



Генеральная Ассамблея

Distr.: General
16 April 2007
Russian
Original: English

**Комиссия Организации Объединенных Наций
по праву международной торговли**
Сороковая сессия
Вена, 25 июня – 12 июля 2007 года

Возможная будущая работа в области электронной торговли

**Комплексный справочный документ о необходимых
элементах правовой базы, благоприятствующей
развитию электронной торговли: выборочный раздел,
касающийся международного использования
электронных методов подписания и удостоверения
подлинности**

Записка Секретариата

Добавление

В приложении к настоящей записке содержится заключительная часть (часть вторая, глава II, раздел В.2) выборочного раздела по правовым вопросам, связанным с международным использованием электронных методов подписания и удостоверения подлинности.



Приложение

Содержание

	<i>Пункты</i>	<i>Стр.</i>
Часть вторая. Трансграничное использование электронных методов подписания и удостоверения подлинности (<i>продолжение</i>)		
II. Методы и критерии установления правовой эквивалентности	1-22	3
V. Эквивалентность стандартов поведения и режимов ответственности	1-22	3
2. Конкретные случаи ответственности в рамках инфраструктуры публичных ключей	1-22	3
Заключение	23-28	12

Часть вторая

Трансграничное использование электронных методов подписания и удостоверения подлинности

[...]

II. Методы и критерии установления правовой эквивалентности

V. Эквивалентность стандартов поведения и режимов ответственности

2. Конкретные случаи ответственности в рамках инфраструктуры публичных ключей

1. Главной темой дискуссий об ответственности в связи с использованием электронных методов подписания и удостоверения подлинности являются основания и параметры ответственности поставщиков сертификационных услуг. Общеизвестно, что основополагающая обязанность поставщика сертификационных услуг заключается в том, чтобы использовать надежные системы, процедуры и людские ресурсы и действовать в соответствии с заверениями, которые поставщик сертификационных услуг дает в отношении принципов и практики своей деятельности¹. Кроме того, поставщик сертификационных услуг должен проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений, которые относятся к сертификату. Вся эта деятельность потенциально влечет за собой различные степени ответственности поставщика сертификационных услуг, в зависимости от применимого права. В нижеследующих пунктах указываются случаи, связанные для поставщика сертификационных услуг с наибольшим риском наступления ответственности, и вкратце говорится о том, как эта ответственность регулируется внутренним законодательством.

a) Невыдача или задержка выдачи сертификата

2. Как правило, поставщик сертификационных услуг выдает сертификаты по заявкам лиц, желающих использовать электронную подпись. Если заявка отвечает критериям, которые установлены поставщиком сертификационных услуг, то поставщик сертификационных услуг может выдать сертификат. Возможны ситуации, когда отвечающая этим критериям заявка тем не менее отклоняется или удовлетворяется с запозданием – либо просто из-за ошибки поставщика сертификационных услуг, либо из-за умышленной или непредвиденной неготовности используемого поставщиком сертификационных услуг механизма приема заявок, либо из-за того, что поставщик сертификационных услуг по тем или иным скрытым мотивам задерживает

¹ Типовой закон ЮНСИТРАЛ об электронных подписях (см. сноску [...]), статья 9, подпункты 1(a) и 1(b).

выдачу сертификата или не желает выдавать сертификат по данной заявке. У подателей заявок, которые были при подобных обстоятельствах отклонены или удовлетворены с запозданием, могут возникнуть претензии к поставщику сертификационных услуг².

3. При наличии конкурентного рынка сертификационных услуг умышленный или неумышленный отказ поставщика сертификационных услуг в выдаче сертификата может не причинить подателю заявки ощутимого ущерба. Однако в отсутствие реальной конкуренции отказ поставщика сертификационных услуг выдать сертификат или выдача сертификата с запозданием может повлечь за собой серьезный ущерб подателю неудовлетворенной заявки, если без сертификата он будет не в состоянии заключить какую-либо сделку. Даже при наличии конкурирующих альтернативных поставщиков можно представить себе ситуации, когда лицо, запросившее сертификат для той или иной сделки, понесет в связи с ней конкретные убытки, если из-за отклонения или позднего удовлетворения заявки сертификат не будет получен своевременно, и подателю заявки придется отказаться от важной сделки³.

