Организация Объединенных Наций A/CN.9/630/Add.1

Генеральная Ассамблея

Distr.: General
25 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 часть (часть первая, глава I, разделы B и C) выборочного раздела комплексного справочного документа по правовым вопросам, связанным с международным использованием электронных методов подписания и удостоверения подлинности.

* Представление настоящего документа секретариатом Комиссии Организации Объединенных Наций по праву международной торговли было задержано по причине нехватки персонала.

V.07-82782 (R) 230507 250507

Приложение

Содержание

Часть первая

Электронные методы подписания и удостоверения подлинности

[…]

I. Определение и методы электронного подписания и удостоверения подлинности

[…]

B. Основные методы электронного подписания и удостоверения подлинности

1. Для целей данного изложения будут рассмотрены четыре основных метода подписания и удостоверения подлинности: цифровые подписи, биометрические методы, использование паролей и комбинированные методы, а также отсканированные подписи или подписи, введенные с клавиатуры.

1. Цифровые подписи, проставляемые с помощью криптографии с использованием публичных ключей

2. "Цифровой подписью" называются технологические решения на основе асимметричной криптографии, именуемые также системами шифрования с публичным ключом, позволяющие обеспечить подлинность электронных сообщений и гарантировать неприкосновенность содержания этих сообщений. Существует множество разных видов цифровой подписи, включая подписи, утрачивающие действительность при подделке, "слепые" подписи и неоспоримые цифровые подписи.

a) Технические понятия и терминология

i) Криптография

3. Цифровые подписи создаются и проверяются с помощью криптографии – отрасли прикладной математики, позволяющей преобразовывать сообщения в кажущуюся непонятной форму и обратно в первоначальную форму. При проставлении цифровых подписей применяется метод, известный как криптография с использованием публичных ключей, который зачастую основывается на применении алгоритмических функций для создания двух разных, но математически соотносящихся "ключей" (т.е. больших чисел, выведенных путем применения ряда математических формул к простым числам[1]). Один такой ключ используется для

[1] Вместе с тем следует отметить, что рассматриваемое здесь понятие криптографии с использованием публичных ключей не обязательно подразумевает применение алгоритмов, основывающихся на простых числах. В настоящее время используются или разрабатываются и другие математические методы, такие, как криптосистемы на основе эллиптических

создания цифровой подписи или преобразования данных в кажущуюся непонятной форму, а другой – для проверки подлинности цифровой подписи или для восстановления сообщения в его первоначальном виде[2]. Компьютерное оборудование и программное обеспечение, использующие два таких ключа, зачастую совокупно именуются "криптосистемами" или, более конкретно, "асимметрическими криптосистемами", если в них применяются асимметричные алгоритмы.

ii) Публичные и частные ключи

4. Взаимно дополняющие друг друга ключи для цифровой подписи – это так называемый "частный ключ", используемый только подписывающим лицом, которое создает с его помощью цифровую подпись и должно держать этот ключ в секрете, и "публичный ключ", который обычно известен более широко и используется полагающейся стороной для проверки подлинности цифровой подписи. Частный ключ может быть записан на интеллектуальной карточке либо доступен через персональный идентификационный номер (ПИН) или биометрическое идентификационное устройство, например определитель отпечатков пальцев. Если подлинность цифровых подписей конкретного лица должна проверяться многими людьми, то публичный ключ должен быть доступен всем этим людям или распространен среди них, например путем присоединения к подписям соответствующих сертификатов или иным способом, обеспечивающим, чтобы эти сертификаты могли быть получены только полагающимися сторонами и теми, кто должен проверять подлинность подписей. Если асимметрическая криптосистема разработана и реализована надежно, то даже несмотря на то, что ключи одной пары математически соотносятся друг с другом, определить частный ключ на основании публичного ключа практически невозможно. Наиболее распространенные алгоритмы кодирования с помощью публичных и частных ключей основаны на важной особенности больших простых чисел: если путем перемножения двух таких чисел получено некое новое число, то определить по нему эти два исходных числа – очень трудная задача, требующая больших затрат времени[3]. Таким образом, хотя знать

кривых, которые часто считаются обеспечивающими высокую степень защиты данных при значительно меньшей длине используемых ключей.

[2] Хотя применение криптографии является одной из основных особенностей цифровых подписей, сам факт использования цифровой подписи для удостоверения подлинности сообщения, содержащего информацию в цифровой форме, не следует путать с более общим применением криптографии в целях обеспечения конфиденциальности. Криптографические методы обеспечения конфиденциальности заключаются в кодировании электронного сообщения, с тем чтобы только его составитель и адресат были в состоянии его прочесть. В ряде стран применение криптографии для обеспечения конфиденциальности ограничивается законом по соображениям публичного порядка, которые могут включать соображения национальной обороны. Однако применение криптографии в целях удостоверения подлинности путем создания цифровой подписи не обязательно предполагает кодирование какой-либо информации для обеспечения ее конфиденциальности при передаче сообщений, поскольку криптографическая цифровая подпись может быть всего лишь добавлена к незакодированному сообщению.

[3] В некоторых существующих стандартах используется понятие "невычисляемости", под которым имеется в виду предполагаемая необратимость этого процесса, т.е. надежда на то, что секретный частный ключ пользователя невозможно определить на основании его публичного ключа. "Невычисляемость" является относительным понятием и определяется исходя из ценности защищаемых данных, дополнительных компьютерных ресурсов, необходимых для их защиты, срока, в течение которого их необходимо защищать, а также материальных затрат и времени, необходимых для взлома защиты данных, – причем эти

публичный ключ того или иного подписавшего лица и использовать этот ключ для проверки подлинности подписей могут многие, это не дает им возможности определить соответствующий частный ключ и подделывать с его помощью цифровые подписи.

iii) Функция хеширования

5. Помимо генерирования пар ключей при создании цифровых подписей и проверке их подлинности используется еще один основополагающий процесс, обычно именуемый "функцией хеширования". Функция хеширования представляет собой математический процесс, основанный на использовании алгоритма, который создает цифровой образ или сжатую форму сообщения (часто называемую "резюме", или "отпечатком" сообщения) в виде "величины хеширования", или "результата хеширования" стандартной длины; обычно она намного короче самого сообщения, но по содержанию может быть отнесена только к нему. Любое изменение в сообщении неизбежно дает иной результат хеширования, если применяемая функция хеширования не изменилась. При использовании надежной функции хеширования, иногда именуемой "функцией одностороннего хеширования", восстановить оригинал сообщения по его величине хеширования практически невозможно. Еще одна важнейшая особенность функций хеширования заключается в том, что практически невозможно также найти другой двоичный объект (кроме объекта, использованного для получения данного резюме), резюме которого было бы идентичным. Соответственно, функции хеширования позволяют программному обеспечению для создания цифровых подписей оперировать меньшим и более предсказуемым количеством данных, сохраняя при этом надежно доказуемую связь подписи с исходным содержанием сообщения и тем самым обеспечивая эффективную гарантию того, что в сообщение не вносились изменения после его подписания в цифровой форме.

