О р д е н а Л е н и н а
ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
имени М.В.Келдыша
Р о с с и й с к о й а к а д е м и и н а у к

А.В.Ермаков, Е.В.Хухлаев

Инфраструктура открытого ключа в системе электронных государственных закупок

Москва
2002 г.

УДК 519.68

***А.В.Ермаков, Е.В.Хухлаев*. Инфраструктура открытого ключа в системе электронных государственных закупок.**

Рассмотрены вопросы технической реализации правовых отношений, имеющих место при осуществлении государственных закупок, в связи с переходом к электронному документообороту. Дан обзор инфраструктуры открытого ключа (PKI), в частности технология электронной цифровой подписи. Защита информации в PKI основана на методах асимметричной криптографии с использованием пары ключей — открытого и закрытого. Рассмотрен закон РФ об электронной цифровой подписи и его соответствие международным стандартам PKI. Предложены методы использования PKI, обеспечивающие адекватную техническую реализацию правовых отношений в системе электронных государственных закупок.

Ключевые слова: электронная цифровая подпись, асимметричная криптография, сертификат ключа, удостоверяющий центр.

***A.V.Ermakov, E.V.Huhlaev.* Public Key Infrastructure in Electronic Government Procurement System.** — Preprint, Keldysh Inst. Appl. Mathem., Russian Academy of Science, 2002.

Problems of technical implementation of the government-procurements legal relations in context of electronic document flow are considered. The review of Public Key Infrastructure (PKI), in particular technology of the electronic digital signature, is given. Information protection in PKI is based on a method of asymmetrical cryptography with usage of pair keys — public and private. The law of the Russian Federation on the electronic digital signature and its conformity to the PKI international standards are considered. The ways to use PKI providing adequate technical implementation of legal relations in electronic government procurement system are offered.

Key words and phrases: digital signature, asymmetrical cryptography, key certificate, certificate authority.

Содержание

1. Введение

С переходом России к рыночным отношениям в целях оптимизации государственных закупок и борьбы с коррупцией организована законодательно закрепленная система проведения открытых торгов (конкурсов) для государственных нужд [1]. С развитием в России Интернета особую актуальность приобретает создание системы электронных государственных закупок, предпосылки развертывания которой рассмотрены в [2].

При осуществлении государственных закупок стороны (госзаказчики и поставщики товаров и услуг) вступают в правовые отношения, регулируемые Гражданским кодексом и прочим законодательством РФ. При традиционном бумажном документообороте обязательства, принимаемые сторонами, и предоставляемые ими сведения подтверждаются документами на бумажном носителе, подписанными уполномоченными должностными лицами соответствующих юридических лиц. Некоторые правовые условия, предусмотренные законодательством, например, конфиденциальность поданной в запечатанном конверте заявки, технически обеспечиваются исключительно добросовестностью организатора конкурса.

При переходе к электронному документообороту необходимо обеспечить адекватную техническую реализацию этих правовых отношений. Такая реализация, помимо всего прочего, должна гарантировать техническую невозможность нарушения сторонами предусмотренных в законодательстве условий или, по крайней мере, существенно затруднить возможность нарушений.

При электронном документообороте собственноручную подпись заменяет *электронная цифровая подпись* (ЭЦП). Недавно (23 января 2002 г.) вступивший в действие “Федеральный закон об электронной цифровой подписи” [3] призван создать необходимую правовую основу для такой замены. Закон определяет правовые условия, при соблюдении которых ЭЦП в электронном документе признается равнозначной собственноручной подписи на бумажном документе (ст. 1 — здесь и далее ссылки на статью закона).

Технически равнозначность обеспечивается тем, что ЭЦП гарантирует неизменность (защиту от подделки) подписанного ЭЦП электронного документа, неотрекаемость от подписи и позволяет безошибочно идентифицировать лицо, подписавшее документ (точнее, правомерного владельца закрытого ключа подписи).

ЭЦП — неотъемлемая составная часть *инфраструктуры открытого ключа* (PKI — public key infrastructure), средства которой получили в настоящее время самое широкое применение для защиты информации в компьютерных сетях. Средства PKI (помимо технологии ЭЦП) обеспечивают также конфиденциальность передаваемой по сети информации и аутентификацию сторон сетевого соединения. Защита информации в PKI основана на методах асимметричной криптографии с использованием пары

ключей — *открытого* (свободно передаваемого по сети) и *закрытого* (хранящегося в тайне у владельца).

В работе дается обзор инфраструктуры открытого ключа, рассматривается Закон об ЭЦП, в частности, соответствие его международным стандартам PKI, и предлагаются методы использования средств PKI, обеспечивающие адекватную техническую реализацию правовых отношений в системе электронных государственных закупок на этапах:

- публикации конкурсной документации госзаказчиком;
- подачи заявки поставщиком;
- вскрытия заявок.

2. Инфраструктура открытого ключа

Инфраструктура открытого ключа — совокупность средств, обеспечивающих защиту информации в компъютерных сетях на базе асимметричной криптографии [4, 5].

2.1. Симметричная и асимметричная криптография

Криптографические методы распадаются на два класса: симметричная (с секретным ключом) и асимметричная (с открытым ключом) криптография.

При симметричной криптографии для расшифровки информации используется тот же самый секретный ключ, что и для зашифровки. За многие десятилетия разработаны алгоритмы шифрования, обладающие высокой производительностью и стойкостью (способность противостоять вскрытию) при достаточно большой длине ключа.