4. В международном контексте такой сценарий маловероятен, так как большинство подписавших скорее всего будут обращаться к поставщикам сертификационных услуг, базирующимся в их собственных странах.

b) Небрежность при выдаче сертификата

5. Основная функция сертификата заключается в увязывании идентификационных данных подписавшего лица с тем или иным публичным ключом. Соответственно, главная задача поставщика сертификационных услуг состоит в том, чтобы, следуя объявленной им практике, проверить, действительно ли податель заявки является подписавшим лицом и имеет в своем распоряжении частный ключ, соответствующий указанному в сертификате публичному ключу. Невыполнение этой задачи может повлечь за собой ответственность поставщика сертификационных услуг по отношению к подписавшему или к третьей стороне, полагающейся на сертификат.

6. Ущерб подписавшему может быть причинен, например, в случае ошибочной выдачи сертификата постороннему лицу, присвоившему себе чужие идентификационные данные. При этом возможен сговор с участием служащих или подрядчиков самого поставщика сертификационных услуг с целью использования ключа подписи этого поставщика сертификационных услуг для удовлетворения мошеннических заявок постороннего лица. Эти сотрудники или подрядчики могут выдать необоснованный сертификат по небрежности, не выполнив должным образом при рассмотрении мошеннической заявки объявленные поставщиком сертификационных услуг процедуры проверки либо использовав ключ подписи поставщика сертификационных услуг для несанкционированного создания сертификата. Наконец, злоумышленник может выдать себя за подписавшее лицо, предъявив поддельные, но схожие с подлинными идентификационные документы, и добиться выдачи сертификата по мошеннической заявке даже при отсутствии небрежности со стороны

² Smedinghoff, "Certification authority: liability issues" (см. сноску [...]), section 3.2.1.

³ Там же.

поставщика сертификационных услуг и при тщательном соблюдении им своих опубликованных правил⁴.

7. Необоснованная выдача сертификата мошеннику может иметь самые серьезные последствия. Полагающиеся стороны, заключающие с мошенником сделки в режиме онлайн, могут, положившись на недостоверные данные в необоснованно выданном сертификате, поставлять товары, перечислять средства, предоставлять кредиты или совершать другие операции, считая, что они ведут дела с тем, за кого выдает себя мошенник. К моменту обнаружения мошенничества полагающимся сторонам может быть причинен значительный ущерб. При подобных обстоятельствах в положении потерпевших оказываются две стороны: полагающаяся сторона, введенная в заблуждение необоснованно выданным сертификатом, и сторона, на имя которой мошеннику был необоснованно выдан сертификат. И у той, и у другой будут претензии к поставщику сертификационных услуг. Еще одним возможным сценарием является выдача сертификата по небрежности на имя несуществующего лица, что чревато причинением ущерба только полагающейся стороне⁵.

8. В статье 9 Типового закона ЮНСИТРАЛ об электронных подписях говорится, в частности, что поставщик сертификационных услуг "проявляет разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений, которые относятся к сертификату в течение всего его жизненного цикла или которые включены в сертификат". Положение о такой общей обязанности буквально воспроизведено во внутреннем законодательстве ряда стран, где применяется Типовой закон⁶, хотя в некоторых странах соответствующий стандарт, по-видимому, был повышен от уровня "разумной осмотрительности" до более высокого уровня гарантии⁷.

9. Режим, установленный Директивой Европейского союза об электронных подписях, обязывает государства – члены ЕС "как минимум" обеспечить, чтобы поставщик сертификационных услуг, выдающий сертификаты, представляемые населению как отвечающие установленным требованиям, или гарантирующий населению такие сертификаты, нес ответственность за возмещение ущерба, причиненного любому субъекту или юридическому или физическому лицу, разумно полагающемуся на такой сертификат: а) в отношении точности всей информации, содержащейся в отвечающем установленным требованиям сертификате на момент его выдачи, а также того, что сертификат содержит все сведения, которые предписано включать в отвечающий установленным требованиям сертификат; б) в отношении гарантий того, что на момент выдачи сертификата у подписавшего лица, указанного в отвечающем установленным

⁴ Там же.

⁵ Там же.

