ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ

A

Генеральная Ассамблея

Distr.
LIMITED

A/CN.9/WG.IV/WP.84
8 December 1999

RUSSIAN
Original: ENGLISH

КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ
Рабочая группа по электронной торговле
Тридцать шестая сессия
Нью-Йорк, 14-25 февраля 1999 года

ПРОЕКТ ЕДИНООБРАЗНЫХ ПРАВИЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

Записка Секретариата

СОДЕРЖАНИЕ

V.99-90617

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 ссылки[1].

2. На тридцатой сессии (1997 год) Комиссии был представлен доклад Рабочей группы о работе ее тридцать первой сессии (A/CN.9/437). Рабочая группа сообщила Комиссии, что она достигла консенсуса в отношении важного значения и необходимости работы в направлении согласования норм права в этой области. Хотя она не приняла окончательного решения в отношении формы и содержания такой работы, Рабочая группа пришла к предварительному выводу о том, что практически можно подготовить проект единообразных правил по крайней мере по вопросам подписей в цифровой форме и сертификационных органов и, возможно, по связанным с этими вопросами проблемам. Рабочая группа напомнила о том, что наряду с подписями в цифровой форме и сертификационными органами в рамках будущей работы в области электронной торговли, возможно, также потребуется рассмотреть следующие темы: вопросы технических альтернатив криптографии публичных ключей; общие вопросы о функциях, выполняемых поставщиками услуг, являющимися третьими сторонами; и заключение контрактов в электронной форме (A/CN.9/437, пункты 156-157).

3. Комиссия одобрила выводы Рабочей группы и поручила ей подготовить единообразные правила по юридическим вопросам подписей в цифровой форме и сертификационных органов (далее в тексте - "проект единообразных правил об электронных подписях" или "единообразные правила"). В отношении конкретной сферы применения и формы 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, 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 рассмотрении 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 соблюдать сертификационные органы, особенно в случае необходимости трансграничной сертификации[2].

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 вопросам[3].

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 способов удостоверения подлинности. В единообразных правилах, как их представляет в настоящее время Рабочая группа, чрезмерно акцентируются способы цифровых подписей и - в сфере применения цифровых подписей - специальная практика 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. 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. Преобладало мнение о 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 от ЮНСИТРАЛ рекомендаций. 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 в том, 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 раздельных 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. Рабочая группа продолжила подготовку проекта единообразных правил на своей тридцать пятой сессии (Вена, сентябрь 1999 года) на основе записки (A/CN.9/WG.IV/WP.82), подготовленной Секретариатом. Доклад о работе этой сессии содержится в документе A/CN.9/465.

11. В настоящей записке содержатся пересмотренные проекты положений, подготовленные с учетом обсуждений и решений Рабочей группы, а также обсуждений и решений Комиссии на ее тридцать второй сессии, воспроизведенные выше (см. пункты 6-9 выше). Положения в новой редакции подчеркнуты. Для удобства пользования сводный текст проектов положений воспроизводится в виде приложения I к настоящей записке.

12. 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

13. В целях информации и сопоставления в настоящий документ 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;

- Руководящие принципы ААА — Американская ассоциация адвокатов, Научно-техническая секция, "Руководящие принципы в отношении цифровых подписей", 1996 год;

- Директива ЕС — Проект директивы Европейского парламента и Совета об общих рамках для электронных подписей; принят 30 ноября 1999 года (PE-CONS 3625/99);

- ГАЙДЕК Международная торговая палата, "Общая практика для международных торговых операций, заверенных в цифровой форме", 1997 год.

I. ОБЩИЕ ЗАМЕЧАНИЯ

14. 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.

15. 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.

16. Единообразные правила основываются на Типовом законе и призваны, в частности, отразить: принцип нейтральности с точки зрения носителей информации; недискриминационный подход в отношении функциональных эквивалентов традиционных понятий и практики, основанных на использовании бумажных документов, и широкое признание автономии сторон. Они предназначаются для использования в качестве как минимальных стандартов в "открытой" среде (т. е. когда стороны сносятся друг с другом с помощью электронных средств без предварительного согласия), так и субсидиарных правил в "закрытой" среде (т. е. когда стороны связаны уже существующими договорными нормами и процедурами, подлежащими соблюдению при передаче сообщений с помощью электронных средств).

17. 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 правового документа.

18. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли в преамбуле разъяснить цель единообразных правил, а именно содействие эффективному использованию электронных коммуникаций путем создания основы для защиты сообщений и придания письменным и электронным сообщениям равного статуса с точки зрения их правовых последствий.

19. На тридцать третьей сессии Рабочей группы были выражены сомнения в отношении приемлемости использования слов "с высокой степенью защиты" 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 слова "с высокой степенью защиты". На тридцать четвертой сессии (A/CN.9/457, пункт 39) было высказано мнение о том, что определение "электронной подписи с высокой степенью защиты", возможно, потребуется 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 электронных подписей с высокой степенью защиты 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 "электронной подписи с высокой степенью защиты", возможно, потребуется разъяснить. На тридцать пятой сессии Рабочей группы была выражена поддержка сохранению концепции "электронной подписи с высокой степенью защиты", которая, как это было описано, способна создать особенно большие возможности для обеспечения определенности в том, что касается использования конкретного вида электронных подписей, а именно применения цифровых подписей посредством инфраструктуры публичных ключей (ИПК). В ответ было указано, что концепция "электронной подписи с высокой степенью защиты" неоправданно усложняет структуру единообразных правил. Кроме того, концепция "электронной подписи с высокой степенью защиты" будет создавать возможности для неверного толкования, так как предполагает, что различные уровни технической надежности могут соответствовать в одинаковой мере разнообразному диапазону юридических последствий. Широко высказывалась обеспокоенность тем, что электронная подпись с высокой степенью защиты будет рассматриваться в качестве отдельной юридической концепции, а не в качестве термина, описывающего набор технических критериев, использование которых делает метод подписания особенно надежным. Рабочая группа, хотя она и отложила окончательное решение по вопросу о том, будет ли использоваться в единообразных правилах концепция "электронной подписи с высокой степенью защиты", в целом согласилась с тем, что при подготовке пересмотренного проекта единообразных правил для продолжения обсуждения на одной из будущих сессий, было бы полезно включить такой вариант проекта статьи, в котором не упоминалась бы эта концепция (A/CN.9/465, пункт 66).

20. С учетом этого проведенного обсуждения вопроса о необходимости в категории "электронных подписей с высокой степенью защиты" в настоящем пересмотренном проекте единообразных правил использован альтернативный подход, предлагаемый на рассмотрение Рабочей группы. Определение "электронной подписи с высокой степенью защиты" в проекте статьи 2(b) было заключено в квадратные скобки, но оно не используется ни в одном из материально-правовых положений единообразных правил. Где это возможно, соответствующие части этого определения включены в соответствующие положения. Цель этого 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 электронные подписи с высокой степенью защиты, с тем чтобы в единообразных правилах регулировалась только единая категория электронных подписей. Примечания, касающиеся возможного изменения определения включены в статью 2. Примечания, касающиеся конкретных предложений, приводятся в соответствующих статьях.

21. В соответствии с договоренностью Рабочей группы на ее тридцать пятой сессии настоящий пересмотренный проект единообразных правил основан на предположении, что ссылка на ситуации, "когда закон требует подписи", не ограничивается случаями, когда электронная подпись используется для удовлетворения императивного требования законодательства о том, что для придания некоторым документам юридической силы, их следует подписывать. Поскольку в законодательстве содержатся лишь немногие подобные требования в отношении документов, используемых для коммерческих сделок, практическим следствием такого неправильного толкования было бы неоправданное сужение сферы применения единообразных правил. В соответствии с этим толкованием слово "законодательство", принятое Комиссией в пункте 68 Руководства по принятию Типового закона (в соответствии с которым слово "законодательство" следует понимать как включающее не только статутное право или подзаконные акты, но также нормы, создаваемые судами, и другие процессуальные нормы"), Единообразные правила (и Типовой закон) призваны очень широко охватить использование электронных подписей, поскольку большинство документов, используемых в контексте коммерческих сделок, вероятно, на практике столкнется с требованиями доказательственного права относительно представления письменных доказательств (A/CN.9/465, пункт 67).

II. ПРОЕКТЫ СТАТЕЙ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

Статья 1. Сфера применения

Настоящие Правила применяются в тех случаях, когда электронные подписи используются в контексте* торговой** деятельности. Они не имеют преимущественной силы по отношению к любой правовой норме, предназначенной для защиты потребителей.

* Комиссия предлагает следующий текст для государств, которые, возможно, пожелают расширить сферу применения настоящих Правил:

"Настоящие Правила применяются в тех случаях, когда используются электронные подписи, за исключением следующих ситуаций: [...]".

** Термин "торговая" 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 о поставке товаров или услуг или обмене товарами или услугами; дистрибьюторские соглашения; торговое представительство и агентские отношения; факторинг; лизинг; строительство промышленных объектов; предоставление консультативных услуг; инжиниринг; купля/продажа лицензий; инвестирование; финансирование; банковские услуги; страхование; соглашения об эксплуатации или концессии; совместные предприятия и другие формы промышленного или предпринимательского сотрудничества; перевозка товаров и пассажиров по воздуху, морем, по железным и автомобильным дорогам.