Несмотря на это, непосредственное применение симметричной криптографии в открытых компьютерных сетях встречает серьезные трудности, поскольку требует наличия единого секретного ключа у каждой стороны. Необходимо иметь безопасные средства предварительного согласования единого ключа. Дело в том, что отправление ключа по открытой сети создает брешь в безопасности, потому что ключ легко может быть перехвачен злоумышленником. Кроме того, симметричная криптография не дает возможности обеспечить аутентификацию (проверку подлинности субъекта) сторон сетевого контакта, не имеющих общего секретного ключа.

При асимметричной криптографии используется пара связанных друг с другом ключей, один из которых называется *закрытым* (private) и хранится в тайне у владельца, другой же, называемый *открытым* (public), свободно передается по сети. Зная открытый ключ, практически невозможно определить соответствующий ему закрытый.

Предполагается, что каждый субъект в компьютерной сети должен владеть известным только ему закрытым ключом из уникальной асимметричной пары ключей. Соответствующий закрытому ключу открытый ключ публикуется в сети для общего доступа.

Асимметричные криптосистемы позволяют не только организовать конфиденциальную передачу информации без предварительного обмена секретным ключом, но и значительно расширяют функции криптографии на основе технологии *электронной цифровой подписи* (ЭЦП).

ЭЦП — это реквизит электронного документа, вырабатываемый с помощью закрытого ключа и проверяемый с помощью соответствующего открытого ключа. Практически невозможно получить ЭЦП, не зная закрытого ключа, или изменить документ так, чтобы правильно выработанная ЭЦП осталась неизменной. Поэтому ЭЦП с высокой степенью достоверности свидетельствует, во-первых, о *неизменности* подписанного ей документа и, во-вторых, что выработавший ее субъект знает закрытый ключ. *Неотрекаемость* от подписи гарантируется тем, что правильно подписать документ можно, только владея закрытым ключом.

Недостатком асимметричной криптографии является существенно более низкая производительность по сравнению с симметричной (в сотни и даже тысячи раз). Этот недостаток преодолевается сокращением объема преобразуемой информации посредством *хэширования* (сжатия некоторым стандартным алгоритмом) и использованием симметричных секретных ключей наряду с асимметричными.

Каждая криптосистема с открытым ключом имеет собственный способ генерации ключевой пары и включает свой набор криптоалгоритмов. Не все криптосистемы имеют полный набор криптоалгоритмов, реализующих все вышеупомянутые криптографические функции. Но все они обладают следующей фундаментальной особенностью, которая и лежит в основе всех приемов защиты информации, применяемых в инфраструктуре открытого ключа: все криптоалгоритмы составляют асимметричные пары. Асимметричность пары алгоритмов заключается в том, что если один из алгоритмов использует закрытый ключ, тогда парный ему алгоритм — соответствующий открытый ключ. Такие пары составляют алгоритмы асимметричного шифрования (зашифровки и расшифровки) или выработки и проверки ЭЦП. Владелец закрытого ключа всегда применяет один алгоритм из пары, а все остальные, знающие только открытый ключ, — парный ему алгоритм.

Любая асимметричная криптосистема должна обеспечить аутентификацию (проверку подлинности) субъекта, которая сводится к доказательству владения им соответствующим закрытым ключом.

Асимметричные алгоритмы шифрования позволяют, вообще говоря, построить универсальную криптосистему, реализующую как технологию ЭЦП, так и конфиденциальную передачу информации. Таковы хорошо известные криптосистемы RSA (Rivest-Shamir-Adleman) [6] и ECC (Elliptic Curve Cryptography) [7].

Другие криптосистемы более специализированы и поддерживают не все возможности. Широко применяются криптосистемы, в основе которых лежат

алгоритмы, не являющиеся алгоритмами шифрования, но реализующие только технологию ЭЦП. К ним относятся следующие алгоритмы:

- российские алгоритмы электронной цифровой подписи ГОСТ Р 34.10-94 [8] и ГОСТ Р 34.10-2001 [9];
- алгоритм электронной цифровой подписи DSA (Digital Signature Algorithm), входящий в принятый в США государственный стандарт цифровой подписи Digital Signature Standard [10].

Отметим еще криптосистему на базе алгоритма DH (Diffie-Hellman) [11] согласования ключа, применяемого при конфиденциальной передаче информации.

2.2. Приемы защиты информации на базе асимметричной криптографии

Рассмотрим принципиальную схему выработки и проверки ЭЦП с применением алгоритмов асимметричного шифрования. Эти алгоритмы обладают тем свойством, что зашифрованная одним из ключей пары информация расшифровывается только другим ключом из этой же пары.

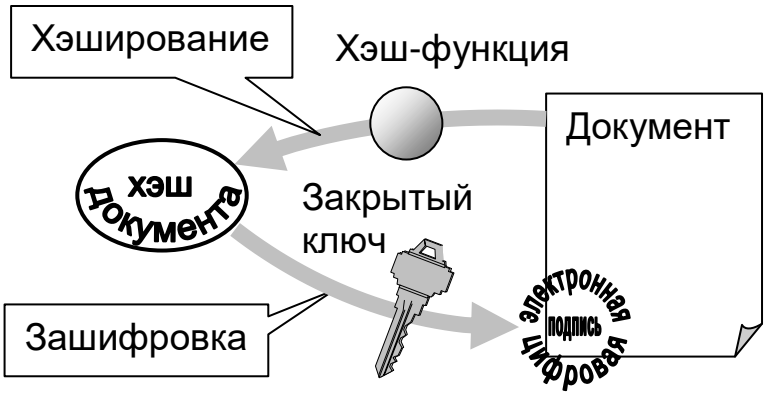

Рис. 1. Схема выработки ЭЦП с применением асимметричного шифрования.