⁶ См., например: Таиланд, Закон об электронных сделках (2001 год), статья 28, пункт 2; а также Каймановы острова (заморская территория Соединенного Королевства), Закон об электронных сделках от 2000 года, статья 28(b).

⁷ См., например: Китай, Закон об электронных подписях, статья 22: "Поставщики электронных сертификационных услуг **обеспечивают** полноту и точность содержания сертификатов электронных подписей в течение срока их действия, а также обеспечивают сторонам, полагающимся на электронные подписи, возможность проверки или понимания всего, что зафиксировано в сертификатах электронных подписей, а также информации по другим связанным с этим вопросам"; выделение добавлено.

требованиям сертификате, имелись данные для создания подписи, соответствующие данным для проверки подписи, приведенным или указанным в сертификате; с) в отношении гарантии того, что эти данные для создания подписи и данные для проверки подписи могут использоваться взаимодополняющим образом в случаях, когда и те, и другие данные генерируются поставщиком сертификационных услуг; за исключением случаев, когда поставщик сертификационных услуг может доказать отсутствие небрежности в своих действиях⁸.

10. Законы других стран в целом не отличаются друг от друга в том смысле, что все они обязывают поставщиков сертификационных услуг проверять точность информации, на основании которой выдается сертификат. В ряде стран поставщик сертификационных услуг вообще несет ответственность перед любым лицом, разумно полагавшимся на сертификат, за точность всей информации, содержащейся в аккредитованном сертификате на момент его выдачи⁹, или гарантирует ее точность¹⁰, хотя в некоторых таких странах поставщик сертификационных услуг может ограничить это гарантийное обязательство, включив в сертификат соответствующее заявление¹¹. Вместе с тем некоторые законы прямо освобождают поставщика сертификационных услуг от ответственности за неточность информации, представленной подписавшим, при условии ее проверки в соответствии с положением о сертификационной практике, если поставщик сертификационных услуг может доказать, что им были приняты все разумные меры для проверки этой информации¹².

11. В других странах достижение такого же результата обеспечивается не с помощью требуемой по закону гарантии, а путем возложения на поставщиков сертификационных услуг общей обязанности перед выдачей сертификата проверять информацию, представленную подписавшим¹³, или создать системы для проверки такой информации¹⁴. В ряде случаев предусмотрена обязанность немедленно аннулировать сертификат, если станет известно, что информация, на основании которой сертификат был выдан, является неточной или ложной¹⁵. В некоторых случаях, однако, закон обходит выдачу сертификатов молчанием, требуя лишь соблюдения поставщиком сертификационных услуг своего положения о сертификационной практике¹⁶ или выдачи сертификата согласно

⁸ Директива Европейского союза об электронных подписях (см. сноску [...]), статья 6, пункт 1.

⁹ Барбадос, глава 308В, Закон об электронных сделках (1998 год), статья 20, пункт 1(а); Бермудские острова, Закон об электронных сделках от 1999 года, статья 23; Гонконг (Особый административный район (ОАР) Китая), Указ об электронных сделках, статья 39; Индия, Закон об информационных технологиях от 2000 года, статья 36(е); Маврикий, Закон об электронных сделках от 2000 года, статья 27, пункт 2(д); а также Сингапур, Закон об электронных сделках, статьи 29, пункт 2(а) и (с), и 30, пункт 1.

¹⁰ Вьетнам, Закон об электронных сделках, статья 31(д); а также Тунис, *Loi relative aux échanges et au commerce électroniques*, статья 18.

¹¹ Например, в Барбадосе, Бермудских Островах, ОАР Гонконге, Маврикий и Сингапуре.

¹² Аргентина, *Ley de firma digital (2001)*, статья 39(с).

¹³ Там же, статья 21(о); Венесуэла (Боливарианская Республика), *Ley sobre mensajes de datos y firmas electrónicas*, статья 35; Мексика, *Código de Comercio: Decreto sobre firma electrónica (2003)*, статья 104(1); а также Чили, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*, статья 12(е).

¹⁴ Эквадор, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, статья 30(д).

¹⁵ Аргентина, *Ley de firma digital (2001)*, статья 19(е)(2).