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 36-42;
A/CN.9/WG.IV/WP.82, пункт 21;
A/CN.9/457, пункты 53-64.

Примечания

22. Вступительная формулировка проекта статьи 1 была пересмотрена с целью обеспечить ее соответствие тексту статьи 1 Типового закона (см. A/CN.9/465, пункт 38). Сноска(*) призвана отразить подход, аналогичный тому, который был принят в контексте Типового закона, в соответствии с которым "ничто в Типовом законе не должно препятствовать намерениям принимающего его государства расширить сферу действия Типового закона, с тем чтобы охватить виды использования электронной торговли за пределами коммерческой сферы" (Руководство по принятию Типового закона, пункт 26). На своей тридцать пятой сессии Рабочая группа постановила, что такой подход следует применить также и в отношении электронных подписей (там же, пункт 39).

Статья 2. Определения

Для целей настоящих Правил:

a) "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 метод, 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) "электронная подпись с высокой степенью защиты" означает электронную подпись, в отношении которой может быть продемонстрировано с помощью использования [какой-либо процедуры защиты] [какого-либо метода защиты], 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";]]

c) "сертификат" означает сообщение данных или иную запись, которая выдается сертификатором информации 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 электронная подпись с высокой степенью защиты 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 электронных подписей [с высокой степенью защиты].

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункт 42;
A/CN.9/WG.IV/WP.82, пункты 22-33;
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 A, B и C); и
A/CN.9/WG.IV/WP.71, пункты 52-60.

Примечания

23. На своей тридцать пятой сессии Рабочая группа постановила отложить рассмотрение содержащихся в проекте статьи 2 определений до материально-правовых положений единообразных правил (A/CN.9/465, пункт 42).

Определение "электронной подписи"

24. 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 метод, который может быть использован в отношении сообщения о данных]" включены для приведения формулировки определения в единообразных правилах в соответствие с формулировкой статьи 7 Типового закона.

Определение "электронной подписи с высокой степенью защиты"

25. На своей тридцать пятой сессии Рабочая группа обсудила вопрос использования в единообразных правилах концепции "электронной подписи с высокой степенью защиты". Была выражена поддержка сохранению концепции электронной подписи с высокой степенью защиты, которая, как это было описано, способна создать особенно большие возможности для обеспечения определенности в том, что касается использования конкретного вида электронных подписей, а именно применения цифровых подписей посредством инфраструктуры публичных ключей (ИПК). В ответ было указано, что концепция "электронной подписи с высокой степенью защиты" неоправданно усложняет структуру единообразных правил. Кроме того, концепция "электронной подписи с высокой степенью защиты" будет создавать возможности для неверного толкования, так как предполагает, что различные уровни технической надежности могут соответствовать в одинаковой мере разнообразному диапазону юридических последствий. Широко высказывалась обеспокоенность тем, что электронная подпись с высокой степенью защиты будет рассматриваться в качестве отдельной юридической концепции, а не в качестве термина, описывающего набор технических критериев, использование которых делает метод подписания особенно надежным. Рабочая группа, хотя она и отложила окончательное решение по вопросу о том, будет ли использоваться в единообразных правилах концепция "электронной подписи с высокой степенью защиты", в целом согласилась с тем, что при подготовке пересмотренного проекта единообразных правил для продолжения обсуждения на одной из будущих сессий, было бы полезно включить такой вариант проекта статьи, в котором не упоминалась бы эта концепция (A/CN.9/465, пункт 66).

26. В соответствии с решением, принятым Рабочей группой на ее тридцать четвертой сессии (A/CN.9/457, пункт 39), определение "электронной подписи с высокой степенью защиты" было пересмотрено: в него в квадратных скобках в качестве необходимой привязки электронной подписи с высокой степенью защиты 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 электронной подписи с высокой степенью защиты 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).

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

28. 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 подписывающего устройства (и, таким образом, потенциально является несанкционированной), не представляет собой электронной подписи с высокой степенью защиты. В результате такого толкования подобные подписи могут быть исключены из сферы действия некоторых статей единообразных правил, включая, например, проекты статей 8, 9 и 11. В частности, могут возникнуть сомнения относительно применимости тех частей проекта статьи 9, которые касаются ответственности за компрометацию подписывающих устройств.

29. Во-вторых, включение этих слов будет равнозначно установлению требования о том, что для того, чтобы какая-либо процедура защиты или какой-либо метод считались электронной подписью с высокой степенью защиты, эта процедура или метод должны создавать возможность продемонстрировать, что подпись была действительно создана и приложена обладателем подписывающего устройства. Поскольку некоторые технологии могут не предусматривать такой возможности, включение такого требования может предполагать необходимость в использовании - в сочетании с применением подписывающего

устройства - какого-либо способа идентификации личности, например, использования биометрики или какого-либо другого аналогичного способа.

30. Еще одним вопросом, который Рабочая группа, возможно, пожелает рассмотреть в контексте подпункта (b)(ii), является взаимосвязь между требованием "исключительного контроля" и проектом статьи 9, в котором предусматриваются обязательства "каждого" обладателя подписывающего устройства. Этот вопрос также возникает в связи с определением "обладателя подписи", которое рассматривается ниже.

31. В подпункте (b)(iii) слова "надежные доказательства" призваны обеспечить соответствие с терминологией статьи 8 Типового закона.

Определение "сертификата"

32. Определение термина "сертификат" было включено в единообразные правила по причине обеспечения полноты охвата. Это определение основывается на определении термина "сертификат личности", содержащегося 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", по следующей причине: концепция "личности" может представлять собой более объемное понятие, чем просто ссылку на имя обладателя подписывающего устройства 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, проводить различие между личностью и другими существенными характеристиками или ограничивать применение единообразных правил только теми ситуациями, при которых используются только сертификаты личности, указывающие имя обладателя подписывающего устройства, возможно, не потребуется. 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, pages 6-9.

33. Рабочая группа, возможно, пожелает рассмотреть вопрос об уместности использования слов "подтверждение личности", поскольку сертификат в действительности может не подтверждать личность обладателя подписывающего устройства, а идентифицировать обладателя подписывающего устройства в результате применения ряда процедур и удостоверять наличие связи между этой личностью и подписывающим устройством или публичным ключом, указанными в сертификате. Для обеспечения нейтральности единообразных правил с технологической точки зрения Рабочая группа, возможно, пожелает также рассмотреть вопрос об использовании такой, например, технологически нейтральной формулировки, как "подписывающее устройство" или "устройство для создания подписи", в качестве альтернативы словам "пара ключей", поскольку понятие "пара ключей" непосредственно связано 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"

34. Определение "сообщение данных" было включено в проект единообразных правил по причине обеспечения полноты охвата. Рабочая группа, возможно, пожелает рассмотреть вопрос о необходимости включения этого определения в контексте взаимосвязи единообразных правил и Типового закона.

Определение "обладателя подписи"

35. 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 "электронной подписи с высокой степенью защиты", приведенного выше, и проекта статьи 9, как на это указывается в пункте 30. С учетом предложения, сделанного на тридцать пятой сессии Рабочей группы, термин "обладатель подписи" был заменен повсеместно в тексте настоящей записки на термин "обладатель подписывающего устройства" (см. A/CN.9/465, пункты 78-82).

Определение "сертификатора информации"

36. Это определение Рабочая группа на ее предыдущей сессии не рассматривала и оно остается 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 побочной части деятельности организации. Принимая во внимание предложение, выдвинутое на тридцать пятой сессии Рабочей группы, термин "сертификатор информации" был заменен повсеместно в оставшейся части единообразных правил на термин "поставщик сертификационных услуг" (A/CN.9/465, пункт 125). Рабочая группа, возможно, пожелает принять решение относительно того, какую терминологию использовать.

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 помощи 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.

Директива 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;

2. "более защищенная электронная подпись" означает электронную подпись, которая отвечает следующим требованиям:
   а) она обладает уникальной связью с подписавшим;

b) она может идентифицировать подписавшего;
c) она создана при помощи средств, 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;

3. "подписавший" означает лицо, которое обладает устройством для создания подписи и действует от своего собственного имени или от имени лица или организации, которых оно представляет;
4. "данные для создания подписи" означает уникальные данные, такие, как коды или частные криптографические ключи, которые используются подписавшим при создании электронной подписи;
5. "устройство для создания подписи" означает конфигурированное программное или аппаратное обеспечение для оперирования данными при создании электронной подписи;
6. "устройство для создания защищенной подписи" означает устройство для создания подписи, которое отвечает требованиям, изложенным в приложении III;
7. "данные для проверки подписи" означает данные, такие, как коды или публичные криптографические ключи, которые используются при проверке электронной подписи;
8. "устройство для проверки подписи" означает конфигурированное программное или аппаратное обеспечение для оперирования данными для проверки подписи;
9. "сертификат" означает электронную аттестацию, которая позволяет установить связь между данными для проверки подписи и каким-либо лицом и которая подтверждает личность этого лица;
10. "сертификат, удовлетворяющий установленным требованиям" означает сертификат, который удовлетворяет требованиям, изложенным в Приложении I, и который обеспечивает поставщик сертификационных услуг, удовлетворяющий требованиям, изложенным в приложении II;
11. "поставщик сертификационных услуг" означает лицо или организацию, которые выдают сертификаты или предоставляют другие услуги, связанные с электронными подписями; [...].