iv) Цифровая подпись

6. Чтобы подписать какой-либо документ или любой другой элемент информации, подписывающее лицо сначала определяет точные границы того, что предстоит подписать. Затем с помощью программного обеспечения, использующего функцию хеширования, подписывающее лицо исчисляет результат хеширования, относящийся (для всех практических целей) только к подписываемой информации. Далее подписывающее лицо при помощи программного обеспечения преобразует результат хеширования в цифровую подпись, используя свой частный ключ. Созданная таким образом цифровая подпись относится только к подписываемой информации и только к частному ключу, использованному для ее создания. Как правило, цифровая подпись (результат хеширования сообщения, зашифрованный частным ключом подписавшего) присоединяется к сообщению и хранится или передается вместе с этим сообщением. Однако она также может передаваться или храниться в качестве отдельного элемента данных до тех пор, пока она сохраняет надежную связь со своим сообщением. Поскольку цифровая подпись относится

факторы оцениваются как на текущий момент, так и с учетом будущего технического прогресса" (American Bar Association, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (Chicago, American Bar Association, 1 August 1996)), p. 9, note 23, размещено по адресу http://www.abanet.org/scitech/ec/isc/dsgfree.html, дата посещения – 5 апреля 2007 года.

только к данному конкретному сообщению, она становится бесполезной, если окончательно утрачивает связь с ним.

v) Проверка подлинности цифровой подписи

7. Проверка подлинности цифровой подписи представляет собой процесс сверки такой подписи с подлинным сообщением и определенным публичным ключом в целях установления того, была ли эта цифровая подпись создана для данного конкретного сообщения с использованием частного ключа, соответствующего указанному публичному ключу. Подлинность цифровой подписи проверяется путем исчисления нового результата хеширования подлинного сообщения с помощью той же функции хеширования, которая была применена для создания цифровой подписи. Затем, используя публичный ключ и новый результат хеширования, проверяющий устанавливает, была ли цифровая подпись создана с использованием соответствующего частного ключа и совпадает ли вновь исчисленный результат хеширования с первоначальным результатом хеширования, который был преобразован в цифровую подпись в процессе подписания.

8. Используемое для такой проверки программное обеспечение подтверждает цифровую подпись как криптографически "проверенную", если a) для подписания сообщения в цифровой форме использовался частный ключ подписавшего лица, что считается доказанным, если подпись прошла проверку публичным ключом подписавшего лица, так как публичный ключ подписавшего лица сходится лишь с цифровой подписью, созданной при помощи частного ключа подписавшего лица; и b) в сообщение не были внесены изменения, что считается доказанным, если результат хеширования, исчисленный проверяющим, идентичен результату хеширования, полученному из цифровой подписи в процессе проверки.

vi) Другие виды применения технологии цифровой подписи

9. Как отмечалось выше, технология цифровой подписи применяется значительно более широко, чем просто для "подписания" электронных сообщений по аналогии с собственноручным подписанием документов (см. выше, пункт […]). Так, подписанные цифровым способом сертификаты часто используются в качестве "удостоверений" для серверов или веб-сайтов – например, чтобы гарантировать пользователям, что данный сервер или веб-сайт является именно тем, в качестве которого он им себя представляет, или действительно связан с компанией, утверждающей, что он находится под ее управлением. Технология цифровой подписи может использоваться также для "удостоверения" компьютерных программ – например, чтобы гарантировать, что скачиваемое через веб-сайт программное обеспечение является подлинным, или что на данном сервере используется технология, которая, по общему признанию, обеспечивает определенный уровень защиты соединений, – или для подтверждения подлинности любых других данных, распространяемых или хранящихся в цифровой форме.

b) Инфраструктура публичных ключей и поставщики сертификационных услуг

10. Чтобы проверить подлинность цифровой подписи, проверяющий должен иметь доступ к публичному ключу подписавшего лица и быть уверенным в том, что он соответствует частному ключу подписавшего лица. Однако пара публичного и частного ключей не имеет внутренне присущей ей связи с каким-

либо лицом; это всего лишь пара чисел. Необходим дополнительный механизм для того, чтобы надежно установить наличие связи какого-либо конкретного физического или юридического лица с данной парой ключей. Это особенно важно, так как между подписавшим и получателями сообщения, имеющего цифровую подпись, ранее могло не существовать доверительных отношений. Поэтому участвующие стороны должны испытывать определенное доверие к выдаваемым публичным и частным ключам.

11. Требуемая степень доверия может наличествовать между сторонами, которые верят друг другу, имели дело друг с другом в течение определенного периода времени, общаются через закрытые системы, действуют в пределах замкнутой группы или которые могут регулировать свои сделки договорным путем, например на основе соглашения о торговом партнерстве. В случае сделки, затрагивающей только две стороны, каждая сторона может просто сообщить (по относительно надежному каналу, такому как курьерская связь или защищенная телефонная линия) публичный ключ из той пары ключей, которую будет использовать каждая сторона. Однако такая степень доверия может отсутствовать, если стороны редко ведут дела друг с другом, общаются через открытые системы (например, по всемирной сети через Интернет), не входят в замкнутую группу или не заключили соглашений о торговом партнерстве и не располагают другими нормами права, регулирующими их взаимоотношения. Кроме того, следует иметь в виду, что в случае необходимости урегулирования споров через суд или арбитраж тот факт, что некий публичный ключ действительно был (или не был) передан получателю его фактическим владельцем, может быть труднодоказуемым.

12. Лицо, намеревающееся использовать цифровую подпись, может сделать публичное заявление о том, что подписи, прошедшие проверку тем или иным конкретным публичным ключом, следует рассматривать как исходящие от этого лица. Форма и юридические последствия такого заявления будут регулироваться законодательством принимающего соответствующую норму государства. Например, презумпция атрибуции электронной подписи конкретному подписывающему лицу может быть установлена путем опубликования соответствующего заявления в официальном бюллетене или в документе, признаваемом государственными органами в качестве "подлинного". Однако другие стороны могут и не пожелать признать это заявление, особенно при отсутствии заранее заключенного договора, устанавливающего юридическую силу такого опубликованного заявления со всей определенностью. Сторона, полагающаяся на такое неподтвержденное заявление, опубликованное в открытой системе, весьма рискует по неосторожности довериться мошеннику или столкнуться с необходимостью уличать другую сторону в ложном отказе от цифровой подписи (вопрос, часто упоминаемый в контексте "неотказа" от цифровых подписей), если сделка окажется невыгодной для подразумеваемого подписавшего лица.