Для *выработки* ЭЦП подписываемый документ подвергается хэшированию (сжатию), а полученный хэш (иногда его называют дайджестом) зашифровывается закрытым ключом (рис. 1). Хэширование применяется, чтобы сократить объем шифруемой информации (повысив тем самым производительность). Хэш-функция (не будучи взаимно однозначным отображением) подбирается таким образом, чтобы было практически невозможно изменить документ, сохранив результат хэширования. По хэшу невозможно восстановить исходный документ, но это и не нужно, поскольку *проверка* ЭЦП заключается в сравнении расшифрованной открытым ключом ЭЦП с хэшем документа (рис. 2). Совпадение гарантирует (с высокой степенью достоверности), во-первых, *неизменность* (защиту от подделки) документа, и, во-вторых, что его подписал (создал ЭЦП) владелец закрытого ключа.

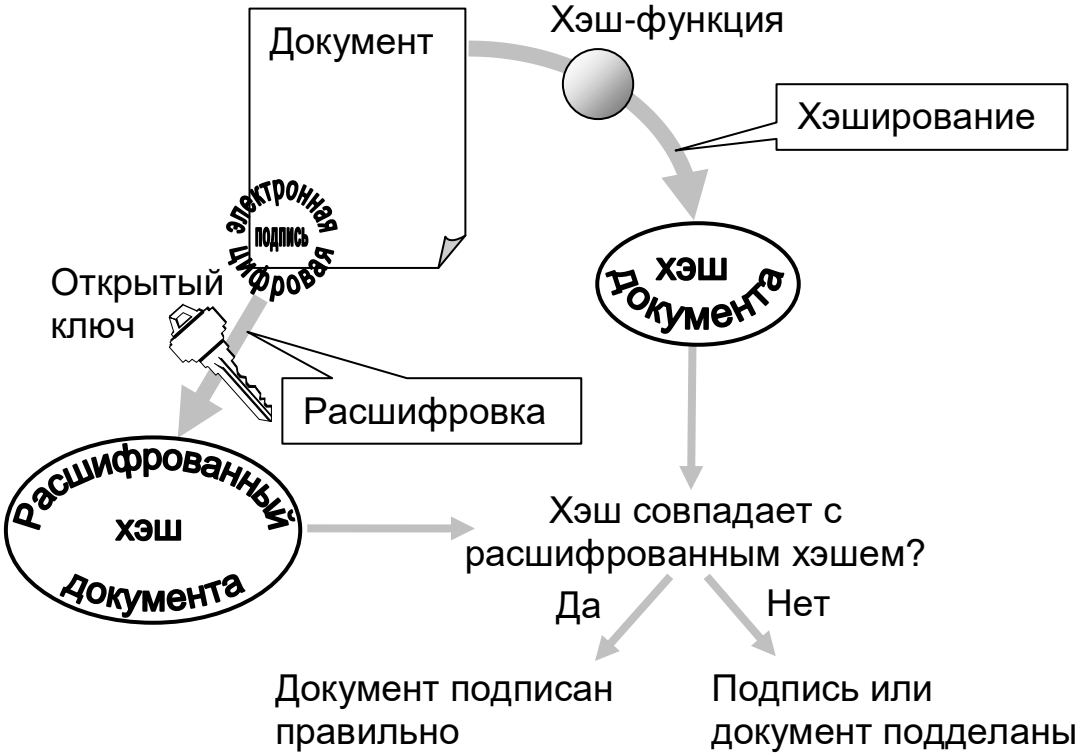

Рис. 2. Схема проверки ЭЦП с применением асимметричного шифрования.

В специализированных криптосистемах, поддерживающих *только* технологию ЭЦП, функции шифрования отсутствуют. Для формирования ЭЦП применяется криптоалгоритм, имеющий на входе хэш документа и закрытый ключ и вырабатывающий ЭЦП. Для проверки ЭЦП применяется другой криптоалгоритм, имеющий на входе хэш документа, проверяемую ЭЦП и открытый ключ. Алгоритм проверки выдает положительный или отрицательный результат в зависимости от правильности ЭЦП.

Аутентификация субъекта сводится к доказательству того, что он владеет закрытым ключом, соответствующим опубликованному открытому. В криптосистемах, поддерживающих технологию ЭЦП, доказательство владения заключается в том, что субъект подписывает своим закрытым ключом присланный ему запрос и посылает его обратно (рис. 3). Если при проверке оказалось, что запрос подписан правильно, то субъект действительно обладает соответствующим закрытым ключом. Необходимо принять меры, чтобы злоумышленник, перехвативший подписанный запрос, не мог впоследствии использовать его, выдавая себя за правомерного владельца закрытого ключа. Для борьбы с этим достаточно, чтобы запрос был неповторяющимся (случайным).