ГАЙДЕК

VI. Глоссарий терминов
2. Сертификат
Аутентифицированное каким-либо лицом сообщение, которое аттестует точность фактов, относящихся к юридической действительности акта какого-либо иного лица.

4. Сертификатор
Лицо, которое выдает сертификат и тем самым аттестует точность факта, относящегося к 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.

Германия

§ 2 Определения
1) Цифровая подпись по смыслу настоящего закона представляет собой печать для скрепления цифровых данных, которая создана с помощью частного подписывающего ключа и которая позволяет при помощи использования соответствующего публичного ключа, к которому приложен сертификат подписывающего ключа, выданный сертификатором или органом согласно § 3, установить владельца ключа подписи и нефальсифицированный характер данных.
2) Сертификатором по смыслу настоящего закона является физическое или юридическое лицо, которое подтверждает принадлежность публичных подписывающих ключей физическим лицам и обладает лицензией на такую деятельность согласно § 4.
3) Сертификат по смыслу настоящего закона является цифровой аттестацией, которая касается подтверждения авторства 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 авторства).

Иллинойс

Статья 5. Электронные записи и подписи в целом
Раздел 5-105. Определения
"Сертификат" означает запись, в которой, как минимум: a) идентифицируется выдавший его сертификационный орган; b) именуется или иным образом идентифицируется абонент, или устройство, или электронный агент под контролем абонента; c) содержится публичный ключ, соответствующий частному ключу, находящемуся под контролем абонента; d) указывается срок действия; и e) 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, приписываемой 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 присоединяются 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. [Технологическая нейтральность] [Равный режим для электронных подписей]

Ни одно из положений настоящих Правил не применяется таким образом, чтобы исключать, ограничивать или лишать юридической силы любой метод [электронной подписи], [который удовлетворяет требованиям, указанным в статье 6(1) настоящих Правил] [который является как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности] [или иным образом отвечает требованиям применимого права].

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 43-48;
A/CN.9/WG.IV/WP.82, пункт 34;
A/CN.9/457, пункты 53-64.

Примечания

37. Проект статьи 3 призвать отразить некоторые предложения редакционного характера, сделанные в контексте тридцать пятой сессии Рабочей группы (A/CN.9/465, пункты 47-48). С учетом своего обсуждения проекта статьи 3 Рабочая группа, возможно, пожелает принять решение о том, следует ли в единообразных правилах пояснить, что любой метод, используемый или рассматриваемый в иных целях, чем создание функционального эквивалента законно значимой собственноручной подписи (т.е. метод, отвечающий требованиям проекта статьи 6 или в иных случаях отвечающий требованиям применимого права), не подпадает в сферу применения единообразных правил.

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.

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.

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 49-50;
A/CN.9/WG.IV/WP.82, пункт 35.

Примечания

38. На своей тридцать пятой сессии Рабочая группа в целом согласилась с основными положениями проекта статьи 4 (A/CN.9/465, пункт 50).

Статья 5. [Изменение по договоренности] [Автономия сторон] [Свобода договора]

Допускается отход от настоящих Правил или [изменение их действия] по договоренности за исключением тех случаев, когда настоящие Правила предусматривают иное или законодательство принимающего государства предусматривает иное.

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 51-61;
A/CN.9/WG.IV/WP.82, пункты 36-40;
A/CN.9/457, пункты 53-64.

Примечания

39. Текст проекта ститьи 5 отражает предложение, получившее широкую поддержку в Рабочей группе на ее тридцать пятой сессии (A/CN.9/465, пункт 59), в соответствии с которым обеспечивается свобода сторон в отношениях между собой в том, что касается отступления от содержащихся в настоящих Правилах положений или их изменения. Это положение об автономии касается только настоящих Правил и ни в коей мере не призвано затрагивать публичный порядок или императивные нормы, применимые к договорам, в частности положения, касающиеся недобросовестных договоров.

40. Фраза в квадратных скобках была включена в качестве возможной формулировки ближе соответствующей тексту статьи 6 Конвенции Организации Объединенных Наций о договорах международной купли-продажи товаров (далее именуемой "Конвенцией о купле-продаже товаров") на основании предложения Рабочей группы (там же, пункт 61).

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

1) В тех случаях, когда законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если использован [использована] [метод] [электронная

подпись], который [которая] является как надежным [надежной], так и соответствующим [соответствующей] цели, для которой сообщение данных было подготовлено или передано с учетом всех обстоятельств, включая любые соответствующие договоренности.

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

Вариант A

3) Считается, что [метод] [электронная подпись] является надежным для цели удовлетворения требования, упомянутого в пункте 1, если этот метод обеспечивает, что:

a) данные, используемые для создания электронной подписи, являются уникальными для обладателя подписывающего [создающего подпись] устройства в том контексте, в котором они используются;

b) обладатель подписывающего [создающего подпись] устройства [имеет] [имел в соответствующий момент времени] исключительный контроль над этим устройством;

c) электронная подпись связана с [информацией] [сообщением данных или с частью этого сообщения], к которому она относится [таким образом, который гарантирует целостность этой информации];

d) обладатель подписывающего [создающего подпись] устройства объективно идентифицируется в контексте [, в котором используется это устройство] [сообщение данных].

Вариант B

3) В отсутствие доказательств противного использование электронной подписи считается способным удостоверить:

a) что электронная подпись удовлетворяет стандарту надежности, изложенному в пункте 1;

b) личность предполагаемого обладателя подписи; и

c) что предполагаемый обладатель подписи согласился с информацией, к которой относится электронная подпись.

4) Презумпция в пункте 3 применяется только в тех случаях, если:

a) лицо, которое предполагает полагаться на электронную подпись, уведомляет предполагаемого обладателя подписи, что данное лицо будет полагаться на электронную подпись [в качестве эквивалента собственноручной подписи предполагаемого обладателя подписи] [в качестве доказательства элементов, перечисленных в пункте 3]; и

b) предполагаемый обладатель подписи не уведомляет в оперативном порядке лицо, которое отправляет уведомление в соответствии с подпунктом (a), о причинах, по которым нельзя полагаться на электронную подпись [в качестве эквивалента собственноручной подписи предполагаемого обладателя подписи] [в качестве доказательства элементов, перечисленных в пункте 3].

Вариант C

3) В отсутствие доказательств противного использование электронной подписи считается способным удостоверить:

a) что электронная подпись удовлетворяет стандарту надежности, изложенному в пункте 1;

b) личность предполагаемого обладателя подписи; и

c) что предполагаемый обладатель подписи согласился с информацией, к которой относится электронная подпись.

[4][5] Положения настоящей статьи не применяются в следующих случаях: [...].

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 62-82;
A/CN.9/WG.IV/WP.82, пункты 42-44;
A/CN.9/457, пункты 48-52;
A/CN.9/WG.IV/WP.80, пункты 11-12.

Примечания

41. В пункты 1 и 2 и в последний пункт проекта статьи 6 включены положения соответственно из статьи 7(1)(b), 7(2) и 7(3) Типового закона. Формулировка, подсказанная статьей 7(1)(a) Типового закона, уже включена в определение "электронной подписи" в проекте статьи 2(a). Однако в проекте статьи 2(a) описывается способ, который "может" быть использован для выполнения функций подписи, определение которой дано в статье 7(1)(a) Типового закона. Если Рабочая группа пожелает подчеркнуть, что главная цель пункта 1 состоит в том, чтобы охватить случай, когда любой тип электронной подписи (включая "незащищенные" способы аутентификации) используется для целей подписания (т.е. с намерением создать функциональный эквивалент собственноручной подписи), Рабочая группа, возможно, сочтет более целесообразным воспроизвести текст статьи 7(1) Типового закона в полном виде. Пункт 1 можно было бы сформулировать следующим образом:

"1) Если законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если:

a) [метод] [электронная подпись] используется для идентификации этого лица и указания на то, что это лицо согласно с информацией, содержащейся в сообщении данных; и

b) что [метод] [электронная подпись] является как надежным [надежной], так и соответствующим [соответствующей] цели, для которой сообщение данных было подготовлено или передано с учетом всех обстоятельств, включая любые соответствующие договоренности".

42. На тридцать пятой сессии Рабочей группы было высказано предположение о том, что, возможно, придется включить в проект статьи 6 положения следующего содержания: "Юридические последствия использования подписи в равной мере применимы к использованию электронных подписей" (см. A/CN.9/465, пункт 74). Рабочая группа, возможно, пожелает обсудить вопрос о том, в какой степени эта концепция равенства между собственноручной и электронной подписями должна быть в дальнейшем отражена в тексте единообразных правил, или вопрос о том, что, возможно, достаточно (и что будет больше соответствовать Типовому закону) указать в руководстве по применению (которое должно быть подготовлено позднее) на то, что при толковании пункта 1 следует иметь в виду, что цель этого положения заключается в обеспечении того, что в случаях, если использование собственноручной подписи повлечет за собой любые правовые последствия, аналогичные последствия должны вытекать из использования надежной электронной подписи.