13. Один вариант решения некоторых из этих проблем заключается в том, чтобы использовать третью сторону или стороны для установления связи между идентифицированным подписавшим лицом или его именем и конкретным публичным ключом. В большинстве технических стандартов и руководящих принципов такую третью сторону обычно называют "сертификационным органом" или "поставщиком сертификационных услуг" (в Типовом законе

ЮНСИТРАЛ об электронных подписях[4] было решено использовать термин "поставщик сертификационных услуг"). В ряде стран такие сертификационные органы образуют иерархию, часто называемую "инфраструктурой публичных ключей" (ИПК). В рамках иерархической структуры ИПК может быть установлен порядок, согласно которому некоторые сертификационные органы занимаются только сертификацией других сертификационных органов, а те в свою очередь предоставляют услуги непосредственно пользователям. В такой структуре одни сертификационные органы подчинены другим сертификационным органам. Возможны и другие структуры, где все сертификационные органы могут действовать на равноправной основе. В любой крупной ИПК скорее всего будут и подчиненные, и вышестоящие сертификационные органы. К прочим возможным решениям относится, например, выдача сертификатов полагающимися сторонами.

i) Инфраструктура публичных ключей

14. Создание ИПК позволяет обеспечить уверенность в том, что a) публичный ключ пользователя не был изменен и действительно соответствует частному ключу этого пользователя; и b) используемые криптографические методы являются надежными. Для обеспечения вышеупомянутой уверенности ИПК может предлагать ряд услуг, включая следующие: a) управление криптографическими ключами, используемыми для цифровых подписей; b) удостоверение того, что публичный ключ соответствует частному ключу; c) предоставление ключей конечным пользователям; d) опубликование информации об аннулировании публичных ключей или сертификатов; e) управление личными опознавательными средствами (например, интеллектуальными карточками), которые могут идентифицировать пользователя с помощью уникальной личной идентификационной информации или могут генерировать и хранить частные ключи соответствующего лица; f) проверку правильности идентификации конечных пользователей и предоставление им услуг; g) предоставление услуг по регистрации времени; и h) управление криптографическими ключами, используемыми для кодирования в целях обеспечения конфиденциальности, если такое их применение санкционировано.

15. ИПК может состоять из различных иерархических уровней. Например, в моделях, рассматриваемых в некоторых странах в связи с возможным созданием ИПК, фигурируют следующие уровни: a) единый "базовый орган", который сертифицирует технологию и практику всех сторон, уполномоченных выдавать пары криптографических ключей или сертификаты в связи с использованием таких пар ключей, и осуществляет регистрацию подчиненных сертификационных органов[5]; b) различные сертификационные органы, занимающие более низкую ступень по сравнению с "базовым" органом, которые удостоверяют, что публичный ключ пользователя действительно соответствует частному ключу этого пользователя (т.е. не был изменен); и c) различные регистрационные органы местного уровня, которые занимают более низкую

---

[4] См. сноску […][издание Организации Объединенных Наций, в продаже под № R.02.V.8].

[5] Вопрос о том, должно ли правительство располагать техническими возможностями для хранения или воссоздания частных ключей, используемых в целях обеспечения конфиденциальности, может быть решен на уровне базового органа.

ступень по сравнению с сертификационными органами и которые принимают заявки пользователей на предоставление пар криптографических ключей или сертификатов в связи с использованием таких пар ключей, запрашивают подтверждение идентификационных данных и проверяют идентификацию потенциальных пользователей. В некоторых странах предусматривается, что выступать в роли местных регистрационных органов или оказывать им поддержку могут государственные нотариусы.

16. ИПК, организованные по иерархическому принципу, можно наращивать, то есть присоединять к ним целые новые "ИПК-сообщества" просто путем установления "базовым органом" доверительных отношений с "базовыми органами" таких сообществ[6]. Базовый орган нового сообщества может непосредственно подчиняться базовому органу принимающей ИПК, приобретая тем самым статус нижестоящего поставщика сертификационных услуг в этой ИПК. Базовый орган нового сообщества может как поставщик сертификационных услуг также занимать подчиненное положение по отношению к одному из поставщиков сертификационных услуг в рамках существующей ИПК. Еще одной привлекательной особенностью иерархических ИПК является простота построения сертификационных цепей, которые пролегают в одном и том же направлении – от пользовательского сертификата обратно к "центру доверия". Кроме того, сертификационные цепи в иерархической ИПК являются сравнительно короткими, причем по положению, занимаемому в иерархии тем или иным поставщиком сертификационных услуг, пользователи способны определить, для каких целей можно использовать его сертификат. Однако у иерархических ИПК есть и недостатки, главным образом связанные с наличием единого "центра доверия". Если базовый орган скомпрометирован, то вместе с ним скомпрометирована вся ИПК. Некоторые страны столкнулись также с трудностями при попытках избрать в качестве базового органа ту или иную конкретную организацию и заставить всех других поставщиков сертификационных услуг принять такую иерархию[7].

17. Альтернативой иерархическому построению ИПК является так называемая "сотовая" ИПК. В рамках этой модели поставщики сертификационных услуг занимают равноправное положение по отношению друг к другу. При этом все они могут быть центрами доверия. Как правило, пользователи доверяют тому поставщику сертификационных услуг, который выдал им сертификат. Поставщики сертификационных услуг выдают сертификаты друг другу; эти пары сертификатов отражают их взаимные отношения доверия. Отсутствие иерархии в такой системе означает, что поставщики сертификационных услуг не могут устанавливать условия, регулирующие типы сертификатов, выдаваемых другими поставщиками сертификационных услуг. Если поставщик сертификационных услуг желает ограничить степень доверия, оказываемого другим поставщикам сертификационных услуг, то он должен указать

---

[6] William T. Polk and Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, National Institute of Standards and Technology (September 2000), размещено по адресу http://csrc.nist.gov/pki/documents/B2B-article.pdf, дата посещения – 30 марта 2007 года).

[7] Как отмечают Polk and Hastings (см. сноску [6]), в Соединенных Штатах Америки оказалось очень нелегко выделить конкретное учреждение федерального правительства, которое приняло бы на себя управление всей федеральной ИПК.

соответствующие ограничения в сертификатах, выдаваемых им своим коллегам[8]. Однако согласование условий и пределов взаимного признания может быть исключительно сложным делом.

18. Третий вариант структуры опирается на так называемого "связующего" поставщика сертификационных услуг. Такая структура может быть особенно полезной в том смысле, что она позволяет различным существующим ИПК-сообществам полагаться на сертификаты друг друга. В отличие от поставщика сертификационных услуг в рамках сотовой ИПК связующий поставщик сертификационных услуг не выдает сертификаты непосредственно пользователям. Он также не должен, подобно базовому поставщику сертификационных услуг, служить центром доверия для пользователей ИПК. Вместо этого связующий поставщик сертификационных услуг вступает в равноправные отношения доверия с различными пользовательскими сообществами, позволяя пользователям сохранять отношения с естественными для них центрами доверия в рамках соответствующих ИПК. Если пользовательское сообщество строит свой домен доверительных отношений в форме иерархической ИПК, то связующий поставщик сертификационных услуг устанавливает отношения с базовым органом этой ИПК. Если же пользовательское сообщество строит домен доверительных отношений по принципу сотовой ИПК, то связующему поставщику сертификационных услуг достаточно установить отношения с одним из поставщиков сертификационных услуг такой ИПК, который при этом становится в ней "основным" поставщиком сертификационных услуг для целей создания "связующего звена доверия" с другой ИПК. Это "звено доверия", объединяющее две или более ИПК через их взаимные отношения со связующим поставщиком сертификационных услуг, дает пользователям, входящим в разные пользовательские сообщества, возможность взаимодействовать друг с другом через связующего поставщика сертификационных услуг при конкретно определенном уровне доверия[9].

ii) Поставщик сертификационных услуг

19. Чтобы установить связь между парой ключей и будущим подписывающим лицом, поставщик сертификационных услуг (или сертификационный орган) выдает сертификат, т.е. электронную запись, в которой в качестве "предмета" сертификата указываются публичный ключ и имя абонента сертификата и в которой также может подтверждаться, что будущее подписывающее лицо, указанное в сертификате, является держателем соответствующего частного ключа. Основная функция сертификата заключается в увязывании публичного ключа с конкретным подписывающим лицом. Получатель сертификата, желающий положиться на цифровую подпись, созданную подписывающим лицом, которое поименовано в сертификате, может использовать указанный в сертификате публичный ключ для проверки того, что данная цифровая подпись была создана с помощью соответствующего частного ключа. Если такая проверка дает положительный результат, то это служит определенной

---

[8] Polk and Hastings, *Bridge Certification Authorities* ... (см. сноску [5]).