¹⁶ Перу, *Decreto reglamentario de la ley de firmas y certificados digitales*, статья 29(а).

договоренности с подписавшим¹⁷. Это не означает, что в законе не предусмотрено никакой ответственности поставщиков сертификационных услуг. Напротив, некоторые законы прямо предусматривают такую ответственность, требуя, чтобы поставщики сертификационных услуг обеспечивали надлежащее страховое покрытие своей гражданской ответственности, распространяющееся на любой охваченный и не охваченный договором ущерб подписавшим лицам и третьим сторонам¹⁸.

12. Обязанность поставщика сертификационных услуг проверять точность представляемой информации дополняется обязанностью подписавшего "проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от подписавшего существенных заверений, которые относятся к сертификату в течение всего его жизненного цикла или которые должны быть включены в сертификат"¹⁹. Таким образом, подписавший может нести ответственность перед поставщиком сертификационных услуг или перед полагающейся стороной за представление поставщику сертификационных услуг ложной или неточной информации при подаче заявки на получение сертификата. Иногда это выражено в форме общего обязательства представлять поставщику сертификационных услуг точную информацию²⁰ или проявлять разумную осмотрительность для обеспечения достоверности этой информации²¹; в других случаях на подписавшего прямо возлагается ответственность за ущерб, причиненный в результате невыполнения им данного конкретного требования²².

c) *Несанкционированное использование подписи или скомпрометированная сертификационная практика*

13. Проблема несанкционированного использования устройств для создания подписи и несанкционированного использования сертификатов имеет два аспекта. С одной стороны, возможны нарушения режима хранения устройств для создания подписи или другие случаи, когда они могут быть скомпрометированы, – например, их незаконное присвоение агентом подписавшего. С другой стороны, может быть скомпрометирована сама иерархия создания подписи, используемая поставщиком сертификационных услуг, – например, в случае утраты собственного ключа подписи поставщика сертификационных услуг или же корневого ключа, а также в случае, если эти

¹⁷ Доминиканская Республика, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, статья 40(а); Колумбия, *Ley 527 sobre comercio electrónico*, статья 32(а); а также Панама, *Ley firma digital (2001)*, статья 49, пункт 7.

¹⁸ Боливарианская Республика Венесуэла, *Ley sobre mensajes de datos y firmas electrónicas*, статья 32.

¹⁹ Типовой закон ЮНСИТРАЛ об электронных подписях (см. сноску [...]), статья 8, подпункт 1(с).

²⁰ Аргентина, *Ley de firma digital (2001)*, статья 25; Мексика, *Código de Comercio: Decreto sobre firma electrónica (2003)*, статья 99(III); а также Чили, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, статья 24.

²¹ Каймановы острова, Закон об электронных подписях от 2000 года, статья 31(с).

²² Доминиканская Республика, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, статья 55; Колумбия, *Ley 527 sobre comercio electrónico*, статья 40; Мексика, *Código de Comercio: Decreto sobre firma electrónica (2003)*, статья 99(III); а также Панама, *Ley de firma digital (2001)*, статья 39.

ключи стали известны посторонним, были использованы ими или иным образом скомпрометированы.

14. Иерархия создания подписей может быть скомпрометирована различными путями. Поставщик сертификационных услуг либо кто-то из его служащих или подрядчиков может случайно уничтожить ключ или выпустить его из-под своего контроля; центр данных, где хранится частный ключ, может быть поврежден в результате аварии, или же ключ, принадлежащий поставщику сертификационных услуг, может быть умышленно уничтожен или скомпрометирован кем-то (например, хакером) в противозаконных целях. Последствия компрометации иерархии создания подписей могут быть весьма серьезными. Например, если частный ключ подписи или корневые ключи попадут в руки злоумышленника, он получит возможность создавать подложные сертификаты и использовать их якобы от имени реальных или фиктивных подписавших лиц, нанося этим ущерб полагающимся сторонам. Кроме того, в случае обнаружения подобного ущерба все сертификаты, выданные данным поставщиком сертификационных услуг, должны будут быть аннулированы, что может стать причиной огромных исков со стороны всего сообщества подписавших лиц о возмещении убытков, причиненных невозможностью использования этих сертификатов.