43. Как указывается в докладе тридцать пятой сессии Рабочей группы (см. A/CN.9/465, пункт 64), в пункте 1 - в той степени, в какой в нем воспроизводится текст статьи 7(1) Типового закона, - речь идет об определении того, что представляет собой надежный метод получения подписи с учетом обстоятельств. Такое определение может вынести на основании статьи 7 Типового закона лишь суд или иное оценивающее факты лицо, действующее ex post, причем, возможно, уже по прошествии длительного срока после использования электронной подписи. Напротив, выгоды, которые, как ожидается, могут быть предоставлены с помощью единообразных правил в отношении некоторых способов, которые признаются в качестве особенно надежных, независимо от обстоятельств, при которых они используются, состоят в создании - в момент или до момента использования любого такого способа получения электронной подписи (ex ante) -определенностей (либо через презумпцию, либо через материально-правовую норму) в том, что использование такого признанного способа приведет к юридическим последствиям, эквивалентным последствиям собственноручной подписи. Именно в этом заключается цель пункта 3.

44. Вариант A пункта 3 основывается на тексте, предложенном и обсужденном на тридцать пятой сессии Рабочей группы (см. A/CN.9/465, пункты 78-82) для выражения объективных критериев технической надежности электронных подписей. В подпункте (c) выражена необходимая связь между подписью и подписываемой информацией с тем, чтобы избежать имплицитного толкования, что электронная подпись может применяться только в отношении полного содержания сообщения данных. Во многих случаях подписываемая информация будет фактически лишь долей информации, содержащейся в сообщении данных.

45. При обсуждении вариантов B и C Рабочая группа, возможно, пожелает пояснить в силу принципиальных соображений, должны ли единообразные правила при установлении критериев "надежности" электронной подписи охватывать исключительно вопросы технической надежности, предусматриваемые в рамках варианта A, или должны быть приняты во внимание другие факторы в качестве альтернативы или в качестве добавления к варианту A.

46. Вариант B вытекает из предложения, внесенного на тридцать пятой сессии Рабочей группы (см. A/CN.9/465, пункты 74-75). Если принятие варианта B подразумевает исключение любой связи между данным уровнем технической надежности, с одной стороны, и правовыми последствиями, которые вытекают из использования электронных подписей, с другой стороны, то действие пунктов 3 и 4 будет заключаться в том, чтобы создавать в пользу любого способа, который может быть использован для создания электронной подписи, то, что порой называют "презумпцией низкого уровня", т.е. презумпцию, которую предполагаемый обладатель подписи может легко опровергнуть с помощью простого заявления. Рабочая группа, возможно, пожелает принять решение по принципиальным соображениям относительно того, можно ли реально обязать пользователей электронных подписей обмениваться уведомлениями, предусматриваемыми в варианте B, и приведет ли такой обмен уведомлениями к ожидаемому уровню удобства для пользователей и заранее предсказуемой определенности в отношении правовых последствий, сопряженных с электронными подписями.

47. Вариант C появился в результате предложения, выдвинутого на тридцать пятой сессии Рабочей группы (см. A/CN.9/465, пункт 76). Вопреки варианту B в нем не предлагается механизм простого опровержения создаваемой им презумпции. Ввиду того, что "доказательство противного" может потребовать проведения тщательных и дорогостоящих исследований различных технических устройств и процедур, участвующих в создании электронной подписи, эффект варианта C будет заключаться в том, чтобы создать очень сильную презумпцию в отношении юридического действия любого способа, используемого для получения электронной подписи.

Справочные национальные законодательные и другие тексты

Директива ЕС

Статья 5
Правовые последствия электронных подписей

1. Государства-члены обеспечивают, чтобы более защищенные электронные подписи, которые основываются на сертификате, удовлетворяющем установленным требованиям, и которые создаются с помощью устройств создания защищенной подписи:

a) удовлетворяли правовым требованиям подписи в отношении данных, передаваемых в электронной форме, точно таким же образом, которым собственноручная подпись удовлетворяет этим требованиям в отношении данных, передаваемых на бумаге; и

b) допускались в качестве свидетельства в судебном процессе.

2. Государства-члены обеспечивают, чтобы электронная подпись не лишалась юридической силы и возможности признания в качестве свидетельства в судебном процессе лишь на том основании, что такая подпись:

- имеет электронную форму, или
- не основывается на сертификате, удовлетворяющем установленным требованиям, или
- не основывается на сертификате, удовлетворяющем установленным требованиям и выданном аккредитованным поставщиком сертификационных услуг, или
- не получена с помощью устройства для создания защищенной подписи.

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) Сообщение данных считается имеющим свою подлинную форму в тех случаях, когда в отношении этого сообщения данных использован [использована] [метод] [электронная подпись] [в соответствии со статьей 6], который [которая]:

a) представляет 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; и

b) при необходимости представления информации эта информация может быть продемонстрирована лицу, которому она должна быть представлена;

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

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 83-89;
A/CN.9/WG.IV/WP.82, пункт 45;
A/CN.9/457, пункты 48-52;
A/CN.9/WG.IV/WP.80, пункты 13-14.

Примечания

48. Текст проекта статьи 7 вытекает из решения, принятого Рабочей группой на ее тридцать пятой сессии (A/CN.9/465, пункт 89). Цель проекта статьи 7 заключается в том, чтобы подтвердить связь со статьей 8 Типового закона и соблюдение требований целостности текста. В его нынешней формулировке пункт 1 не подразумевает никакой связи между функцией сохранения целостности информации и функцией подписания в соответствии с проектом статьи 6. Независимость этих двух статей, которые могут применяться совместно или раздельно в отношении различных способов аутентификации, основывается на признании того факта, что в условиях применения бумажных документов соответствующие две функции могут также рассматриваться как отдельные.

Статья 8. Удовлетворение требований статей 6 и 7

Вариант A

1) [Орган или ведомство, назначенный (-ое) принимающим государством в качестве компетентного органа или ведомства] может определять, какие способы удовлетворяют требованиям статей 6 и 7.

2) Любое определение, вынесенное в соответствии с пунктом 1, должно соответствовать признанным международным стандартам.

Вариант B

1) Один или несколько методов электронной подписи могут быть определены в качестве методов, удовлетворяющих требованиям статей 6 и 7.

2) Любое определение, вынесенное в соответствии с пунктом 1, должно соответствовать признанным международным стандартам.

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 90-98;
A/CN.9/WG.IV/WP.82, пункт 46;
A/CN.9/457, пункты 48-52;
A/CN.9/WG.IV/WP.80, пункт 15.

Примечания

49. Цель проекта статьи 8 состоит в том, чтобы пояснить, что принимающее государство может назначить орган или ведомство, которые будут уполномочены выносить определения, какие конкретные технологии могут выиграть от презумпций, установленных в проектах статей 6 и 7. В соответствии с решением Рабочей группы, принятым на ее тридцать пятой сессии, проект статьи 8 не следует толковать таким образом, что пользователям запрещается, например, использовать способы, которые не были определены как способы, отвечающие требованиям надежности в проектах статей 6 и 7, если именно об этом стороны договорились между собой. Стороны должны обладать свободой доказывать, будь то в суде или в арбитраже, что избранный ими метод подписания удовлетворяет требованиям проектов статей 6 и 7, даже если в отношении этого способа заранее не было вынесено соответствующего определения. Проект статьи 8 следует рассматривать не как статью, рекомендующую государствам единственное средство обеспечения признания подписывающих технологий, а как статью, в которой указываются те ограничения, которые должны применяться в случае, если государства пожелают принять подобный подход. Эти вопросы, возможно, потребуется четко разъяснить, вероятнее всего, в руководстве по применению единообразных правил (см. A/CN.9/465, пункт 93).

50. Цель вариантов A и B заключается в том, чтобы поощрять государства обеспечивать положение, при котором определения, выносимые в соответствии с пунктом 1, соответствовали международным стандартам, если это уместно, содействуя тем самым установлению согласованной практики в том, что касается электронных подписей с высокой степенью защиты и трансграничного признания подписи. В варианте A говорится о возможном вмешательстве государства путем назначения органа или структуры власти, компетентных давать оценки технической надежности способов подписания (независимо от того, учрежден ли этот орган в качестве государственной или частной организации). Для того чтобы не переоценивать роль государства, в вынесении определений, упомянутых в пункте 1, вариант B оставляет открытой возможность для того, чтобы любой орган или любое ведомство, создаваемые для оценки технической надежности способов подписания, должен быть учрежден государством (в качестве государственного органа или частной организации) или исключительно промышленностью.

51. Выдвинутое в контексте тридцать пятой сессии Рабочей группы предложение (а именно, что "любое выносимое определение должно учитывать не только необходимость, чтобы определенные способы удовлетворяли требованиям проекта статей 6 и 7, но также степени или объему, в котором эти требования удовлетворяются"), не было отражено в пересмотренном варианте проекта статьи 8. Рабочая группа, возможно, пожелает пояснить, имеется ли в виду, что такое требование, как использование собственноручной подписи (или подготовка подлинного документа), может удовлетворяться только отчасти в отношении документа, обрабатываемого в электронной среде, что, как представляется, будет отступлением от подхода функционального эквивалента, принятого в ходе подготовки Типового закона и единообразных правил. Если намерение Рабочей группы заключается в том, чтобы просто отметить, что электронная подпись (или обеспечения целостности текста) не обязательно применяется к содержанию сообщения данных в целом, но что оно должно быть применимо только к выборной части информации, содержащейся в данном сообщении, то это указание можно легко обеспечить в руководстве по применению.