[9] Структура с использованием "связующего" поставщика сертификационных услуг была в итоге избрана для создания системы ИПК федерального правительства Соединенных Штатов Америки (Polk and Hastings, см. сноску [6]). По той же схеме разрабатывалась система ИПК для правительства Японии.

технической гарантией того, что цифровая подпись была создана данным подписывающим лицом и что часть сообщения, к которой была применена функция хеширования (и, следовательно, соответствующее сообщение данных), не подверглась изменениям после ее подписания в цифровой форме.

20. Чтобы удостоверить подлинность сертификата с точки зрения как его содержания, так и его источника, поставщик сертификационных услуг скрепляет его цифровой подписью. Подлинность цифровой подписи поставщика сертификационных услуг на выданном им сертификате может быть проверена с помощью публичного ключа этого поставщика сертификационных услуг, указанного в другом сертификате другим поставщиком сертификационных услуг (который может находиться на более высоком уровне в иерархии, но не обязательно), а подлинность этого другого сертификата может быть, в свою очередь, удостоверена публичным ключом, указанным в еще одном сертификате, и т.д. до тех пор, пока лицо, полагающееся на цифровую подпись, не получит должной гарантии ее истинности. Еще одним возможным способом подтверждения подлинности цифровой подписи является ее включение в сертификат, выданный поставщиком сертификационных услуг (который иногда именуется "базовым сертификатом")[10].

21. В каждом случае выдающий сертификат поставщик сертификационных услуг должен подписать в цифровой форме свой собственный сертификат в течение срока действия другого сертификата, используемого для проверки подлинности цифровой подписи данного поставщика сертификационных услуг. Согласно законам некоторых государств, одним из способов повышения доверия к цифровой подписи поставщика сертификационных услуг может быть опубликование публичного ключа этого поставщика сертификационных услуг или некоторых данных, относящихся к базовому сертификату (таких, как "цифровой отпечаток"), в официальном бюллетене.

22. Соответствующая сообщению цифровая подпись, независимо от того, была ли она создана подписавшим лицом для удостоверения подлинности сообщения или же поставщиком сертификационных услуг для удостоверения подлинности своего сертификата, должна быть, как правило, надежно датирована, чтобы проверяющий мог точно установить, была ли цифровая подпись создана в течение "срока действия", указанного в сертификате, и в любом случае был ли сертификат действительным (т.е. не числился ли он в списке аннулированных сертификатов) на соответствующий момент, что является условием подтверждения подлинности цифровой подписи.

23. Чтобы публичный ключ и данные о его соответствии конкретному подписавшему лицу были легкодоступными для использования при проверке подлинности, сертификат может быть опубликован в соответствующем реестре или предоставляться для ознакомления каким-либо иным образом. Реестры обычно представляют собой функционирующие в режиме онлайн базы данных о сертификатах и другой информации, которая может быть получена и использована для проверки подлинности цифровых подписей.

---

[10] *Официальные отчеты Генеральной Ассамблеи, пятьдесят шестая сессия, Дополнение № 17* и исправление (A/56/17 и Corr. 3), пункт 279.

24. Уже выданный сертификат может оказаться ненадежным, например в ситуациях, когда подписавший представил поставщику сертификационных услуг неверные идентификационные данные. В других случаях сертификат может быть достаточно надежным при выдаче, но стать ненадежным впоследствии. Если частный ключ "скомпрометирован", например в результате потери подписывающим лицом контроля над ним, то сертификат может перестать заслуживать доверия или утратить надежность, и поставщик сертификационных услуг (по просьбе подписывающего лица или, в зависимости от обстоятельств, даже без его согласия) может приостановить действие (временно прервать срок действия) такого сертификата или аннулировать (навсегда признать недействительность) его. После приостановления действия или аннулирования сертификата от поставщика сертификационных услуг может ожидаться своевременная публикация уведомления об аннулировании или приостановлении действия сертификата либо направление извещений об этом лицам, запрашивающим такую информацию или получившим, согласно имеющимся данным, цифровую подпись, для проверки которой предназначен утративший надежность сертификат. Аналогичным образом, проверке на предмет возможного аннулирования должен, если это применимо, подлежать сертификат самого поставщика сертификационных услуг, равно как и тот сертификат, которым подтверждается подпись, проставляемая органом по регистрации времени на временных метках, и сертификат поставщика сертификационных услуг, выдавшего сертификат органу по регистрации времени.

25. Функционирование сертификационных органов может обеспечиваться частными поставщиками услуг или правительственными учреждениями. В ряде стран по соображениям публичного порядка предусматривается, что только правительственные учреждения могут быть уполномочены действовать в качестве сертификационных органов. В большинстве стран, однако, оказание сертификационных услуг либо целиком предоставлено частному сектору, либо осуществляется параллельно государственными и частными поставщиками. Существуют также закрытые системы сертификации, в рамках которых небольшие группы учреждают собственного поставщика сертификационных услуг. В некоторых странах государственные поставщики сертификационных услуг выдают сертификаты только для подтверждения цифровых подписей, используемых органами государственного управления. Независимо от того, обеспечивается ли функционирование сертификационных органов государственными учреждениями или частными поставщиками услуг и требуется ли, чтобы сертификационные органы получали лицензию на свою деятельность, обычно в рамках ИПК действуют не один, а несколько поставщиков сертификационных услуг. Особого внимания требуют взаимоотношения между различными сертификационными органами (см. пункты [15]-[18] выше).

26. На поставщика сертификационных услуг или базовый орган может быть возложена обязанность обеспечивать, чтобы его требования в отношении надлежащих действий выполнялись на постоянной основе. Хотя выбор сертификационных органов может основываться на ряде факторов, включая надежность используемого публичного ключа и идентификационные данные пользователя, доверие к любому поставщику сертификационных услуг может также зависеть от его способности обеспечить соблюдение стандартов,

касающихся выдачи сертификатов, и от надежности проводимой им оценки данных, получаемых от пользователей, которые обращаются за сертификатами. Особое значение имеет режим ответственности, применяемый к любому поставщику сертификационных услуг в связи с необходимостью постоянного выполнения им требований в отношении надлежащих действий и обеспечения неприкосновенности данных, установленных базовым органом или вышестоящим поставщиком сертификационных услуг, или же любых других соответствующих требований. Не меньшее значение имеет и обязанность поставщика сертификационных услуг действовать в соответствии с заверениями, которые он дает в отношении принципов и практики своей деятельности, предусмотренная в пункте 1 (a) статьи 9 Типового закона об электронных подписях.

c) Практические проблемы внедрения инфраструктур публичных ключей

27. Несмотря на немалый объем знаний о технологиях цифровой подписи и о том, как они функционируют, практическое внедрение инфраструктур публичных ключей и систем цифровой подписи сдерживается рядом проблем, из-за которых масштабы применения цифровых подписей до сих пор не соответствуют ожиданиям.