15. В Типовом законе ЮНСИТРАЛ об электронных подписях данный вопрос подробно не рассматривается. Можно исходить из того, что предусмотренное Типовым законом общее обязательство поставщика сертификационных услуг "использовать надежные системы, процедуры и людские ресурсы"²³ означает, что поставщик сертификационных услуг должен принимать все необходимые меры для недопущения компрометации своего собственного ключа (а вместе с ним и всей своей иерархии создания подписей). В законах нескольких стран такое обязательство предусмотрено прямо, нередко в сочетании с обязанностью поставщика сертификационных услуг использовать надежные системы²⁴. В некоторых случаях особо оговорена обязанность принимать меры во избежание подделки сертификатов²⁵. Поставщик сертификационных услуг обязан воздерживаться от создания подписей подписавших лиц и от получения доступа к данным, используемым для создания их подписей, и может нести ответственность за подобные действия, умышленно совершенные его служащими²⁶. Если данные, предназначенные для создания подписи, были скомпрометированы, то это обязывает поставщика сертификационных услуг просить об аннулировании соответствующего сертификата, выданного им самим²⁷.

²³ Типовой закон ЮНСИТРАЛ об электронных подписях (см. сноску [...]), статья 9, подпункт 1(f).

²⁴ Аргентина, *Ley de firma digital (2001)*, статья 21(c) и (d); Колумбия, *Ley 527 sobre comercio electrónico*, статья 32(b); Маврикий, Закон об электронных сделках от 2000 года, статья 24; Панама, *Ley de firma digital (2001)*, статья 49, пункт 5; Таиланд, Закон об электронных сделках от 2001 года, статья 28, пункт 6; а также Тунис, *Loi relative aux échanges et au commerce électroniques*, статья 13.

²⁵ Боливарианская Республика Венесуэла, *Ley sobre mensajes de datos y firmas electrónicas*, статья 35.

²⁶ Аргентина, *Ley de firma digital (2001)*, статья 21(b).

²⁷ Там же, статья 21(p).

16. Соблюдение всей необходимой осмотрительности требуется и от подписавшего. Например, согласно Типовому закону ЮНСИТРАЛ об электронных подписях подписавший должен "проявлять разумную осмотрительность для недопущения несанкционированного использования его данных для создания подписи"²⁸. Аналогичная обязанность, хотя и с некоторыми вариациями, предусмотрена в большинстве национальных законов. В некоторых случаях закон налагает на подписавшего строгое обязательство сохранять за собой эксклюзивный контроль над устройством для создания подписи и не допускать его несанкционированного использования²⁹ или объявляет подписавшего единолично ответственным за сохранность устройства для создания подписи³⁰. Нередко, однако, это обязательство сопровождается оговоркой, ограничивающей его обязанностью сохранять надлежащий контроль над устройством для создания подписи или принимать надлежащие меры для сохранения над ним контроля³¹, либо предпринимать добросовестные действия для предотвращения его несанкционированного использования³², либо проявлять разумную осмотрительность во избежание несанкционированного использования своего устройства для создания подписи³³.

d) *Непринятие мер по приостановлению действия или аннулированию сертификата*

17. Поставщик сертификационных услуг может также нести ответственность за непринятие мер по приостановлению действия или аннулированию скомпрометированного сертификата. Для того чтобы инфраструктура цифровых подписей функционировала должным образом и пользовалась доверием, совершенно необходим механизм, позволяющий в режиме реального времени определять, является ли тот или иной сертификат действительным или же его действие приостановлено либо он аннулирован. Например, в случае любой компрометации частного ключа аннулирование сертификата представляет собой главный механизм, с помощью которого подписавший может оградить себя от

²⁸ Типовой закон ЮНСИТРАЛ об электронных подписях (см. сноску [...]), статья 8, подпункт 1(a).

²⁹ Аргентина, *Ley de firma digital (2001)*, статья 25(a); Доминиканская Республика, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, статья 53(d); Колумбия, *Ley 527 sobre comercio electrónico*, статья 39, пункт 3; Панама, *Ley de firma digital (2001)*, статья 37, пункт 4; Российская Федерация, Федеральный закон об электронной цифровой подписи (2002 год), статья 12, пункт 1; а также Турция, Указ о процедурах и принципах, связанных с исполнением Закона об электронной подписи (2005 год), статья 15(е).