Статья 9. Ответственность обладателя подписывающего устройства

1) Каждый обладатель подписывающего устройства:

a) проявляет разумную заботливость для недопущения несанкционированного использования его подписывающего устройства;

b) уведомляет соответствующих лиц без ненадлежащих задержек, если:

i) обладателю подписывающего устройства известно, что подписывающее устройство было скомпрометировано; или

ii) обстоятельства, известные обладателю подписывающего устройства, обусловливают существенный риск того, что подписывающее устройство могло быть скомпрометировано;

c) [В тех случаях, когда для подтверждения подписывающего устройства используется сертификат,] [В тех случаях, когда подписывающее устройство требует использования сертификата,] проявляется разумная заботливость для обеспечения точности и полноты всех существенных заверений, сделанных обладателем подписывающего устройства, которые имеют отношение к [жизненному циклу] сертификата или которые должны быть включены в сертификат.

2) Обладатель подписывающего устройства несет ответственность за невыполнение требований пункта 1.

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 99-108;

A/CN.9/WG.IV/WP.82, пункты 50-55;
A/CN.9/457, пункты 65-98;
A/CN.9/WG.IV/WP.80, пункты 18-19.

Примечания

52. Рабочая группа на ее тридцать пятой сессии в целом одобрила проект статьи 9. В пункте 1 введена ссылка на "каждого" обладателя с целью отразить общую точку зрения, в соответствии с которой в ряде случаев, возможно, несправедливо предусматривать, чтобы каждый обладатель устройства нес ответственность за все убытки, которые могут быть причинены несанкционированным использованием устройства (например, в случае несанкционированного использования корпоративного подписывающего устройства, находящегося в распоряжении ряда сотрудников). Соответственно каждый обладатель должен нести ответственность только в той мере, в которой он лично не выполнил требования пункта 1 (см. A/CN.9/465, пункт 105).

53. В основу пункта 2 положено заключение, к которому пришла Рабочая группа на своей тридцать пятой сессии, относительно того, что, возможно, будет трудно достичь консенсуса в отношении того, какие последствия могут вытекать из ответственности обладателя подписывающего устройства. В зависимости от контекста использования электронной подписи такие последствия могут в рамках действующего законодательства иметь широкий диапазон: от последствий для обладателя подписывающего устройства, когда он связан условиями содержания сообщения, до ответственности за причиненный ущерб. Соответственно в пункте 2 лишь устанавливается принцип, в соответствии с которым обладатель подписывающего устройства должен нести ответственность за несоблюдение требований пункта 1 и на усмотрение права, применимого в каждом принимающем государстве вне действия единообразных правил остаются вопросы урегулирования правовых последствий, которые будут вытекать из такой ответственности (там же, пункт 108). Согласно другой точке зрения, правило, основанное на критерии предсказуемости убытков (соответствующее с положениям статьи 74 Конвенции о купле-продаже и вновь подтверждающее основополагающую норму, которая будет применяться во многих странах в рамках легко применимого законодательства), должно быть включено в проект статьи 9 (там же, пункт 107).

Справочные национальные законодательные и другие тексты

Пункт 1(a) - существенные заверения

Руководящие принципы ААА

4.2 Обязательства абонента
Все существенные 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.

ГАЙДЕК

VII. Аутентификация сообщения
7. Заверения сертификатору
Абонент должен точно представить сертификатору все факты, относящиеся к сертификату.

Иллинойс

Статья 20. Обязанности абонентов
Раздел 20-101. Получение сертификата
Все существенные 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 относящиеся к 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 существенные 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.

ГАЙДЕК

VII. Удостоверение сообщения

6. Охрана удостоверяющего устройства

Если лицо удостоверяет 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 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.

Пункт 2 - 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 соответствующему представлению факта абонентом;
2) несообщению абонентом соответствующего 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. Ответственность поставщика сертификационных услуг

1) Поставщик сертификационных услуг:

a) действует в соответствии с заверениями, которые он делает в отношении своей практики;

b) проявляет должную осмотрительность для обеспечения точности и полноты всех существенных заверений, сделанных поставщиком сертификационных услуг, которые относятся к жизненному циклу сертификата или которые включены в сертификат;

c) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить:

i) идентификационные данные поставщика сертификационных услуг;

ii) что лицо, которое идентифицировано в сертификате, обладает в соответствующий момент времени подписывающим устройством, указанным в сертификате;

iii) метод, использованный для идентификации обладателя подписывающего устройства;

iv) любые ограничения в отношении целей или стоимостного объема, в связи с которыми может использоваться подписывающее устройство; и

v) является ли подписывающее устройство действительным и не было ли оно скомпрометировано;

d) обеспечивает обладателей подписывающего устройства средством для направления уведомлений о том, что подписывающее устройство было скомпрометировано, и обеспечивает своевременное функционирование службы аннулирования;

e) использует надежные системы, процедуры и людские ресурсы при предоставлении своих услуг.

2) При вынесении определения в отношении надежности и степени надежности любых систем, процедур и людских ресурсов для целей подпункта (e) пункта 1 учитываются следующие факторы:

a) финансовые и людские ресурсы, в том числе наличие активов в пределах юрисдикции:

b) надежность систем аппаратного и программного обеспечения;

c) процедуры для обработки сертификатов и заявок на сертификаты и хранение записей;

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

e) регулярность и пределы аудита, проводимого независимым органом;

f) наличие заявления, сделанного государством, аккредитующим органом или поставщиком сертификационных услуг в отношении соблюдения или наличия вышеуказанных положений;

g) подсудность судам принимающего государства; и

h) степень расхождения между правом, применимым к поведению поставщика сертификационных услуг, и правом принимающего государства.

3) Сертификат устанавливает:

a) идентификационные данные поставщика сертификационных услуг;

b) что лицо, которое идентифицируется в сертификате, обладает в соответствующий момент времени подписывающим устройством, указанным в сертификате;

c) что подписывающее устройство было действительным на дату или до даты выдачи сертификата;

d) любые ограничения целей или стоимостного объема, в связи с которыми может использоваться сертификат; и

e) любое ограничение масштаба или объема финансовой ответственности, с которым соглашается поставщик сертификационных услуг в отношении любого лица.

Вариант X

4) Поставщик сертификационных услуг несет финансовую ответственность за невыполнение требований пункта 1.

5) Финансовая ответственность поставщика сертификационных услуг не может превышать ущерба, который поставщик сертификационных услуг предвидел или должен был предвидеть на момент неисполнения с учетом фактов или обстоятельств, которые поставщику сертификационных услуг были известны или должны были быть известны в качестве возможных последствий несоблюдения [невыполнения обязательств [обязанностей] в отношении] [требований] пункта 1.

Вариант Y

4) Поставщик сертификационных услуг несет финансовую ответственность за невыполнение требований пункта 1.

5) При оценке ущерба во внимание принимаются следующие факторы:

a) затраты на получение сертификата;

b) характер сертифицируемой информации;

c) наличие и степень любого ограничения цели, для которой может использоваться сертификат;

d) наличие любого заявления, ограничивающего масштаб или степень финансовой ответственности поставщика сертификационных услуг; и

e) любое действие полагающейся стороны, способствовавшее убыткам.

Вариант Z

4) Если ущерб был причинен в результате неверного или порочного сертификата, поставщик сертификационных услуг несет финансовую ответственность за убытки, понесенные либо:

a) стороной, вступившей в договорные отношения с поставщиком сертификационных услуг с целью получения сертификата; или

b) любым лицом, которое разумно полагается на сертификат, выданный поставщиком сертификационных услуг.

5) Поставщик сертификационных услуг не несет финансовой ответственности согласно пункту 2:

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

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

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 123-142 (проект статьи 12);
A/CN.9/WG.IV/WP.82, пункты 59-68 (проект статьи 12);
A/CN.9/457, пункты 108-119;
A/CN.9/WG.IV/WP.80, пункты 22-24.

Примечания

54. Проект статьи 10 (бывший проект статьи 12) был пересмотрен в соответствии с решениями Рабочей группы, принятыми на ее тридцать пятой сессии.

55. Рабочая группа на своей предыдущей сессии в целом приняла существо пункта 1, за исключением небольших редакционных изменений. Пункт 2 появился в результате внесенного на этой сессии предложения о том, что характеристики сертификатора информации, как они описываются в проекте статьи 13, должны учитываться не только в отношении иностранных юридических лиц, но должны применяться в равной мере и к внутренним поставщикам сертификационных услуг (A/CN.9/465, пункт 136).

56. Пункт 3 появился в результате предложения, к которому Рабочая группа на своей предыдущей сессии также отнеслась с большим интересом и в соответствии с которым в проекте статьи 12 следует установить дополнительное правило, оговаривающее минимальные параметры содержания сертификата (там же, пункт 135). Хотя элементы, необходимые для изложения в сертификате, перечислены в отдельном пункте, едва ли целесообразно сохранять пункт 1(c) и пункт 3 в качестве отдельных положений. Рабочая группа, возможно, пожелает пояснить, следует ли эти два положения объединить, предположительно в рамках подпункта 1(c), который мог бы начинаться со следующих слов: "указывает в каждом сертификате ...".