28. Цифровые технологии подписания хорошо обеспечивают проверку подлинности подписей, созданных в период действительности сертификата. Однако по истечении срока действия сертификата или в случае его аннулирования соответствующий публичный ключ становится недействительным, даже если соответствующая пара ключей не была скомпрометирована. Соответственно, в рамках ИПК должна быть предусмотрена система обслуживания цифровых подписей, обеспечивающая возможность их использования в течение длительного времени. Главная трудность здесь связана с тем, что "исходные" электронные записи (т.е. единицы двоичного кода, или биты, из которых состоит компьютерный файл с записью соответствующей информации), включая цифровую подпись, могут со временем стать недоступными для прочтения или утратить надежность – прежде всего в связи с устареванием программного обеспечения, оборудования или того или другого. Так, защита цифровой подписи может стать ненадежной из-за новых научных достижений в области криптографического анализа, программное обеспечение для проверки подписей может по прошествии длительного времени стать труднодоступным, либо может быть нарушена целостность самого документа[11]. В силу этого долгосрочное сохранение электронных подписей в целом представляется проблематичным. Хотя одно время бытовало мнение о незаменимости электронных подписей для архивных нужд, опыт показал, что они не позволяют избавиться от долгосрочных факторов риска. Поскольку любое изменение записанных данных после создания подписи приводит к тому, что подпись при проверке перестает опознаваться как подлинная, операции по переформатированию (такие как перенос или преобразование данных),

---

[11] Jean-François Blanchette, “Defining electronic authenticity: an interdisciplinary journey”, available at http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf, дата посещения – 5 апреля 2007 года (статья, опубликованная в подборке дополнительных материалов 2004 International Conference on Dependable Systems and Networks (DSN 2004), Florence, Italy, 28 June – 1 July 2004), pp. 228-232.

призванные обеспечить возможность считки записи в будущем, могут отразиться на долговечности подписи[12]. Собственно говоря, цифровые подписи были задуманы скорее как средство защиты информации при ее передаче, чем как средство ее сохранения в течение длительного времени[13]. Инициативы по преодолению этой проблемы до сих пор не привели к ее надежному решению[14].

---

[12] "В конечном счете сохранение информации в электронной форме сводится к сохранению битов. Однако давно стало очевидным, что сохранение набора битов на неопределенный срок представляет собой очень нелегкую задачу. С течением времени набор битов перестает поддаваться расшифровке (компьютером, а значит и человеком) из-за технического устаревания прикладных программ и/или аппаратуры (например, считывающего устройства). Проблема долговечности цифровых подписей на основе ИПК до сих пор мало изучена по причине ее сложности. … Хотя средства удостоверения, применявшиеся в прошлом, – такие как собственноручные подписи, печати, штемпели, отпечатки пальцев и т.д. – также нуждаются в переформатировании (например, переносе на микропленку) в связи с устареванием бумажного носителя, после такого переформатирования они никогда не становятся полностью непригодными для использования по назначению. Всегда остается хотя бы копия, которую можно сравнить с подлинниками других средств удостоверения". (Jos Dumortier and Sofie Van den Eynde, *Electronic Signatures and Trusted Archival Services,* p. 5), размещено по адресу http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where, дата посещения – 5 апреля 2007 года.

[13] В 1999 году архивными работниками ряда стран был начат Международный исследовательский проект по бессрочному сохранению подлинных записей в электронных системах (ИнтерПАРЕС), направленный на "получение теоретических и методологических знаний, необходимых для долгосрочного сохранения подлинных записей, созданных и/или существующих в цифровой форме" (см. http://www.interpares.org/, дата посещения – 5 апреля 2007 года). В проекте доклада Целевой группы по вопросам подлинности, действовавшей в рамках первого этапа проекта (ИнтерПАРЕС-1, завершен в 2001 году), отмечается, что "цифровые подписи и инфраструктуры публичных ключей (ИПК) являются примерами технологий, разработанных и внедренных для целей удостоверения подлинности электронных записей **при передаче в пространстве**. Хотя хранители документации и специалисты по информатике полагаются на технологии удостоверения подлинности как средство подтверждения подлинного происхождения записей, эти технологии никогда не предназначались и на сегодняшний день не могут служить в качестве средства, гарантирующего подлинность электронных записей **по прошествии времени"** (выделение добавлено) (размещено по адресу http://www.interpares.org/documents/atf_draft_final_report.pdf, дата посещения – 5 апреля 2007 года). Следующий этап проекта (ИнтерПАРЕС-2) нацелен на разработку и формулирование концепций, принципов, критериев и методов, позволяющих обеспечить создание и хранение точных и надежных записей, а также долгосрочную сохранность подлинных записей, связанных с художественной, научной и правительственной деятельностью, за период с 1999 по 2001 год.

[14] Например, в 1999 году Совет по стандартам в области информационных и коммуникационных технологий – группа сотрудничающих между собой организаций, занимающихся стандартизацией и связанной с этим деятельностью в области информационных и коммуникационных технологий, призванная координировать усилия по стандартизации во исполнение Директивы ЕС 1999/93/ЕС об электронных подписях, – положил начало Европейской инициативе по стандартам для электронных подписей (ЕИСЭП) (см. сноску […][*Official Journal of the European Communities*, L 13/12]). Консорциум ЕИСЭП (предпринимавший усилия по стандартизации с целью воплощения положений директивы Европейского союза об электронных подписях в конкретные нормы для европейских стран) стремился обеспечить удовлетворение потребности в долгосрочном хранении документов, подписанных криптографическим способом, на основе своего стандартного "формата электронной подписи" (*Electronic Signature Formats ES 201 733*, ETSI, 2000). Согласно этому формату в процессе подтверждения подлинности подписей выделяются такие моменты, как исходное подтверждение и последующее подтверждение.

29. Еще одна область, где в связи с цифровыми подписями и ИПК могут возникать проблемы практического характера, связана с защитой данных и неприкосновенностью частной жизни. Поставщики сертификационных услуг должны надежно хранить ключи, используемые для подписания сертификатов, которые они выдают своим клиентам, в условиях, когда посторонние лица могут пытаться получить несанкционированный доступ к этим ключам (см. также Часть вторую, пункты […]-[…] ниже). Кроме того, поставщики сертификационных услуг должны получать от лиц, обращающихся за сертификатами, персональные данные и коммерческую информацию по ряду вопросов. Эта информация должна храниться у поставщика сертификационных услуг для последующей сверки. Поставщики сертификационных услуг должны принимать необходимые меры для обеспечения того, чтобы доступ к такой информации осуществлялся в соответствии с действующими законами о защите данных[15]. Тем не менее угроза несанкционированного доступа остается реальной.