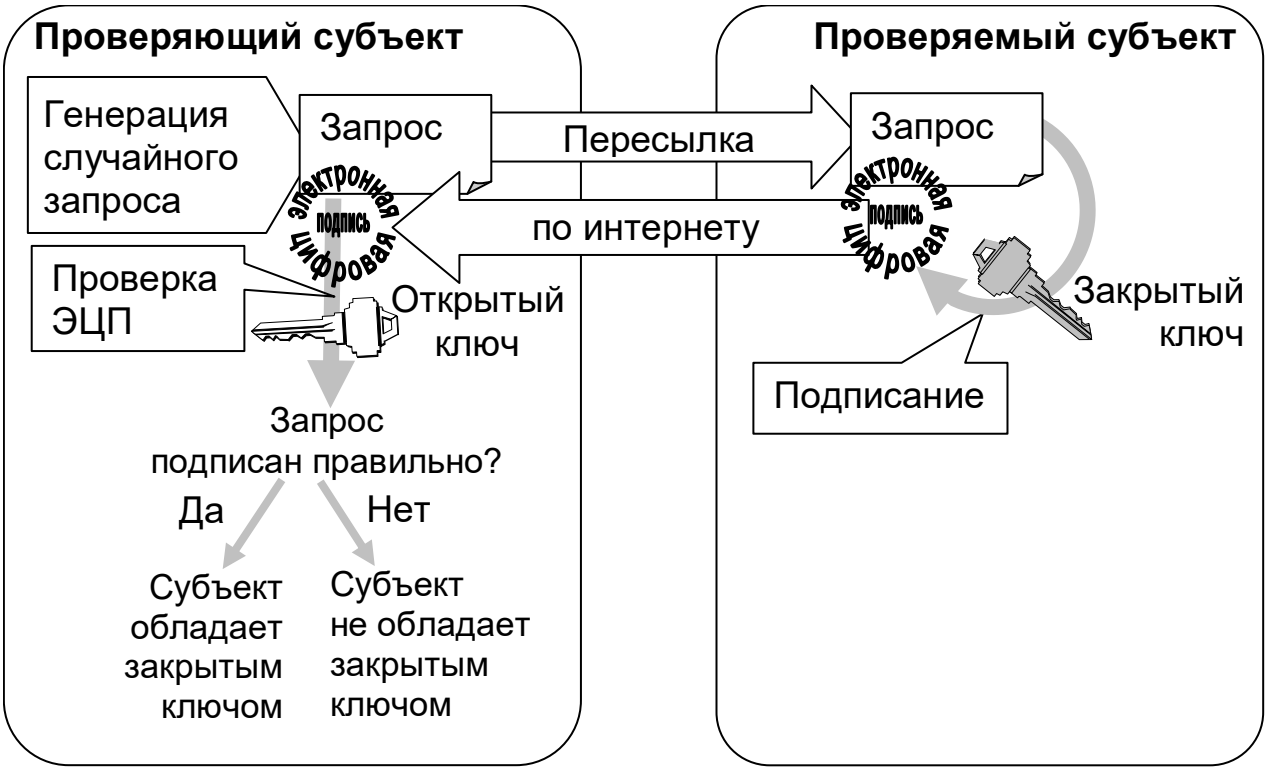

Рис. 3. Проверка обладания закрытым ключом при аутентификации.

Асимметричные алгоритмы шифрования помогают обеспечить *конфиденциальность* при передаче сообщения от одного субъекта другому. Для этого отправителю достаточно зашифровывать сообщение открытым ключом получателя. Поскольку расшифровать сообщение можно, только зная соответствующий закрытый ключ, то это гарантирует, что прочитать его не сможет никто, кроме получателя.

На практике никогда не шифруют открытым ключом все сообщение. Дело в том, что производительность асимметричного шифрования существенно ниже симметричного. Поэтому обычно в начале интерактивного сеанса связи одна из сторон генерирует симметричный секретный ключ (*ключ сеанса*), шифрует его открытым ключом другой стороны и передает только этот зашифрованный ключ. Другая сторона принимает и расшифровывает его (очевидно, что при этом сохраняется конфиденциальность — рис. 4), а все дальнейшие сообщения уже могут быть зашифрованы согласованным ключом сеанса (рис. 5). По окончании сеанса этот ключ уничтожается.

Если нужно послать сообщение вне интерактивного сеанса, то достаточно приложить к зашифрованному сообщению секретный ключ, зашифрованный открытым ключом получателя.