³⁰ Тунис, *Loi relative aux échanges et au commerce électroniques*, статья 21.

³¹ Вьетнам, Закон об электронных сделках, статья 25, пункт 2(a), а также Чили, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, статья 24.

³² Боливарианская Республика Венесуэла, *Ley sobre mensajes de datos y firmas electrónicas*, статья 19.

³³ Индия, Закон об информационных технологиях от 2000 года, статья 42, пункт 1; Каймановы острова, Закон об электронных сделках от 2000 года, статья 39(a); Маврикий, Закон об электронных сделках от 2000 года, статья 35, пункт 1(a) и (b); Мексика, *Código de Comercio: Decreto sobre firma electrónica (2003)*, статья 99(II); Сингапур, Закон об электронных сделках (глава 88), статья 39; Таиланд, Закон об электронных сделках (2001 год), статья 27, пункт 1; а также Эквадор, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, статья 17(b).

попыток совершения мошеннических сделок посторонними лицами, которые могли завладеть копией его частного ключа.

18. Следовательно, оперативность, с которой поставщик сертификационных услуг по просьбе подписавшего аннулирует выданный ему сертификат или приостанавливает его действие, имеет решающее значение. Промежуток времени между просьбой подписавшего лица об аннулировании сертификата, его фактическим аннулированием и публикацией уведомления об аннулировании может быть использован посторонним лицом для заключения мошеннических сделок. Поэтому если поставщик сертификационных услуг допускает необоснованные задержки с внесением соответствующих данных в список аннулированных сертификатов или не делает этого вовсе, это может повлечь за собой значительный ущерб как для подписавшего, так и для введенной в заблуждение третьей стороны, полагающейся на якобы действительный сертификат. Кроме того, в ассортимент сертификационных услуг, предлагаемых их поставщиками, могут входить услуги депозитариев и списки аннулированных сертификатов, доступные полагающимся сторонам в режиме онлайн. Наличие такой базы данных связано с двумя основными факторами риска: возможными неточностями в данных депозитария или в списках аннулированных сертификатов, на которые получатели такой информации будут полагаться в ущерб себе, а также возможностью того, что депозитарий или список аннулированных сертификатов окажется недоступным (например, из-за отказа системы), что помешает завершению сделок между подписавшими и полагающимися сторонами.

19. Как уже отмечалось, в Типовом законе ЮНСИТРАЛ об электронных подписях предполагается возможность выдачи поставщиком сертификационных услуг сертификатов различных уровней с разной степенью надежности и защищенности. Соответственно, Типовой закон не предписывает поставщику сертификационных услуг обеспечивать наличие системы аннулирования сертификатов при любых обстоятельствах, так как применительно к некоторым видам сертификатов, рассчитанным на небольшие суммы, это может быть экономически неоправданным. Вместо этого Типовой закон обязывает поставщика сертификационных услуг лишь предоставить "разумно доступные средства", которые позволят полагающейся стороне установить по сертификату, в частности, "существуют ли средства для направления подписавшим уведомления" о том, что данные для создания подписи были скомпрометированы, и "предлагается ли услуга по своевременному аннулированию"³⁴. В случаях, когда услуга по своевременному аннулированию предусмотрена, поставщик сертификационных услуг должен обеспечить фактическое наличие такой возможности³⁵.

20. Режим, установленный Директивой Европейского союза об электронных подписях, обязывает государства – члены ЕС "как минимум" обеспечить, чтобы поставщик сертификационных услуг, выдающий сертификаты, представляемые населению как отвечающие установленным требованиям, нес ответственность за возмещение ущерба, причиненного любому субъекту или юридическому или

³⁴ Типовой закон ЮНСИТРАЛ об электронных подписях (см. сноску [...]), статья 9, подпункт 1(d), (v) и (vi).

³⁵ Там же, статья 9, подпункт 1(e).

физическому лицу, разумно полагающемуся на такой сертификат, вследствие непринятия мер по регистрации аннулирования сертификата, за исключением случаев, когда поставщик сертификационных услуг может доказать отсутствие небрежности в своих действиях³⁶. Законы некоторых стран предписывают поставщику сертификационных услуг принимать меры для недопущения подделки сертификатов³⁷ или аннулировать сертификат, как только станет известно, что информация, на основании которой он был выдан, является неточной или ложной³⁸.