57. Пункты 4 и 5 касаются финансовой ответственности поставщика сертификационных услуг.

58. В пункте 4 вариантов X и Y устанавливается правило, в соответствии с которым поставщик сертификационных услуг несет ответственность за несоблюдение обязательств или обязанностей, перечисленных в пункте 1, но оставляет на усмотрение национального права принятие решения о том, какие последствия могут возникнуть в результате этого невыполнения.

59. В пункте 5 варианта X устанавливается правило предсказуемости ущерба на основе статьи 74 Конвенции о купле-продаже. Действие этого пункта направлено на ограничение объема любой финансовой ответственности поставщика сертификационных услуг, которая может возникнуть согласно пунктам 1 и 2. В варианте Y пункт 5 основывается на предложении, внесенном на тридцать пятой сессии Рабочей группы (A/CN.9/465, пункт 140), в соответствии с которым в единообразных правилах - не затрагивая действия внутреннего законодательства - можно предусмотреть перечень факторов, которые должны учитываться при применении внутреннего законодательства к поставщикам сертификационных услуг.

60. Вариант Z на тридцать пятой сессии Рабочей группы не обсуждался. В его основе лежит мысль, которая широко высказывалась на тридцать четвертой сессии Рабочей группы (A/CN.9/457, пункт 115), что было бы целесообразно подготовить единообразное правило, выходящее за рамки простой ссылки на применимое право и устанавливающее общую норму ответственности за небрежность при условии возможных договорных исключений (при условии, что это ограничение не будет явно несправедливым) и при условии, что поставщик сертификационных услуг освобождается от ответственности, если он докажет, что выполнил обязательство по пункту 1. В пункте 4 варианта Z рассматривается вопрос о том, перед кем может нести финансовую ответственность поставщик сертификационных услуг. В пункте 5 предусматривается правило, разрешающее поставщику сертификационных услуг полагаться на любое ограничение финансовой ответственности, предусмотренное в сертификате, или доказывать, что он не проявил небрежности или что он принял все разумные меры для недопущения убытков (A/CN.9/WG.IV/WP.82, пункт 67).

Справочные национальные законодательные и другие тексты

Пункты 1, 2 и 3 - 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 существенные заявления о практике сертификации, а также информацию об уведомлении об аннулировании и приостановлении действия сертификата сертификационного 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 сертификационного органа.

3) [...]

4) В случае события, имеющего существенные и негативные последствия для надежной системы сертификационного органа или его сертификата сертификационного органа, сертификационный 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 сертификационного органа в сертификате

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

1) сертификационный орган при выдаче сертификата выполнил все применимые требования настоящих Руководящих принципов и, если сертификационный 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 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.

Кроме того, сертификационный орган заверяет, что в сертификате не опущены никакие известные существенные 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 сертификационным органом и абонентом, сертификационный орган должен приостановить действие сертификата в кратчайший возможный срок после получения просьбы от лица, которое, как это может разумно полагать сертификационный 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.

Директива 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;

c) обеспечить возможность установления даты и времени выдачи или аннулирования сертификата;

d) 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;

e) 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;

f) использовать надежные системы и продукты, которые защищены от модификации и которые должны обеспечивать техническую и криптографическую безопасность поддерживаемых ими процессов;

g) 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;

h) 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;

i) регистрировать всю соответствующую информацию, касающуюся сертификата, отвечающего установленным требованиям, в течение надлежащего срока, в частности, для представления доказательств сертификации для целей юридических процедур. Такую регистрацию можно вести электронным способом;

j) не хранить или не копировать данных для создания подписи лица, которому поставщик сертификационных услуг предлагает услуги по управлению использованием ключа;

k) 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;

l) 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.

ГАЙДЕК

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) сертификатор подтверждает, что существенный факт, заверенный в сертификате, является ложным;

b) сертификатор 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 сертификатором сертификатор должен сделать надлежащее уведомление об аннулировании или приостановлении действия.

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 сертификатор 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 сертификатор 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 сертификатором 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, потребуется 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 сертификатор прекращает свои операции и их осуществление не продолжается каким-либо другим сертификатором, 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.

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
B) 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
a) 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.
b) 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

a) 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 аннулирования 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.

b) 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.

Пункты 4 и 5 - 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 ЕС

Статья 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, при условии, что это ограничение признают третьи стороны. Поставщик сертификационных услуг не несет финансовой ответственности за ущерб, причиненный в результате превышения этого максимального предела.

5. Положения пунктов 1-4 не противоречат положениям Директивы Совета 93/13/ЕЕС от 5 апреля 1993 года о недобросовестных условиях, содержащихся в договорах с потребителями.

Миссури

Раздел 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.

Сингапур

Пределы 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 11. Доверие к электронным подписям

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

2) [При определении того, является ли доверие разумным,] [При определении того, являлось ли поведение лица, положившегося на электронную подпись, разумным,] учитывается, если это уместно, следующее:

a) характер основной сделки, подтвердить которую предполагалось с помощью электронной подписи;

b) предприняла ли полагающаяся сторона надлежащие шаги для определения надежности электронной подписи;

c) предприняла ли полагающаяся сторона шаги для выяснения того, была ли электронная подпись подкреплена сертификатом;

d) было ли полагающейся стороне известно или должно было быть известно, что электронное подписывающее устройство было скомпрометировано или аннулировано;

e) любое соглашение или практика в отношениях между полагающейся стороной и абонентом или любой другой торговый обычай, который может быть применим;

f) любой другой соответствующий фактор.

Статья 12. Доверие к сертификатам

1) Лицо не имеет права полагаться на информацию в сертификате в той мере, в которой такое поведение не является разумным.

2) [При определении того, является ли доверие разумным,] [При определении того, являлось ли поведение лица, полагавшегося на информацию в сертификате, 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 или приостановленных сертификатов, когда это уместно;

c) любое соглашение или практика, существующие или существовавшие в соответствующий момент времени в отношениях между полагающейся стороной и поставщиком сертификационных услуг или абонентом, или любой торговый обычай, который может быть применим;

d) любые другие соответствующие факторы.

Вариант A

3) Если доверие к электронной подписи является неразумным в обстоятельствах, учитывающих факторы в пункте 1, полагающаяся сторона принимает на себя риск того, что подпись является недействительной.

Вариант B

3) Если доверие к подписи является неразумным в обстоятельствах, учитывающих факторы в пункте 1, полагающаяся сторона не имеет никаких претензий к обладателю подписывающего устройства или поставщику сертификационных услуг.

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 109-122 (проекты статей 10 и 11);
A/CN.9/WG.IV/WP.82, пункты 56-58 (проекты статей 10 и 11);
A/CN.9/457, пункты 99-107;
A/CN.9/WG.IV/WP.80, пункты 20-21.

Примечания

61. Проекты статей 11 и 12, в которых соответственно рассматриваются вопросы разумного доверия к электронным подписям и сертификатам, подверглись небольшим редакционным изменениям с учетом их обсуждений Рабочей группой на ее тридцать пятой сессии. Хотя на тридцать четвертой сессии Рабочей группы преобладало мнение, что в единообразные правила должны быть включены положения, касающиеся обязательств стороны, которая намеревается полагаться на сертификат, на тридцать пятой сессии были высказаны сомнения относительно практической пользы от использования понятия "доверие", которое касается как сообщения, так и подписи и в связи с которым могут возникнуть трудные вопросы при соприкосновении с обязательственным правом и необходимостью распределять риски (см. A/CN.9/465, пункт 111). Рабочая группа, возможно, пожелает принять решение по принципиальному вопросу в отношении того, следует ли в единообразных правилах специально устанавливать обязательства для полагающихся сторон. Если статьи 11 и 12 понимать как устанавливающие обязательства для полагающихся сторон, то последствия невыполнения этих обязательств, возможно, потребуется обсудить

дополнительно. Если статьи 11 и 12 понимаются как устанавливающие лишь "кодекс поведения" без уточнения последствий несоблюдения указанного поведения (см. A/CN.9/465, пункт 113), то такие предложения об установлении кодекса поведения для полагающейся стороны, возможно, целесообразнее включить в пояснительный документ, например, в руководство по применению единообразных правил.

62. Варианты A и B, которые оба строятся на предположении о том, что единообразные правила должны касаться правовых последствий, которые могут вытекать из непроявления полагающейся стороной должной заботливости при оценке надежности электронной подписи (независимо от того, подкрепляется ли такая электронная подпись сертификатом или не подкрепляется), призваны отразить два предложения, выдвинутые в этой связи на тридцать пятой сессии Рабочей группы (A/CN.9/465, пункт 117).

63. Рабочая группа, возможно, пожелает подробнее рассмотреть связь между проектами статей 11 и 12, с одной стороны, и проектом статьи 6, с другой стороны.

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 аутентификации 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.