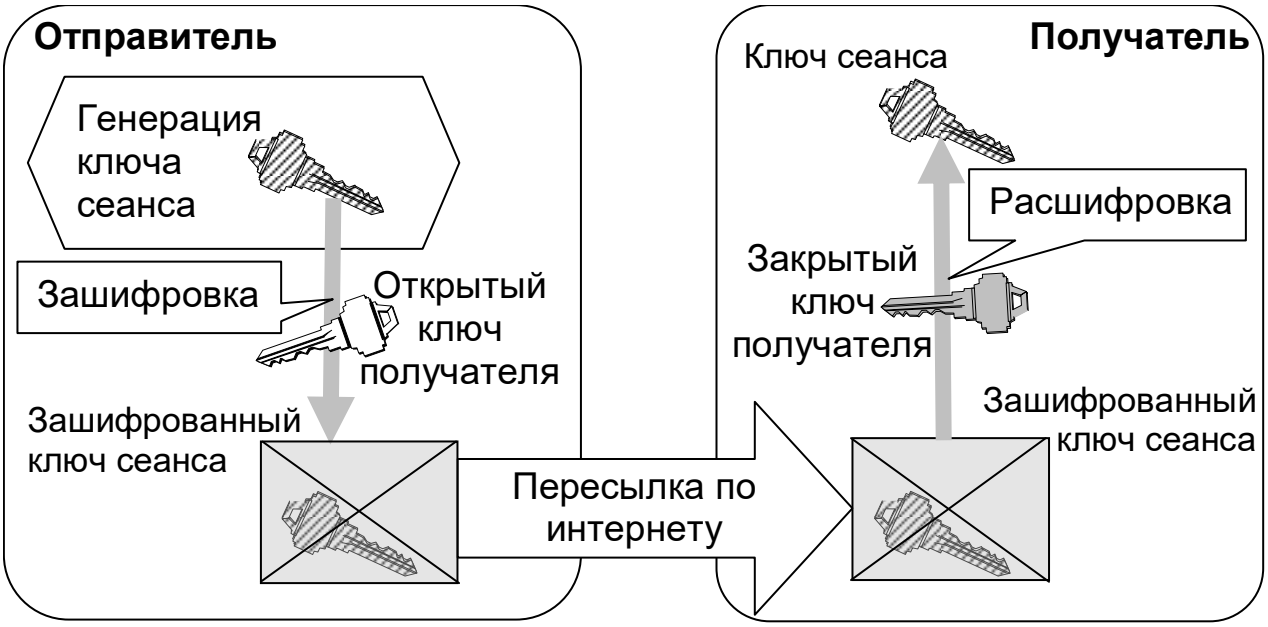

Рис. 4. Согласование ключа сеанса с помощью асимметричного шифрования.

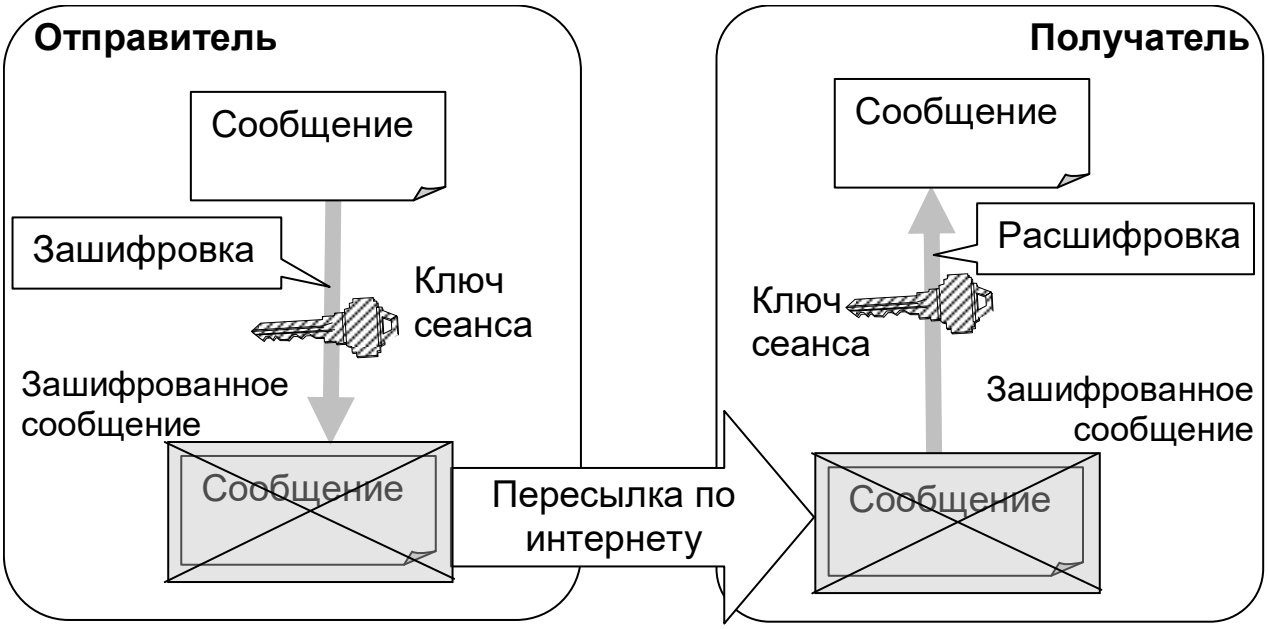

Рис. 5. Конфиденциальный обмен сообщениями
с применением ключа сеанса.

Специализированный алгоритм DH (Diffie-Hellman) согласования ключа позволяет каждой стороне контакта, зная свой закрытый ключ и открытый ключ партнера, получить “общий секрет”, используемый для создания единого секретного ключа, предназначенного для заранее согласованного алгоритма симметричного шифрования. Практически невозможно, зная только открытые ключи, воспроизвести “общий секрет”, что гарантирует защиту от

злоумышленника. При интерактивном контакте стороны сначала обмениваются открытыми ключами, а потом получают единый ключ сеанса. При посылке зашифрованного сообщения вне интерактивного сеанса отправителю должен быть известен открытый ключ получателя; к сообщению же прилагается открытый ключ отправителя, что позволяет получателю воссоздать секретный ключ. В криптосистеме на базе этого алгоритма процедура доказательства владения закрытым ключом подобна процедуре подписывания ЭЦП за тем исключением, что при подписании используется не сам закрытый ключ, а “общий секрет”, зависящий еще и от открытого ключа проверяющей стороны. Выработанная таким образом подпись не может использоваться в качестве универсальной ЭЦП, но только для проверки владения ключом.

