если только сертификационный орган не заявил в сертификате, что точность конкретно оговоренной информации не подтверждается, или не указал на это с помощью включения в сертификат соответствующей ссылки; и
 - e) сертификационному органу неизвестно ни о каком имеющем существенное значение факте, который, если бы он был включен в сертификат, оказал бы неблагоприятное воздействие на надежность заверений согласно пунктам (a)-(d).
- 3) В тех случаях, когда имеется применимое заявление о практике сертификации, которое было включено посредством ссылки в сертификат или о котором было уведомлено полагающееся лицо, подраздел 2 применяется в той мере, в которой заверения не противоречат заявлению о практике сертификации.

Приостановление действия сертификата

31. Если сертификационный орган и абонент не договорились об ином, сертификационный орган, выдавший сертификат, приостанавливает действие сертификата в кратчайший возможный срок после получения просьбы от лица, которое, как это может разумно полагать сертификационный орган, является

- a) абонентом, указанным в сертификате;
- b) лицом, должным образом уполномоченным действовать от имени этого абонента; или
- c) лицом, действующим от имени этого абонента, который не может выйти на связь.

Аннулирование сертификата

32. Сертификационный орган аннулирует выданный им сертификат

- a) после получения просьбы об аннулировании от абонента, поименованного в сертификате, и подтверждения того, что лицо, обращающееся с просьбой об аннулировании, является абонентом или агентом абонента, уполномоченным обращаться с просьбой об аннулировании;
- b) после получения заверенной копии свидетельства о смерти абонента или по подтверждении на основании других доказательств факта смерти абонента; или
- c) по представлении документов, на основании которых осуществляется расформирование абонента, или по подтверждении на основании других доказательств, что абонент был расформирован или прекратил существование.

Аннулирование без согласия абонента

33. 1) Сертификационный орган аннулирует сертификат, независимо от согласия на это абонента, указанного в сертификате, если сертификационный орган подтверждает, что:

- a) какой-либо существенный факт, заверенный в сертификате, является ложным;
- b) какое-либо требование для выдачи сертификата не было выполнено;
- c) частный ключ или надежная система сертификационного органа были скомпрометированы таким образом, который существенно затрагивает надежность сертификата;
- d) абонент, являющийся физическим лицом, умер; или
- e) абонент, являющийся юридическим лицом, был расформирован, ликвидирован или иным образом прекратил существование.

2) По осуществлении такого аннулирования на иных основаниях, чем указанные в подразделе 1(d) или (e), сертификационный орган незамедлительно уведомляет об этом абонента, указанного в аннулированном сертификате.

Уведомление о приостановлении действия

34. 1) Незамедлительно по приостановлении действия сертификата сертификационным органом сертификационный орган публикует подписанное уведомление о приостановлении в месте для опубликования уведомлений о приостановлении действия, указанном в сертификате.

2) В тех случаях, когда указаны одно или более таких мест, сертификационный орган публикует подписанные уведомления о приостановлении во всех таких местах.

Уведомление об аннулировании

35. 1) Незамедлительно по аннулировании сертификата сертификационным органом сертификационный орган публикует подписанное уведомление об аннулировании в месте для опубликования уведомлений об аннулировании, указанном в сертификате.

2) В тех случаях, когда указаны одно или более таких мест, сертификационный орган публикует подписанные уведомления об аннулировании во всех таких местах.

Статья 12, пункты 2 и 3 - финансовая ответственность

Руководящие принципы ААА

3.14 Финансовая ответственность сертификационного органа, выполняющего установленные требования

Сертификационный орган, выполняющий настоящие Руководящие принципы и любые другие применимые законодательные или договорные нормы, не несет финансовой ответственности за любые убытки, которые

- 1) понесены абонентом сертификата, выданного этим сертификационным органом, или любым другим лицом или
- 2) причинены в результате доверия к сертификату, выданному сертификационным органом, к цифровой подписи, которую можно проверить с помощью публичного ключа, указанного в сертификате, или к информации, заверенной в таком сертификате или хранилище информации.