ГАЙДЕК

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 сертификатор 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 13. Признание иностранных сертификатов и электронных подписей

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

2) Сертификаты, выданные иностранным поставщиком сертификационных услуг, признаются юридически эквивалентными сертификатам, выданным поставщиками сертификационных услуг, функционирующим на основании ... [законодательство принимающего государства], если практика иностранных поставщиков сертификационных услуг обеспечивает уровень надежности, по меньшей мере эквивалентный тому, который требуется от поставщиков сертификационных услуг 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 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) При определении эквивалентности учитываются, если это уместно, [факторы в пункте 2 статьи 10] [следующие факторы:

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

b) надежность систем аппаратного и программного обеспечения;

c) процедуры оформления сертификатов и рассмотрения заявлений на сертификаты и хранение 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 ведомства относительно соблюдения или наличия вышеизложенного;

g) подсудность судам принимающего государства; и

h) степень расхождения между законодательством, применимым к действиям сертификационного органа, и законодательством принимающего государства.

5) Независимо от положений пунктов 2 и 3 стороны коммерческих и других сделок могут оговорить, что в связи с представляемыми им сообщениями или подписями должен использоваться тот или иной конкретный поставщик сертификационных услуг, класс поставщиков сертификационных услуг и класс сертификатов.

6) В тех случаях, когда, независимо от положений пунктов 2 и 3, стороны соглашаются между собой в отношении использования электронных подписей и сертификатов, [такое соглашение признается достаточным для цели трансграничного признания]. [При определении того, обладает ли - и в какой мере обладает - электронная подпись или сертификат юридической силой, учитывается любое соглашение между сторонами сделки, в которой используется эта подпись или этот сертификат.]

Справочные документы ЮНСИТРАЛ

A/CN.9/465, пункты 21-35;
A/CN.9/WG.IV/WP.82, пункты 69-71;
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

64. Хотя на тридцать пятой сессии Рабочей группы в целом поддержку получил изложенный в пункте 1 принцип недискриминационного подхода, были высказаны сомнения в отношении целесообразности ссылки на страну происхождения. Было выражено мнение, что ссылка на страну происхождения приводит к излишнему сужению положения о недискриминации и оставляет открытой возможность для дискриминации по ряду других оснований, что было бы нежелательным. Было также высказано мнение, что на самом деле могут быть случаи, когда страна происхождения, подписи или сертификата имеет важное значение для вопроса признания. Однако никакой поддержки не получило предложение заменить нынешнюю формулировку, в соответствии с которой "не учитывается" страна происхождения, на формулировку, в соответствии с которой определение юридической силы электронной подписи не должно основываться "только" на стране происхождения (см. A/CN.9/465, пункты 23-24). Рабочая группа, возможно, пожелает принять принципиальное решение по вопросу о том, следует ли уточненное положение, в котором сформулирован принцип недискриминации, включить в проект статьи 13 или разъяснение этого принципа следует поместить в качестве ссылки более общего характера в преамбулу или в руководство по применению единообразных правил.

65. Пункты 2, 3, 4 и 5 были в целом согласованы Рабочей группой на ее предыдущей сессии как положения, устанавливающие надлежащее правило признания иностранных сертификатов и подписей (там же, пункт 34). Что касается факторов, перечисленных в пункте 4, то перекрестная ссылка на проект статьи 10, возможно, является достаточной, если эти же самые факторы используются для определения надежности систем, используемых внутренними поставщиками сертификационных услуг. Пункт 5 отражает общую точку зрения Рабочей группы на то, что сторонам коммерческих и других сделок следует предоставить право выбора конкретного поставщика сертификационных услуг, класса поставщиков сертификационных услуг или класса сертификатов, которыми они желают воспользоваться в связи с сообщениями или подписями, которые они получают. Ссылка на стороны коммерческих и других сделок предполагает охват государственных учреждений, выступающих в качестве коммерческих сторон.

66. Пункт 6 содержит предложения, выражающие принятое Рабочей группой на ее тридцать пятой сессии решение о том, что проект статьи 13 должен предусматривать признание договоренностей между заинтересованными сторонами в отношении использования определенных типов электронных подписей или сертификатов в качестве достаточных оснований для трансграничного признания (в отношениях между сторонами) таких согласованных подписей или сертификатов (A/CN.9/465, пункт 34).

67. Рабочая группа, возможно, пожелает принять принципиальное решение о том, следует ли в проекте статьи 13 охватить как сертификаты, так и подписи.

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 продвинутых 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. Взаимопременимость

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 взаимопременимости 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].

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 аутентификации 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.

ГАЙДЕК

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 сертификатор 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.

Приложение I. ПРОЕКТ ЕДИНООБРАЗНЫХ ПРАВИЛ ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

(Сводный текст проектов статей 1-13 в том виде, в котором они были рассмотрены в части II настоящей записки)

Статья 1. Сфера применения

Настоящие Правила применяются в тех случаях, когда электронные подписи используются в контексте* торговой** деятельности. Они не имеют преимущественной силы по отношению к любой правовой норме, предназначенной для защиты потребителей.

* Комиссия предлагает следующий текст для государств, которые, возможно, пожелают расширить сферу применения настоящих Правил:

"Настоящие Правила применяются в тех случаях, когда используются электронные подписи, за исключением следующих ситуаций: [...]".

** Термин "торговая" 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 о поставке товаров или услуг или обмене товарами или услугами; дистрибьюторские соглашения; торговое представительство и агентские отношения; факторинг; лизинг; строительство промышленных объектов; предоставление консультативных услуг; инжиниринг; купля/продажа лицензий; инвестирование; финансирование; банковские услуги; страхование; соглашения об эксплуатации или концессии; совместные предприятия и другие формы промышленного или предпринимательского сотрудничества; перевозка товаров и пассажиров по воздуху, морем, по железным и автомобильным дорогам.

Статья 2. Определения

Для целей настоящих Правил:

a) "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 метод, 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) "электронная подпись с высокой степенью защиты" означает электронную подпись, в отношении которой может быть продемонстрировано с помощью использования [какой-либо процедуры защиты] [какого-либо метода защиты], 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";]]

c) "сертификат" означает сообщение данных или иную запись, которая выдается сертификатором информации 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 электронная подпись с высокой степенью защиты 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 электронных подписей [с высокой степенью защиты].

Статья 3. [Технологическая нейтральность] [Равный режим для электронных подписей]

Ни одно из положений настоящих Правил не применяется таким образом, чтобы исключать, ограничивать или лишать юридической силы любой метод [электронной подписи], [который удовлетворяет требованиям, указанным в статье 6(1) настоящих Правил] [который является как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности] [или иным образом отвечает требованиям применимого права].

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.

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.

Статья 5. [Изменение по договоренности] [Автономия сторон]
[Свобода договора]

Допускается отход от настоящих Правил или [изменение их действия] по договоренности за исключением тех случаев, когда настоящие Правила предусматривают иное или законодательство принимающего государства предусматривает иное.

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

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

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

Вариант A

3) Считается, что [метод] [электронная подпись] является надежным для цели удовлетворения требования, упомянутого в пункте 1, если этот метод обеспечивает, что:

a) данные, используемые для создания электронной подписи, являются уникальными для обладателя подписывающего [создающего подпись] устройства в том контексте, в котором они используются;

b) обладатель подписывающего [создающего подпись] устройства [имеет] [имел в соответствующий момент времени] исключительный контроль над этим устройством;

c) электронная подпись связана с [информацией] [сообщением данных или с частью этого сообщения], к которому она относится [таким образом, который гарантирует целостность этой информации];

d) обладатель подписывающего [создающего подпись] устройства объективно идентифицируется в контексте [, в котором используется это устройство] [сообщение данных].

Вариант B

3) В отсутствие доказательств противного использование электронной подписи считается способным удостоверить:

a) что электронная подпись удовлетворяет стандарту надежности, изложенному в пункте 1;

b) личность предполагаемого обладателя подписи; и

c) что предполагаемый обладатель подписи согласился с информацией, к которой относится электронная подпись.

4) Презумпция в пункте 3 применяется только в тех случаях, если:

a) лицо, которое предполагает полагаться на электронную подпись, уведомляет предполагаемого обладателя подписи, что данное лицо будет полагаться на электронную подпись [в качестве эквивалента собственноручной подписи предполагаемого обладателя подписи] [в качестве доказательства элементов, перечисленных в пункте 3]; и

b) предполагаемый обладатель подписи не уведомляет в оперативном порядке лицо, которое отправляет уведомление в соответствии с подпунктом (a), о причинах, по которым нельзя полагаться на электронную подпись [в качестве эквивалента собственноручной подписи предполагаемого обладателя подписи] [в качестве доказательства элементов, перечисленных в пункте 3].

Вариант C

3) В отсутствие доказательств противного использование электронной подписи считается способным удостоверить:

a) что электронная подпись удовлетворяет стандарту надежности, изложенному в пункте 1;

b) личность предполагаемого обладателя подписи; и

c) что предполагаемый обладатель подписи согласился с информацией, к которой относится электронная подпись.

[4][5] Положения настоящей статьи не применяются в следующих случаях: [...].