2.3. Сертификат ключа

Для верификации открытого ключа применяется *сертификат ключа* — электронный документ, связывающий открытый ключ с субъектом, правомерно владеющим соответствующим закрытым ключом. Без такой верификации злоумышленник может выдать себя за любого субъекта, подменив открытый ключ.

Для заверения сертификата используется ЭЦП учреждения, издающего сертификаты, — удостоверяющего центра (CA — certificate authority). По набору своих функций удостоверяющий центр — основная компонента PKI. Имея открытый ключ удостоверяющего центра, любой субъект может проверить достоверность изданного им сертификата. За достоверность содержащихся в нем данных, идентифицирующих правомерного владельца, отвечает издавший его удостоверяющий центр.

Для получения сертификата ключа субъект должен средствами PKI сформировать пару ключей (открытый и закрытый) и отправить открытый ключ вместе с идентифицирующей себя информацией в удостоверяющий центр, а закрытый ключ сохранить в тайне у себя (рис. 6). Возможна и схема с формированием ключевой пары по просьбе субъекта в самом удостоверяющем центре.

Для сохранения в тайне закрытого ключа применяются разные методы. Он может храниться в защищенной области на диске (HD или FD) или в памяти специализированного автономного носителя, например, USB-брелока или смарт-карты. Как правило, ключ дополнительно шифруется с использованием пароля или PIN-кода, известных только правомерному владельцу. Ключ может быть защищен и с помощью других методов, идентифицирующих владельца.

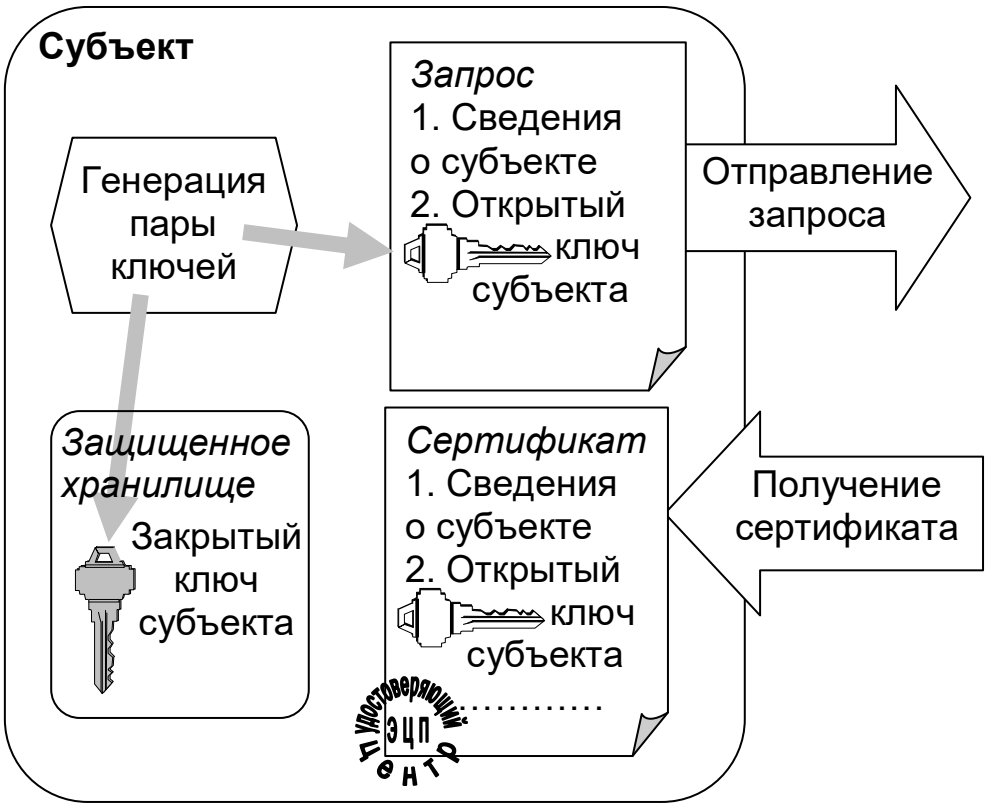

Рис. 6. Запрос на издание сертификата.

После необходимой проверки сведений, включаемых в сертификат (иногда требуется личная явка и предъявление подтверждающих документов), удостоверяющий центр издает и подписывает сертификат, в котором, кроме открытого ключа и идентифицирующей владельца информации указывается период его действия и атрибуты сертификата ключа издателя, необходимые для проверки сертификата (рис. 7).

Очевидно, что подделать сертификат, не владея соответствующим закрытым ключом удостоверяющего центра, практически невозможно. Таким образом, сертификат надежно связывает открытый ключ с данными о субъекте, правомерно владеющем соответствующим закрытым ключом.

Сертификат может свободно распространяться по сети. Никто, не владеющий соответствующим закрытым ключом, не сможет им воспользоваться ни в каких злоумышленных целях, но только для проверки ЭЦП и извлечения данных о правомерном владельце.