Проект директивы ЕССтатья 6. Финансовая ответственность

1. Государства-члены, как минимум, обеспечивают, что в результате публичной выдачи сертификата в качестве сертификата, отвечающего установленным требованиям, или в результате публичного гарантирования сертификата поставщик сертификационных услуг несет финансовую ответственность за ущерб, причиненный любому лицу, которое разумно полагается на сертификат, в связи с:

- a) точностью всей информации в сертификате, отвечающем установленным требованиям, в момент его выдачи;
- b) [...];
- c) гарантией того, что в момент выдачи сертификата лицо, идентифицированное в сертификате, отвечающем установленным требованиям, обладало данными для создания подписи, соответствующими данным для проверки подписи, приведенным или указанным в сертификате;
- d) гарантией того, что данные для создания подписи и данные для проверки подписи могут использоваться взаимодополняющим образом в случаях, когда поставщик сертификационных услуг готовит оба вида таких данных;

если только поставщик сертификационных услуг не докажет, что он не проявил небрежности.

1a. Государства-члены, как минимум, обеспечивают, что поставщик сертификационных услуг, публично выдавший сертификат в качестве сертификата, отвечающего установленным требованиям, несет финансовую ответственность за ущерб, причиненный любому лицу, которое разумно полагается на сертификат, в связи с нерегистрацией аннулирования сертификата, если только поставщик сертификационных услуг не докажет, что он не проявил небрежности.

3. Государства-члены обеспечивают, что поставщик сертификационных услуг может указать в сертификате, отвечающем установленным требованиям, ограничения на использование определенных сертификатов; эти ограничения должны быть понятными для третьих сторон. Поставщик сертификационных услуг не несет финансовой ответственности за ущерб, возникающий из неправомерного использования отвечающего установленным требованиям сертификата, который включает ограничения на его использование.

4. Государства-члены обеспечивают, что поставщик сертификационных услуг может указать в сертификате, отвечающем установленным требованиям, ограничение на стоимостной объем сделок, для которых может быть использован этот сертификат.

МиссуриРаздел 17.1

В результате указания в сертификате рекомендованного предела доверия выдающий сертификационный орган и акцептующий абонент рекомендует соответствующим лицам полагаться на сертификат только в том объеме, при котором общая сумма риска не превышает рекомендуемый предел доверия.

Раздел 17.2

Если обладающий лицензией сертификационный орган не отказывается от применения настоящего подраздела, обладающий лицензией сертификационный орган:

- 1) не несет финансовой ответственности за любые убытки, причиненные доверием к ложной или подделанной цифровой подписи абонента, если в отношении такой ложной или подделанной цифровой подписи сертификационный орган выполнил все материальные требования разделов 1-27 настоящего закона;
- 2) не несет финансовой ответственности в превышение суммы, указанной в сертификате в качестве рекомендованного предела доверия, в связи либо с:
 - a) убытками, причиненными доверием к неверному указанию в сертификате какого-либо факта, подтвердить который требуется обладающему лицензией сертификационному органу; либо
 - b) несоблюдением раздела 10 настоящего закона при выдаче сертификата;
- 3) несет финансовую ответственность только за прямые фактические убытки по любому иску о возмещении ущерба, причиненного доверием к сертификату, причем такие убытки не включают:
 - a) штрафные или заранее оцененные убытки;
 - b) убытки в связи с утраченными выгодой, экономией или возможностями; или
 - c) убытки в связи с причиненной болью или страданиями.

СингапурПределы финансовой ответственности для обладающих лицензией сертификационных органов

45. Если обладающий лицензией сертификационный орган не отказывается от применения настоящего раздела, обладающий лицензией сертификационный орган:

- a) не несет финансовой ответственности за любые убытки, причиненные доверием к ложной или подделанной цифровой подписи абонента, если в отношении такой ложной или подделанной цифровой подписи обладающий лицензией сертификационный орган выполнил требования настоящего Закона;
- b) не несет финансовой ответственности в превышение суммы, указанной в сертификате в качестве рекомендованного предела доверия, в связи либо с:

- i) убытками, причиненными доверием к неверному указанию в сертификате какого-либо факта, подтвердить который требуется обладающему лицензией сертификационному органу; или
- ii) несоблюдением разделов 29 и 30 при выдаче сертификата.