Формат для последующего подтверждения заключает в себе всю информацию, которая может быть рано или поздно использована в ходе такого подтверждения: данные об аннулировании, маркеры времени, сведения о процедурах создания подписей и т.д. Эта информация собирается на этапе исходного подтверждения подлинности. Разработчики упомянутых форматов электронной подписи были озабочены тем, что из-за постепенного снижения надежности криптографической защиты действительность подписи может со временем оказаться под угрозой. Чтобы застраховаться от такого снижения надежности, подписи, основанные на стандарте ЕИСЭП, регулярно маркируются свежими временными метками, несущими в себе алгоритмы подписания и данные о длине ключей, соответствующие наиболее современным методам криптографического анализа. Проблема долговечности программного обеспечения рассматривалась в докладе ЕИСЭП за 2000 год, где впервые говорилось об "услугах по доверительному архивному хранению" – новой разновидности коммерческих услуг, которые предлагались бы не названными конкретно компетентными организациями и специалистами в целях гарантированного длительного сохранения документов, подписанных криптографическим способом. В докладе перечислен ряд технических требований, которым должны отвечать такие архивные услуги; в их число входит "совместимость с предыдущими версиями" компьютерной аппаратуры и программного обеспечения, достигаемая путем сохранения такой аппаратуры и/или ее имитации (см. Blanchette, "Defining electronic authenticity …"(см. сноску [11])). Дальнейшее исследование на эту тему под названием *European Electronic Signature Standardization Initiative: Trusted Archival Services* (Phase 3, final report, 28 August 2000), проведенное Междисциплинарным центром права и информационных технологий при Лювенском католическом университете, Бельгия, и посвященное рекомендации ЕИСЭП об услугах по доверительному архивному хранению, размещено по адресу http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf?where=, дата посещения – 12 апреля 2007 года). ЕИСЭП была завершена в октябре 2004 года. Системы, позволяющие реализовать ее рекомендации, судя по всему, до сих пор не внедрены (см. Dumortier and Van den Eynde, *Electronic Signatures and Trusted Archival Services* (см. сноску [12])).

[15] См. Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris, 1980) размещено по адресу http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, дата посещения – 7 февраля 2007 года; Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, *European Treaty Series*, No. 108), размещено по адресу http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, дата посещения – 7 февраля 2007 года; Руководящие принципы регламентации компьютерных картотек, содержащих данные личного характера (резолюция 45/95 Генеральной Ассамблеи), размещено по адресу http://193.194.138.190/html/menu3/b/71.htm, дата посещения – 7 февраля 2007 года; и

2. Биометрические данные

30. Биометрическими данными называются данные измерений, используемые для идентификации конкретного лица по его физическим или поведенческим особенностям. К особенностям, которые могут служить для биометрического опознания, относятся ДНК, отпечатки пальцев, радужная оболочка глаза, сетчатка глаза, геометрия ладони или лица, термальный образ лица, форма ушной раковины, голос, естественный запах, конфигурация кровеносных сосудов, почерк, походка и динамика ввода данных с клавиатуры.

31. Использование биометрических устройств, как правило, предполагает фиксацию биометрического образца той или иной биологической особенности человека. Образец фиксируется в цифровой форме. Затем из этого образца извлекаются биометрические данные, с помощью которых составляется проверочный эталон. Впоследствии заключенные в проверочном эталоне биометрические данные сопоставляются с данными, полученными от конечного пользователя для целей проверки, что позволяет определить, прошло ли данное лицо идентификацию или проверку личности[16].

32. Биометрические устройства по своей природе обладают уникальными особенностями, которые следует должным образом учитывать. Наличие этих особенностей, несколько различающихся в зависимости от того, какой параметр принимается за основу, в значительной мере определяет пригодность данной технологии для тех или иных целей.

33. Хранение биометрических данных связано с целым рядом факторов риска, так как биометрические особенности человека, как правило, не могут быть аннулированы. Если биометрические системы оказываются скомпрометированными, то законные пользователи не имеют возможности аннулировать свои идентификационные данные и заменить их другим набором таких данных, который не был скомпрометирован. Поэтому для предотвращения неправомерного использования банков биометрических данных необходимы специальные правила.

34. Биометрические методы не могут быть абсолютно точными, так как биологическим параметрам изначально свойственна изменчивость, и при любых измерениях возможны погрешности. В свете этого биометрические данные рассматриваются не как уникальные, а лишь как "полууникальные" отличительные признаки. Для учета возможных вариаций точность биометрического контроля можно регулировать, устанавливая пороговые уровни соответствия извлеченного образца проверочному эталону. При этом, однако, низкий пороговый уровень может чрезмерно повышать вероятность ложных совпадений, а высокий – вероятность ложных несовпадений. И все же точность

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*Official Journal of the European Communities*, L 281, 23 November 1995), размещено по адресу http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett, дата посещения – 7 февраля 2007 года.

[16] International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), *1999 Glossary of Biometric Terms*, размещено по адресу http://www.afb.org.uk/docs/glossary.htm, дата посещения – 7 февраля 2007 года.

удостоверения, обеспечиваемая биометрическими устройствами, может быть достаточной для большинства видов их коммерческого применения.

35. Кроме того, в связи с хранением и раскрытием биометрических данных возникают вопросы, касающиеся защиты данных и прав человека. Законы о защите данных[17], хотя они могут и не содержать прямых упоминаний о биометрической информации, направлены на защиту индивидуальных данных, относящихся к физическим лицам, обработка которых как в сыром виде, так и в виде эталонов составляет основу биометрической технологии[18]. При этом могут требоваться меры для защиты потребителей от опасностей, связанных с частным использованием биометрической информации, а также с возможным хищением идентификационных данных. Свою роль здесь могут играть и другие области законодательства, такие как законы о труде и охране здоровья[19].

36. Для ряда проблем могут быть предложены технические решения. Например, хранение биометрических данных на интеллектуальных карточках или аппаратных ключах может предохранить их от несанкционированного доступа, возможного в случае, если эти данные содержатся в централизованной компьютерной системе. Разработаны также оптимальные способы снижения риска применительно к таким различным аспектам, как сфера применения и возможности устройств, защита данных, контроль пользователя над персональными данными, а также раскрытие данных, аудит, подотчетность и надзор[20].

37. Как правило, биометрические устройства считаются обеспечивающими высокую степень надежности. Хотя они подходят для разнообразного применения, в настоящее время их используют в основном в государственных учреждениях и, в частности, в правоохранительных органах – например, для иммиграционного контроля и в системах режимного доступа.

38. Разработаны также коммерческие технологии использования биометрических данных; многие из них предусматривают процедуру удостоверения по сочетанию двух параметров, один из которых должен физически наличествовать у удостоверяемого лица (биометрические данные), а другой должен быть ему известен (как правило, пароль или ПИН). Созданы даже системы, позволяющие фиксировать и сопоставлять характеристики собственноручных подписей. Для этого используются цифровые планшеты, регистрирующие нажим ручки и время, затрачиваемое на проставление подписи. Соответствующие данные затем сохраняются в виде алгоритма для сверки с

---

17 См. сноску [15].