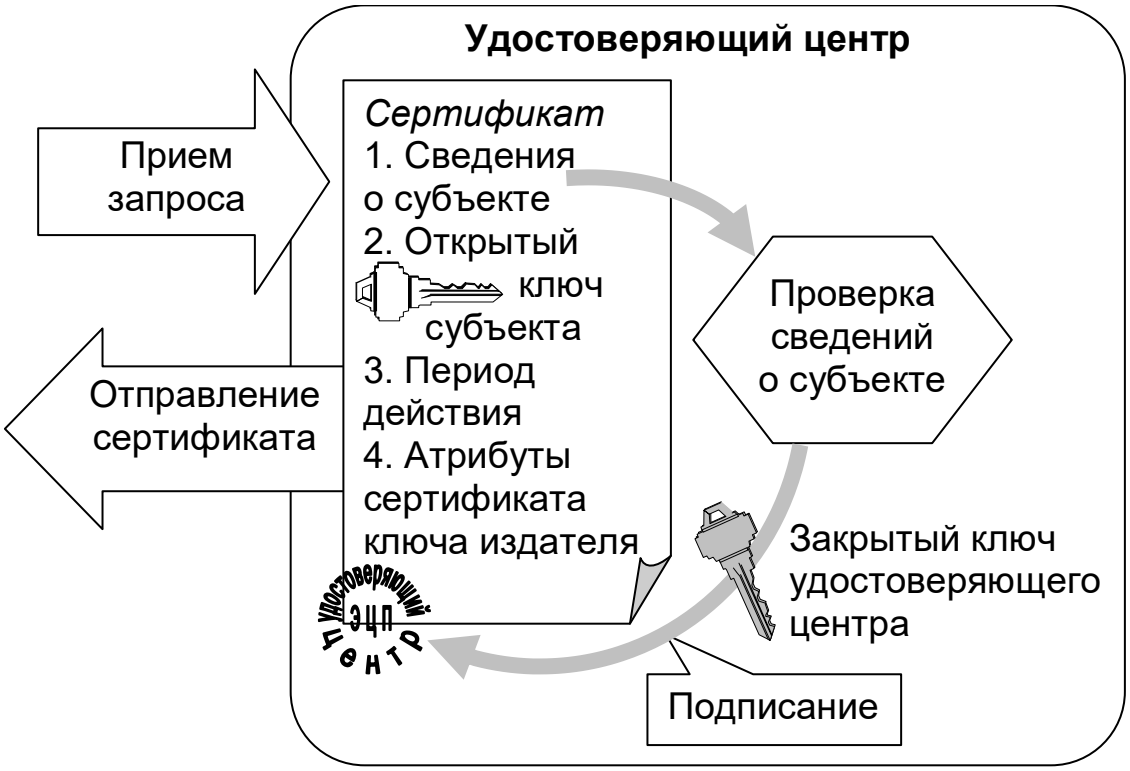

Рис. 7. Издание сертификата.

2.4. Удостоверяющий центр и проверка сертификата

Удостоверяющий центр владеет сертификатом ключа, закрытый ключ которого он использует для заверения издаваемых сертификатов.

Удостоверяющий центр ведет общедоступный реестр изданных им сертификатов. Сертификаты идентифицируются уникальным регистрационным номером.

В функции удостоверяющего центра входит также ведение списка отозванных (до истечения срока действия) по разным причинам (например, при компрометации закрытого ключа или утрате юридической силы документов, на основании которых он выдан) сертификатов (CRL — Certificate Revocation List). Этот список подписывается ЭЦП удостоверяющего центра и открыто публикуется. Для каждого отозванного сертификата в списке указываются регистрационный номер, дата и причина отзыва.

Различают подчиненный удостоверяющий центр, сертификат которого издан другим удостоверяющим центром, и корневой удостоверяющий центр, сертификат которого издан им самим. Корневых удостоверяющих центров (независимых друг от друга) может быть несколько. Тем самым все множество удостоверяющих центров образует “лес” (совокупность иерархических деревьев) в смысле теории графов.

Сертификаты всех удостоверяющих центров (корневых и подчиненных), которым доверяет субъект, должны быть ему известны и храниться в защищенном хранилище. Чтобы доверять некоторому сертификату, надо

пройти по “цепочке доверия” от сертификата его издателя до сертификата удостоверяющего центра, которому доверяет субъект.

Субъект при проверке сертификата, изданного некоторым удостоверяющим центром, должен проверить, не числится ли этот сертификат в числе отозванных.

2.5. Международные стандарты PKI

В основе всех международных стандартов PKI лежит стандарт X.509 ITU-T [12], определяющий формат сертификата ключа и списка отозванных сертификатов.

Рекомендации X.509 оставляют много степеней свободы при определении формата сертификата. Каждое более или менее автономное сообщество пользователей PKI исходя из своих потребностей конкретизирует его. Такую конкретизацию принято называть *профилем*. В настоящее время существует довольно много разнообразных профилей X.509.

Профиль X.509 для использования в интернет (RFC 2549) [13] и другие международные интернет-стандарты PKI выпускаются рабочей группой PKI IETF (Internet Engineering Task Force) [14].

Европейский Парламент в директивах, задающих единые рамки для ЭЦП в странах ЕС [15], ввел понятие *квалифицирующий сертификат* (qualified certificate) и определил требования к нему. ЭЦП, основанная на квалифицирующем сертификате, признается равнозначной собственноручной подписи. IETF выпустила стандарт (RFC 3039) [16], основанный на RFC 2549 и определяющий профиль квалифицирующего сертификата.

В некоторых других странах (США, Австралия, Швеция) также разработаны профили X.509.