Статья 13. Признание иностранных сертификатов и подписей

1) При определении того, обладает ли - и в какой мере обладает - сертификат [подпись] юридической силой, не учитываются ни место выдачи сертификата [подписи], ни государство, в котором находится коммерческое предприятие эмитента.

Вариант А

2) Сертификаты, выданные иностранным сертифицирующим органом информации, признаются юридически эквивалентными сертификатам, выданным сертифицирующими органами информации, функционирующими на основании ... [законодательство принимающего государства], если практика иностранного сертифицирующего органа информации обеспечивает уровень надежности, по меньшей мере эквивалентный тому, который требуется от сертифицирующих органов информации на основании ... [законодательство принимающего государства]. [Такое признание может быть осуществлено путем опубликования соответствующего государственного решения либо путем заключения двустороннего или многостороннего соглашения между заинтересованными государствами.]

3) Подписи, отвечающие законодательству другого государства, касающемуся цифровых и других электронных подписей, признаются юридически эквивалентными подписям на основании ... [законодательство принимающего государства], если законодательство другого государства требует уровень надежности, по меньшей мере эквивалентный тому, который требуется для таких подписей на основании ... [законодательство принимающего государства]. [Такое признание может быть осуществлено путем опубликования соответствующего государственного решения либо путем заключения двустороннего или многостороннего соглашения с другими государствами.]

4) Независимо от положений предыдущего пункта, стороны коммерческих и других сделок могут оговорить, что в связи с представляемыми им сообщениями или подписями должны использоваться тот или иной конкретный сертифицирующий орган информации, класс сертифицирующих органов информации или класс сертификатов.

Вариант В

2) Сертификаты, выданные иностранным сертифицирующим органом информации, признаются юридически эквивалентными сертификатам, выданным сертифицирующими органами информации, функционирующими на основании ... [законодательство принимающего государства], если практика иностранного сертифицирующего органа информации обеспечивает уровень надежности, по меньшей мере эквивалентный тому, который требуется от сертифицирующих органов информации на основании ... [законодательство принимающего государства].

[3) Определение эквивалентности, упомянутое в пункте 2, может быть осуществлено путем опубликования соответствующего государственного решения либо путем заключения двустороннего или многостороннего соглашения с другими государствами.]

4) При определении эквивалентности учитываются следующие факторы:

- a) финансовые и людские ресурсы, включая наличие активов в пределах юрисдикции;
- b) надежность систем аппаратного и программного обеспечения;

- с) процедуры оформления сертификатов и рассмотрения заявок на сертификаты, а также хранения записей;
- d) наличие информации для [подписавшихся] [субъектов], идентифицированных в сертификатах, и для потенциальных полагающихся сторон;
- 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 действиям сертификационного органа, и законодательством принимающего государства.

Справочные документы ЮНСИТРАЛ

A/CN.9/454, пункт 173;
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.

Примечания

69. В проекте статьи 13 регулируются вопросы, которые на тридцать первой сессии Рабочей группы назывались вопросами "трансграничного признания" (см. A/CN.9/437, пункты 77-78). Пункт 1 основывается на предложении, которое было сделано на тридцать четвертой сессии Рабочей группы (A/CN.9/457, пункт 120) и которое заключалось в том, что Рабочая группа, возможно, пожелает рассмотреть вопрос о включении статьи, устанавливающей запрещение дискриминации в отношении сертификатов на основе места их выдачи.