21. Аналогичная обязанность может существовать также для подписавшего и других уполномоченных лиц. В частности, Типовой закон ЮНСИТРАЛ об электронных подписях требует, чтобы подписавший "без неоправданных задержек" использовал "средства, предоставленные в его распоряжение поставщиком сертификационных услуг", или "иным образом предпринимал разумные усилия для уведомления любого лица, которое, как подписавший может разумно предполагать, полагается на электронную подпись или предоставляет услуги в связи с ней", если подписавшему стало "известно, что данные для создания подписи были скомпрометированы", или если "обстоятельства, известные подписавшему, обуславливают существенный риск того, что данные для создания подписи могли быть скомпрометированы"³⁹.

22. Во внутреннем законодательстве нередко предусмотрена обязанность подписавшего ходатайствовать об аннулировании сертификата при любых обстоятельствах, когда секретность данных для создания подписи могла быть нарушена⁴⁰, хотя в некоторых случаях закон обязывает подписавшего лишь сообщать об этом поставщику сертификационных услуг⁴¹. В законах нескольких стран принята формулировка Типового закона ЮНСИТРАЛ об электронных подписях, который обязывает подписавшего уведомлять также любое лицо, которое, как может разумно предполагать владелец устройства для создания подписи, полагается на электронную подпись или предоставляет услуги в связи с ней⁴². Хотя в целом ряде правовых систем последствия неисполнения этой обязанности могут носить имплицитный характер, в некоторых странах закон прямо предусматривает ответственность подписавшего за несообщение об

³⁶ Директива Европейского союза об электронных подписях (см. сноску [...]), статья 6, пункт 2; см. также пункт (b) приложения II к Директиве.

³⁷ Панама, *Ley de firma digital (2001)*, статья 49, пункт 6.

³⁸ Аргентина, *Ley de firma digital (2001)*, статья 19(e)(2).

³⁹ Типовой закон ЮНСИТРАЛ об электронных подписях (см. сноску [...]), статья 8, подпункты 1(b), (i) и (ii).

⁴⁰ Аргентина, *Ley de firma digital (2001)*, статья 25(c); Доминиканская Республика, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, статьи 49 и 53(e); Колумбия, *Ley 527 sobre comercio electrónico*, статья 39, пункт 4; Маврикий, Закон об электронных сделках от 2000 года, статья 36; Панама, *Ley de firma digital (2001)*, статья 37, пункт 5; Российская Федерация, Федеральный закон об электронной цифровой подписи (2002 год), статья 12, пункт 1; Сингапур, Закон об электронных сделках (глава 88), статья 40; а также Эквадор, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, статья 17(f).

⁴¹ Индия, Закон об информационных технологиях от 2000 года, статья 42, пункт 2; а также Турция, Указ о процедурах и принципах, связанных с исполнением Закона об электронной подписи (2005 год), статья 15(f) и (i).

⁴² Вьетнам, Закон об электронных сделках, статья 25, пункт 2(b); Каймановы острова, Закон об электронных подписях от 2000 года, статья 31(b); Китай, Закон об электронных подписях, статья 15; а также Таиланд, Закон об электронных сделках (2001 год), статья 27, пункт 2.

утрате контроля над частным ключом или необращение с просьбой об аннулировании сертификата⁴³.

Заключение

23. Широкое внедрение электронных методов подписания и удостоверения подлинности может стать важным шагом, способствующим сокращению объемов коммерческой документации и связанных с ней операционных издержек в международной торговле. Хотя темпы изменений в этой сфере во многом определяются прежде всего качеством и надежностью технических решений, правовые нормы могут внести существенный вклад в создание благоприятных условий для использования электронных методов подписания и удостоверения подлинности.