18 Paul de Hert, *Biometrics: Legal Issues and Implications*, background paper for the Institute for Prospective Technological Studies of the European Commission (European Communities, Directorate General Joint Research Centre, 2005), p. 13, размещено по адресу http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de Hert.pdf.

19 Например, в Канаде использование биометрических данных обсуждалось в связи с применением Закона о защите персональной информации и электронных документах (2000, с. 5) на рабочих местах (см. *Turner v. TELUS Communications Inc.*, 2005 FC 1601, 29 November 2005 (Federal Court of Canada)).

20 В качестве примера оптимальной практики см. the International Biometric Group BioPrivacy Initiative, "Best practices for privacy-sympathetic biometric deployment", размещено по адресу http://www.bioprivacy.org.

будущими подписями. Однако ввиду имманентных особенностей биометрической информации в этой связи высказываются также предостережения о рисках, связанных с постепенным бесконтрольным распространением таких систем в повседневной коммерческой практике.

39. Если биометрические подписи станут использоваться вместо собственноручных, это может привести к возникновению проблемы доказывания. Уже отмечалось, что степень надежности биометрических данных как доказательства может быть различной в зависимости от используемой технологии и выбранного допустимого процента ложных совпадений. Кроме того, хранящиеся в цифровой форме биометрические данные могут быть умышленно искажены или фальсифицированы.

40. К использованию биометрических подписей могут применяться общие критерии надежности, предусмотренные Типовым законом ЮНСИТРАЛ об электронных подписях[21] и Типовым законом ЮНСИТРАЛ об электронной торговле[22], а также принятой позднее Конвенцией Организации Объединенных Наций об использовании электронных сообщений в международных договорах[23]. Для обеспечения единообразия может также быть полезной разработка международных руководящих принципов использования и регулирования биометрических методов[24]. Вопрос о том, не будет ли установление таких стандартов преждевременным при нынешнем уровне развития биометрических технологий и не станет ли это препятствием их дальнейшему совершенствованию, необходимо тщательно продумать.

3. Пароли и комбинированные методы

41. Пароли и коды используются как для регулирования доступа к информации или услугам, так и для "подписания" электронных сообщений. Последнее практикуется реже, чем первое, из-за опасности компрометации кода в случае его передачи в незашифрованных сообщениях. Вместе с тем пароли и коды являются наиболее широко применяемым средством "удостоверения" для целей регулирования доступа и проверки личности при совершении самых различных операций: так, они чаще всего используются при управлении банковскими счетами через Интернет, при пользовании автоматами для выдачи наличных и при расчетах по потребительским кредитным картам.

42. Следует иметь в виду, что для целей "удостоверения" при электронных сделках могут использоваться различные технологии. При этом в связи с одной и той же сделкой возможно применение нескольких технологий либо несколько видов применения одной технологии. Например, анализ динамики проставления

---

[21] См. сноску […][издание Организации Объединенных Наций, в продаже под No. R.02.V.8].

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

[23] Конвенция Организации Объединенных Наций об использовании электронных сообщений в международных договорах была окончательно согласована ЮНСИТРАЛ на ее тридцать восьмой сессии (Вена, 4-15 июля 2005 года) и официально принята Генеральной Ассамблеей 23 ноября 2005 года (резолюция 60/21 Генеральной Ассамблеи, приложение); размещена по адресу http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

[24] Их можно сопоставить с критериями надежности, изложенными в *Руководстве по принятию Типового закона ЮНСИТРАЛ об электронных подписях* (см. сноску […][издание Организации Объединенных Наций, в продаже под No. R.02.V.8], пункт 75).

собственноручной подписи для подтверждения подлинности может сочетаться с криптографией для защиты целостности сообщения. В другом варианте пароли могут передаваться через Интернет с применением криптографической защиты (например, SSL-протокола в Интернет-обозревателях), в то время как биометрические данные могут использоваться для создания цифровой подписи (асимметричная криптография), которая после ее доставки получателю генерирует пользовательский мандат согласно протоколу "Керберос" (симметричная криптография). При разработке юридических рамок и общих правил использования этих технологий следует уделить внимание роли их возможных сочетаний. Юридические рамки и общие правила электронного удостоверения подлинности должны быть достаточно гибкими для того, чтобы ими можно было охватить комбинированные технологические решения, так как их привязка к конкретным технологиям может помешать совместному использованию этих технологий[25]. Положения, нейтральные с точки зрения технологий, способствовали бы внедрению таких комбинированных технологических решений.

4. Отсканированные подписи и имена, введенные с клавиатуры

43. Интерес законодателей к вопросам электронной торговли с точки зрения частного права объясняется прежде всего озабоченностью тем, как появление новых технологий может отразиться на применении правовых норм, задуманных в расчете на иные носители информации. Такое повышенное внимание к техническим аспектам нередко приводит к умышленному или неумышленному сосредоточению на сложных технологиях, обеспечивающих наиболее высокую надежность электронного удостоверения подлинности и электронных подписей. При этом часто забывают, что очень большое количество, если не большинство, сообщений, связанных с деловыми операциями повсюду в мире, пересылаются вообще без применения каких бы то ни было технологий подписания или удостоверения подлинности.

44. В своей повседневной практике компании разных стран нередко довольствуются, например, перепиской по электронной почте без применения каких-либо способов удостоверения подлинности или подписания помимо указания имен, должностей и адресов участников, вводимого с помощью клавиатуры в конце сообщения. Иногда сообщениям придают более официальный вид, используя факсимильные или отсканированные изображения собственноручных подписей, которые, разумеется, представляют собой не более чем оцифрованную копию рукописного оригинала. Ни подписи, введенные с клавиатуры, ни передаваемые по электронной почте незашифрованные письма, ни отсканированные изображения подписей не обеспечивают высокой степени надежности и не могут служить однозначным подтверждением личности составителя электронного сообщения, частью которого они являются. Тем не менее коммерческие структуры сознательно отдают предпочтение таким формам "удостоверения подлинности" в интересах простоты, оперативности и

---

[25] Foundation for Information Policy Research, *Signature Directive Consultation Compilation*, 28 October 1998 – подготовленная по просьбе Европейской комиссии подборка замечаний, высказанных в ходе консультаций по проекту директивы Европейского союза об электронных подписях, размещена по адресу www.fipr.org/publications/sigdirecon.html, дата посещения – 12 апреля 2007 года.

удешевления связи. Важно, чтобы законодатели и руководители, рассматривая вопрос о регулировании электронных методов подписания и удостоверения подлинности, имели в виду эту широко распространенную в деловых отношениях практику. Строгие требования в отношении электронного удостоверения подлинности и использования электронных подписей, и особенно навязывание того или иного метода или технологии, могут косвенным образом поставить под сомнение действительность и исковую силу значительного числа сделок, заключаемых ежедневно без применения каких-либо специальных методов удостоверения подлинности и подписания. Это, в свою очередь, может подтолкнуть недобросовестные стороны к уклонению от последствий добровольно принятых ими обязательств путем оспаривания подлинности своих собственных электронных сообщений. Нереалистично ожидать, что директивное установление высоких требований к удостоверению подлинности и подписанию в итоге приведет к тому, что все стороны будут фактически применять их на повседневной основе. Опыт использования наиболее современных методов, таких как цифровое подписание, показывает, что сомнения, обусловленные дороговизной и сложностью технологий подписания и удостоверения подлинности, зачастую ограничивают масштабы их практического применения.