70. Вариант А основывается на внесенном на тридцать второй сессии Рабочей группы предложении об объединении ряда пунктов (см. A/CN.9/446, пункты 197-204). В данном варианте в его нынешнем виде устанавливаются критерии, которые могут быть применены в принимающем государстве в целях признания сертификатов, выданных иностранными сертифицирующими органами информации, а также подписей, удовлетворяющих требованиям законодательства другого государства. В пункте 4 отражено общее мнение Рабочей группы о том, что за сторонами коммерческих и других сделок следует признать право выбирать конкретного сертифицирующего органа информации, класс сертифицирующих органов информации или класс сертификатов, которые они желают использовать в связи с получаемыми ими сообщениями или подписями. Ссылка на стороны коммерческих и других сделок будет включать правительственные учреждения, действующие в коммерческом качестве.

71. В варианте В содержится иллюстративный перечень критериев, которые должны приниматься во внимание при оценке надежности иностранных сертификатов.

Справочные национальные законодательные и другие тексты

Проект директивы ЕС

Статья 7. Международные аспекты

1. Государства-члены обеспечивают, чтобы сертификаты, которые публично выданы в качестве сертификатов, отвечающих установленным требованиям, поставщиком сертификационных услуг, предприятие которого расположено в

третьей стране, признавались юридически эквивалентными сертификатам, выданным поставщиком сертификационных услуг, предприятие которого расположено в пределах Европейского сообщества;

- a) если поставщик сертификационных услуг удовлетворяет требованиям, установленным в настоящей Директиве, и был аккредитован в контексте системы добровольной аккредитации, созданной в государстве - члене Европейского сообщества; или
- b) если поставщик сертификационных услуг, предприятие которого расположено в рамках Сообщества и который отвечает требованиям, установленным в настоящей Директиве, гарантирует сертификат; или
- c) если сертификат или поставщик сертификационных услуг признаются согласно режиму двустороннего или многостороннего соглашения между Сообществом и третьими странами или международными организациями.

2. В целях содействия трансграничным сертификационным услугам с третьими странами и юридическому признанию продвинутого электронных подписей, подготовленных в третьих странах, Комиссия, если это уместно, будет вносить предложения, направленные на достижение эффективного осуществления стандартов и международных соглашений, применимых к сертификационным услугам. В частности, и если это необходимо, она будет представлять предложения в Совет относительно надлежащих мандатов на проведение переговоров по двусторонним и многосторонним соглашениям с третьими странами и международными организациями. Совет принимает решения квалифицированным большинством голосов.

Германия

§ 15 Иностранные сертификаты

- 1) Цифровые подписи, которые могут быть проверены с помощью публичного подписывающего ключа, на который имеется иностранный сертификат другого государства - члена Европейского союза или другого договаривающегося государства Договора о Европейском экономическом пространстве, эквивалентны цифровым подписям на основании настоящего закона в той мере, в которой они демонстрируют эквивалентный уровень защиты.
- 2) Пункт 1 также применяется к другим государствам в той мере, в которой заключены надгосударственные или международные соглашения относительно признания сертификатов.

Иллинойс

Статья 25. Использование электронных подписей и записей Агентством штата

Раздел 25-115. Взаимоприменимость

В той мере, в которой это разумно с учетом обстоятельств, правила, принимаемые Департаментом центральных управленческих услуг или Агентством штата в отношении использования электронных записей или электронных подписей, составляются таким образом, который направлен на поощрение и содействие сочетаемости и взаимоприменимости с аналогичными требованиями, принятыми правительственными агентствами других штатов и федеральным правительством.

Сингапур

Часть X. Регулирование деятельности сертификационных органов

Признание иностранных сертификационных органов

43. Министр может посредством принимаемых в порядке регулирования актов предусмотреть, что Ревизор может осуществлять признание сертификационных органов за пределами Сингапура, которые отвечают установленным требованиям, для любых из нижеследующих целей:

- a) рекомендованный предел доверия, если таковой имеется, указанный в сертификате, выданном сертификационным органом;
- b) презумпция, упомянутая в разделах 20(b)(ii) [цифровые подписи при определенных обстоятельствах должны рассматриваться в качестве защищенных электронных подписей] и 21 [презумпция правильности сертификата, если он акцептуется абонентом].

Примечания

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

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

³Там же, пятьдесят третья сессия, Дополнение № 17 (A/53/17), пункт 208.