24. Во многих странах уже приняты внутренние меры в этом направлении в форме законодательства, подтверждающего юридическую значимость электронных сообщений и определяющего критерии их эквивалентности сообщениям, составленным на бумаге. Важной составляющей таких законов часто являются положения, регулирующие применение электронных методов подписания и удостоверения подлинности. Наиболее авторитетным образцом законодательства на эту тему стал Типовой закон ЮНСИТРАЛ об электронной торговле⁴⁴, широкое внедрение положений которого способствует обеспечению весьма важной согласованности на международном уровне. Еще большей согласованности позволила бы достичь широкая ратификация Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах⁴⁵, в которой предложен ряд конкретных правил, касающихся международных сделок.

25. Принятие этих норм ЮНСИТРАЛ может способствовать и международному применению электронных методов подписания и удостоверения подлинности. Так, содержащиеся в Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах гибкие критерии функциональной эквивалентности электронных подписей и подписей под бумажными документами могут составить единую международную основу для обеспечения соответствия электронных методов подписания и удостоверения подлинности иностранным требованиям в отношении формы подписи. Однако при этом могут оставаться нерешенными некоторые проблемы, в частности связанные с международным использованием электронных методов подписания и удостоверения подлинности, требующих участия доверенной третьей стороны в процессе такого удостоверения или подписания.

⁴³ Венесуэла (Боливарианская Республика), *Ley sobre mensajes de datos y firmas electrónicas*, статья 40; Доминиканская Республика, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, статья 55; Китай, Закон об электронных подписях, статья 27; Панама, *Ley de firma digital (2001)*, статья 39; Российская Федерация, Федеральный закон об электронной цифровой подписи (2002 год), статья 12, пункт 2; а также Эквадор, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, статья 17(e).

⁴⁴ См. сноску [...] [издание Организации Объединенных Наций, в продаже под No. R.99.V.4].

⁴⁵ См. сноску [...] [резолюция Генеральной Ассамблеи 60/21, приложение].

26. Возникающие в данной области проблемы в очень большой степени обусловлены расхождениями в технических стандартах или несовместимостью оборудования либо программного обеспечения, что сужает возможности взаимодействия между системами, существующими в разных странах. Усилия по согласованию стандартов и повышению технической совместимости могут позволить преодолеть имеющиеся на сегодняшний день трудности. Однако использование электронных методов подписания и удостоверения подлинности наталкивается и на трудности юридического характера, связанные, в частности, с внутренним законодательством, предписывающим или поощряющим использование тех или иных конкретных технологий электронного подписания – как правило, цифровых подписей.

27. Законы, определяющие юридическую значимость цифровых подписей, обычно признают такую же юридическую значимость за подписями, подтверждаемыми иностранными сертификатами, лишь в той мере, в какой эти сертификаты рассматриваются как эквивалентные сертификатам, выданным в данной стране. Анализ, проведенный в рамках настоящего исследования, указывает на то, что для правильной оценки юридической эквивалентности необходимо сравнивать между собой не только технические стандарты и стандарты защиты, присущие каждой конкретной технологии подписания, но и нормы, регулирующие ответственность различных сторон, вовлеченных в этот процесс. В Типовом законе ЮНСИТРАЛ об электронных подписях сформулирован общий комплекс основных правил, определяющих некоторые обязанности сторон в процессе подписания и удостоверения подлинности, которые могут влиять на их индивидуальную ответственность. Существуют также тексты, принятые на региональном уровне, – такие, как Директива Европейского союза об электронных подписях, – создающие аналогичную законодательную основу для ответственности поставщиков сертификационных услуг, которые действуют в соответствующем регионе. Однако ни один из этих текстов не охватывает все вопросы ответственности, связанные с международным использованием некоторых электронных методов подписания и удостоверения подлинности.

28. Законодателям и лицам, ответственным за выработку политики, важно уяснить для себя различия между внутренними режимами ответственности, существующими в разных странах, а также те элементы, которые их объединяют, с тем чтобы разработать надлежащие методы и процедуры признания подписей, подтверждаемых иностранными сертификатами. Возможно, уже сегодня во внутреннем законодательстве различных стран даются в основном аналогичные ответы на вопросы, рассмотренные в настоящем справочном документе, что может объясняться общностью правовых традиций этих стран или их участием в региональных механизмах интеграции. Для таких стран могут быть целесообразными выработка единых стандартов ответственности и даже взаимное согласование внутренних правил в целях содействия трансграничному использованию электронных методов подписания и удостоверения подлинности.