[Статья 7. Презумпция наличия подлинника

1) Сообщение данных считается имеющим свою подлинную форму в тех случаях, когда в отношении этого сообщения данных использован [использована] [метод] [электронная подпись] [в соответствии со статьей 6], который [которая]:

a) представляет 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; и

b) при необходимости представления информации эта информация может быть продемонстрирована лицу, которому она должна быть представлена;

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

Статья 8. Удовлетворение требований статей 6 и 7

Вариант A

1) [Орган или ведомство, назначенный (-ое) принимающим государством в качестве компетентного органа или ведомства] может определять, какие способы удовлетворяют требованиям статей 6 и 7.

2) Любое определение, вынесенное в соответствии с пунктом 1, должно соответствовать признанным международным стандартам.

Вариант B

1) Один или несколько методов электронной подписи могут быть определены в качестве методов, удовлетворяющих требованиям статей 6 и 7.

2) Любое определение, вынесенное в соответствии с пунктом 1, должно соответствовать признанным международным стандартам.

Статья 9. Ответственность обладателя подписывающего устройства

1) Каждый обладатель подписывающего устройства:

a) проявляет разумную заботливость для недопущения несанкционированного использования его подписывающего устройства;

b) уведомляет соответствующих лиц без ненадлежащих задержек, если:

i) обладателю подписывающего устройства известно, что подписывающее устройство было скомпрометировано; или

ii) обстоятельства, известные обладателю подписывающего устройства, обусловливают существенный риск того, что подписывающее устройство могло быть скомпрометировано;

c) [В тех случаях, когда для подтверждения подписывающего устройства используется сертификат,] [В тех случаях, когда подписывающее устройство требует использования сертификата,] проявляется разумная заботливость для обеспечения точности и полноты всех существенных заверений, сделанных обладателем подписывающего устройства, которые имеют отношение к [жизненному циклу] сертификата или которые должны быть включены в сертификат.

2) Обладатель подписывающего устройства несет ответственность за невыполнение требований пункта 1.

Статья 10. Ответственность поставщика сертификационных услуг

1) Поставщик сертификационных услуг:

a) действует в соответствии с заверениями, которые он делает в отношении своей практики;

b) проявляет должную осмотрительность для обеспечения точности и полноты всех существенных заверений, сделанных поставщиком сертификационных услуг, которые относятся к жизненному циклу сертификата или которые включены в сертификат;

c) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить:

i) идентификационные данные поставщика сертификационных услуг;

ii) что лицо, которое идентифицировано в сертификате, обладает в соответствующий момент времени подписывающим устройством, указанным в сертификате;

iii) метод, использованный для идентификации обладателя подписывающего устройства;

iv) любые ограничения в отношении целей или стоимостного объема, в связи с которыми может использоваться подписывающее устройство; и

v) является ли подписывающее устройство действительным и не было ли оно скомпрометировано;

d) обеспечивает обладателей подписывающего устройства средством для направления уведомлений о том, что подписывающее устройство было скомпрометировано, и обеспечивает своевременное функционирование службы аннулирования;

e) использует надежные системы, процедуры и людские ресурсы при предоставлении своих услуг.

2) При вынесении определения в отношении надежности и степени надежности любых систем, процедур и людских ресурсов для целей подпункта (e) пункта 1 учитываются следующие факторы:

a) финансовые и людские ресурсы, в том числе наличие активов в пределах юрисдикции:

b) надежность систем аппаратного и программного обеспечения;

c) процедуры для обработки сертификатов и заявок на сертификаты и хранение записей;

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

e) регулярность и пределы аудита, проводимого независимым органом;

f) наличие заявления, сделанного государством, аккредитующим органом или поставщиком сертификационных услуг в отношении соблюдения или наличия вышеуказанных положений;

g) подсудность судам принимающего государства; и

h) степень расхождения между правом, применимым к поведению поставщика сертификационных услуг, и правом принимающего государства.

3) Сертификат устанавливает:

a) идентификационные данные поставщика сертификационных услуг;

b) что лицо, которое идентифицируется в сертификате, обладает в соответствующий момент времени подписывающим устройством, указанным в сертификате;

c) что подписывающее устройство было действительным на дату или до даты выдачи сертификата;

d) любые ограничения целей или стоимостного объема, в связи с которыми может использоваться сертификат; и

e) любое ограничение масштаба или объема финансовой ответственности, с которым соглашается поставщик сертификационных услуг в отношении любого лица.

Вариант X

4) Поставщик сертификационных услуг несет финансовую ответственность за невыполнение требований пункта 1.

5) Финансовая ответственность поставщика сертификационных услуг не может превышать ущерба, который поставщик сертификационных услуг предвидел или должен был предвидеть на момент неисполнения с учетом фактов или обстоятельств, которые поставщику сертификационных услуг были известны или должны были быть известны в качестве возможных последствий несоблюдения [невыполнения обязательств [обязанностей] в отношении] [требований] пункта 1.

Вариант Y

4) Поставщик сертификационных услуг несет финансовую ответственность за невыполнение требований пункта 1.

5) При оценке ущерба во внимание принимаются следующие факторы:

a) затраты на получение сертификата;

b) характер сертифицируемой информации;

c) наличие и степень любого ограничения цели, для которой может использоваться сертификат;

d) наличие любого заявления, ограничивающего масштаб или степень финансовой ответственности поставщика сертификационных услуг; и

e) любое действие полагающейся стороны, способствовавшее убыткам.

Вариант Z

4) Если ущерб был причинен в результате неверного или порочного сертификата, поставщик сертификационных услуг несет финансовую ответственность за убытки, понесенные либо:

a) стороной, вступившей в договорные отношения с поставщиком сертификационных услуг с целью получения сертификата; или

b) любым лицом, которое разумно полагается на сертификат, выданный поставщиком сертификационных услуг.

5) Поставщик сертификационных услуг не несет финансовой ответственности согласно пункту 2:

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

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

Статья 11. Доверие к электронным подписям

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

2) [При определении того, является ли доверие разумным,] [При определении того, являлось ли поведение лица, положившегося на электронную подпись, разумным,] учитывается, если это уместно, следующее:

a) характер основной сделки, подтвердить которую предполагалось с помощью электронной подписи;

b) предприняла ли полагающаяся сторона надлежащие шаги для определения надежности электронной подписи;

c) предприняла ли полагающаяся сторона шаги для выяснения того, была ли электронная подпись подкреплена сертификатом;

d) было ли полагающейся стороне известно или должно было быть известно, что электронное подписывающее устройство было скомпрометировано или аннулировано;

e) любое соглашение или практика в отношениях между полагающейся стороной и абонентом или любой другой торговый обычай, который может быть применим;

f) любой другой соответствующий фактор.

Статья 12. Доверие к сертификатам

1) Лицо не имеет права полагаться на информацию в сертификате в той мере, в которой такое поведение не является разумным.

2) [При определении того, является ли доверие разумным,] [При определении того, являлось ли поведение лица, полагавшегося на информацию в сертификате, 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 или приостановленных сертификатов, когда это уместно;

c) любое соглашение или практика, существующие или существовавшие в соответствующий момент времени в отношениях между полагающейся стороной и поставщиком сертификационных услуг или абонентом, или любой торговый обычай, который может быть применим;

d) любые другие соответствующие факторы.

Вариант A

3) Если доверие к электронной подписи является неразумным в обстоятельствах, учитывающих факторы в пункте 1, полагающаяся сторона принимает на себя риск того, что подпись является недействительной.

Вариант B

3) Если доверие к подписи является неразумным в обстоятельствах, учитывающих факторы в пункте 1, полагающаяся сторона не имеет никаких претензий к обладателю подписывающего устройства или поставщику сертификационных услуг.

Статья 13. Признание иностранных сертификатов и электронных подписей

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

2) Сертификаты, выданные иностранным поставщиком сертификационных услуг, признаются юридически эквивалентными сертификатам, выданным поставщиками сертификационных услуг, функционирующим на основании ... [законодательство принимающего государства], если практика иностранных поставщиков сертификационных услуг обеспечивает уровень надежности, по меньшей мере эквивалентный тому, который требуется от поставщиков сертификационных услуг 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 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) При определении эквивалентности учитываются, если это уместно, [факторы в пункте 2 статьи 10] [следующие факторы:

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

b) надежность систем аппаратного и программного обеспечения;

c) процедуры оформления сертификатов и рассмотрения заявлений на сертификаты и хранение 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 ведомства относительно соблюдения или наличия вышеизложенного;

g) подсудность судам принимающего государства; и

h) степень расхождения между законодательством, применимым к действиям сертификационного органа, и законодательством принимающего государства.

5) Независимо от положений пунктов 2 и 3 стороны коммерческих и других сделок могут оговорить, что в связи с представляемыми им сообщениями или подписями должен использоваться тот или иной конкретный поставщик сертификационных услуг, класс поставщиков сертификационных услуг и класс сертификатов.

6) В тех случаях, когда, независимо от положений пунктов 2 и 3, стороны соглашаются между собой в отношении использования электронных подписей и сертификатов, [такое соглашение признается достаточным для цели трансграничного признания]. [При определении того, обладает ли - и в какой мере обладает - электронная подпись или сертификат юридической силой, учитывается любое соглашение между сторонами сделки, в которой используется эта подпись или этот сертификат.]

Примечания

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

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

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

[4]Там же, пятьдесят четвертая сессия, Дополнение № 17 (A/54/17), пункты 308-314.