C. Управление электронными идентификационными записями*

45. В электронной среде физические и юридические лица имеют возможность прибегать к услугам целого ряда поставщиков. Всякий раз, когда лицо регистрируется у провайдера услуг с целью получения доступа к этим услугам, для него создается электронная идентификационная запись. При этом одна такая запись может быть связана с целым рядом учетных записей для каждой прикладной программы или платформы. Умножение числа идентификационных записей и соответствующих им учетных записей может затруднять работу с ними как для пользователя, так и для поставщика услуг. Этих трудностей можно избежать, предусмотрев для каждого лица единую электронную идентификационную запись.

46. Регистрация у поставщика услуг и создание идентификационной записи ведут к установлению отношений взаимного доверия между данным лицом и соответствующим поставщиком. Для создания единой электронной идентификационной записи эти двусторонние отношения должны быть сведены в более общую систему, позволяющую управлять ими совместно; это называется управлением идентификационными записями. С точки зрения поставщиков преимущества управления идентификационными записями могут включать более надежную защиту, упрощение соблюдения норм регулирования и повышение маневренности при осуществлении коммерческих операций, а с точки зрения пользователей – облегчение доступа к информации.

47. Управление идентификационными записями можно представить себе в рамках двух подходов: традиционного принципа пользовательского доступа (регистрация в системе) с использованием интеллектуальных карточек и соответствующих данных, при вводе которых клиент получает доступ к услуге, и

---

* Данный раздел получит дальнейшее развитие в окончательном варианте комплексного справочного документа.

более новаторского принципа обслуживания на базе системы, предоставляющей пользователям и их устройствам персонализованные услуги.

48. Подход к управлению идентификационными записями, основанный на пользовательском доступе, нацелен на административную поддержку процедур удостоверения пользователей, прав доступа, ограничений доступа, учетных записей, паролей и других атрибутов одной или нескольких прикладных программ или систем. Он призван облегчать и регулировать доступ к прикладным программам и ресурсам, одновременно обеспечивая защиту конфиденциальной личной и коммерческой информации от несанкционированных пользователей.

49. При подходе, основанном на принципе обслуживания, рамки управления идентификационными записями расширяются и охватывают все ресурсы компании, используемые для оказания услуг в режиме онлайн: сетевое оборудование, серверы, порталы, информационное наполнение, прикладные программы и продукты, а также данные, подтверждающие статус пользователей, принадлежащие пользователям адресные книги, сведения об их предпочтениях и правах. На практике речь может идти, например, о настройках детского доступа или участии в программах для постоянных клиентов.

50. Усилия по расширению практики управления идентификационными записями предпринимаются как на уровне коммерческих предприятий, так и на уровне правительств. Следует отметить, однако, что политика, проводимая в этом отношении одними и другими, может существенно различаться. Так, подход правительств может быть в большей степени направлен на оптимальное удовлетворение нужд граждан и, следовательно, более ориентирован на взаимодействие с физическими лицами. С другой стороны, решения, применяемые коммерческими структурами, должны учитывать расширяющееся использование автоматической аппаратуры при проведении деловых операций, и поэтому могут содержать элементы, рассчитанные на специфические потребности такой аппаратуры.

51. Трудности, отмечаемые в связи с использованием систем управления идентификационными записями, включают проблемы защиты конфиденциальных личных данных от риска, связанного с неправомерным использованием уникальных опознавательных признаков. Проблемы могут возникать также из-за различий в действующих юридических нормах, особенно касающихся возможности делегирования полномочий на совершение действий от имени другого лица. В этой связи предлагаются решения, основанные на добровольном деловом сотрудничестве по принципу так называемого кругового доверия, когда участники должны полагаться на достоверность и точность информации, предоставляемой им другими членами круга. Однако такой подход сам по себе может быть не вполне достаточным для урегулирования всех связанных с этим вопросов, и наряду с ним может потребоваться принятие юридических норм[26]. Разработаны также руководящие принципы определения

---

[26] См. *Modinis Study on Identity Management in eGovernment: Identity Management Issue Report* (European Commission, Directorate General Information Society and Media, June 2006), pp. 9-12, размещено по адресу https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.9_Identity_Management_Issue_Interim_Report_II1.pdf.

юридических требований, в рамках которых могло бы функционировать сообщество пользующихся взаимным доверием инфраструктур[27].

52. В связи с проблемой технического взаимодействия систем Международный союз электросвязи учредил фокус-группу по вопросам управления идентификационными записями "для облегчения и ускорения разработки единой схемы [управления идентификационными записями], а также средств обнаружения рассредоточенных автономных идентификационных записей, их федераций и разновидностей"[28].

53. Способы управления идентификационными записями предлагаются также в контексте электронного правления. Например, в рамках инициативы Европейского союза "i2010: европейское информационное общество как фактор экономического роста и обеспечения занятости" начато исследование, посвященное управлению идентификационными записями в процессе электронного правления и призванное ускорить выработку согласованного подхода к данному вопросу в Европейском союзе на основе экспертных знаний и инициатив, имеющихся в государствах – членах Европейского союза[29].

54. Распространение устройств для создания электронных подписей, нередко выполненных в форме интеллектуальных карточек, все шире практикуется в рамках инициатив по переходу к электронному правлению. Общенациональные мероприятия по выдаче таких карточек населению начали проводиться, наряду с другими странами, в Бельгии[30] и в Эстонии. В результате этих инициатив очень многие граждане получают в свое распоряжение недорогостоящие устройства, способные, среди прочего, служить для создания электронных подписей. Хотя основные цели таких инициатив не обязательно связаны с торговлей, устройства подобного рода могут с тем же успехом использоваться и в коммерческой сфере. Сближение этих двух областей их применения признается все чаще[31].

---

[27] Проект "Альянс за свободу" (см. www.projectliberty.org) представляет собой консорциум с участием более 150 компаний, некоммерческих и государственных организаций разных стран мира. Он ставит перед собой задачу выработки открытого стандарта "федеративной" сетевой идентификационной записи, совместимой со всеми существующими и разрабатываемыми видами сетевого оборудования. "Федеративная" идентификационная запись позволяет коммерческим предприятиям, правительствам, служащим и потребителям проще и надежнее контролировать идентификационную информацию в условиях современной компьютеризованной экономики и является ключевым фактором, способствующим более активному использованию электронной торговли и персонализованных информационных услуг, а также услуг, предоставляемых через Интернет. Возможность присоединения к консорциуму открыта для всех коммерческих и некоммерческих организаций.

[28] http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html.

[29] См. https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi.

[30] См. http://eid.belgium.be/en/navigation/12000/index.html.

[31] См., например, *2006 Korea Internet White Paper* (Seoul, National Internet Development Agency of Korea, 2006), p. 81, где упоминается о двойном применении положений Закона Республики Кореи об электронной подписи для целей электронного правления и электронной торговли; размещено по адресу http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1.