Компания Microsoft разработала программную среду, реализующую PKI, которая де-факто определяет собственный профиль.

Разнообразие профилей создает значительные трудности для обмена сертификатами.

2.6. Формат сертификата X.509

Сертификат включает основные поля и поля дополнений. Основные поля должны единообразно интерпретироваться любым ПО, разрабатываемым в соответствии со стандартами PKI. К основным полям относятся:

- Серийный номер сертификата.
- Идентификатор алгоритма ЭЦП.
- Идентификатор издателя сертификата.
- Период действия сертификата.
- Идентификатор владельца сертификата.
- Открытый ключ владельца сертификата.

Поля дополнений могут обладать признаком критичности. Если в сертификате в некотором дополнительном поле установлен признак

критичности, но прикладное ПО не может его интерпретировать, то оно обязано отвергнуть такой сертификат. Если же признак критичности не установлен, то поле может быть просто проигнорировано. В стандартных полях дополнений могут быть указаны:

- Область применения ключа.
- Дополнительная область применения ключа (по требованиям прикладного ПО).
- Дополнительные сведения о владельце и издателе сертификата.
- Информация о списке отозванных сертификатов издателя.
- Некоторые другие сведения.

Возможно и определение любых других дополнений по требованиям прикладного ПО.

Сертификат должен быть подписан ЭЦП издателя сертификата.

2.7. Стандартные протоколы защиты информации в Интернет

На основе стандартов PKI разработаны следующие стандартные протоколы:

- S/MIME (IETF) [17] — протокол защищенной электронной почты.
- SSL (Secure Socket Layer — Netscape) [18] и покрывающий его TLS (Transport Layer Security — IETF) [19] — протоколы, стандартизующие защиту на транспортном уровне и использующиеся при создании защищенных клиент-серверных интернет-приложений.
- SET (Secure Electronic Transactions — Visa, Master Card) [20] — протокол для электронных банковских расчетов и использования пластиковых карточек.
- IPSEC (IETF) [21] — протокол криптографической защиты IP на сетевом уровне.

3. Закон об электронной цифровой подписи. Особый путь России

Пребывая полтора года (с мая 2000 г.) в недрах Государственной Думы, закон об ЭЦП [3] претерпел существенные изменения по сравнению с внесенным правительством законопроектом [22]. В результате обсуждения в комитетах он приобрел своеобычные, сугубо российские особенности.

Справедливости ради следует признать, что некоторые изменения можно только приветствовать. Так, например, дефиниции (ст. 3) стали более четкими. Однако общее впечатление таково, что возникают сильные сомнения в возможности технической реализации закона с соблюдением общепринятых международных стандартов PKI. В частности, вряд ли возможно использование общеупотребительного программного обеспечения, например, Microsoft CryptoAPI и Microsoft Certificate Service.

Основные изменения по сравнению с первоначальной версией закона таковы:

- владельцем сертификата ключа подписи (далее будем называть его “сертификат”, имея в виду его электронную форму) может быть только физическое лицо (но не юридическое лицо);
- упразднен корневой государственный удостоверяющий центр;
- введен институт уполномоченных лиц удостоверяющих центров;
- исключены (по-видимому, неявно подразумеваются) пункты о печати времени и выдаче заверенных бумажных копий электронных документов, подписанных ЭЦП.

Рассмотрим основные положения закона, обращая особое внимание на эти изменения. Все последующие рассуждения основываются на том предположении, что техническая реализация закона должна быть произведена в сооответствии с международными стандартами PKI, а не с вновь изобретенными самобытными российскими стандартами.

3.1. Юридическое значение ЭЦП

Согласно ст. 4.1 закона ЭЦП признается равнозначной собственноручной подписи (правомерного владельца сертификата), если подтверждена ее подлинность, а сертификат ее действителен на момент проверки или на момент подписания (при наличии доказательств о времени подписания). Под доказательствами, возможно, имеется в виду печать времени.

В законе различаются информационные системы общего назначения и корпоративные информационные системы. Из закона не вполне ясно юридическое значение ЭЦП в корпоративной системе, поскольку статус и порядок деятельности удостоверяющего центра, обеспечивающего ее функционирование, а также порядок использования в ней ЭЦП, не определяются законом (ст. 8.1, 17).

3.2. Средства ЭЦП и их использование

Ст. 3 закона определяет средства ЭЦП как аппаратные и (или) программные средства, реализующие хотя бы одну из функций: создание ключей ЭЦП; подписывание электронного документа; проверка подлинности ЭЦП. Средства ЭЦП подвергаются сертификации на предмет подтверждения их соответствия установленным требованиям.

Ст. 5 регламентирует использование средств ЭЦП. В информационных корпоративных системах государственных органов допускается использование только сертифицированных средств ЭЦП (ст. 5.3). Согласно ст. 1 проверка подлинности ЭЦП (во всех системах) может производиться только сертифицированными средствами. В информационных системах общего назначения средства ЭЦП, вырабатывающие ключи, должны быть сертифицированными (ст. 5.2). Средства же ЭЦП, применяющиеся для

подписывания, ничем не ограничиваются. Следовательно, для подписывания в информационных системах общего назначения допускается использование и несертифицированных средств, в том числе и сами удостоверяющие центры для заверения издаваемых сертификатов и выполнения прочих функций могут применять несертифицированные средства. Это вполне допустимо, поскольку выработанная несертифицированным средством неправильная ЭЦП будет отвергнута сертифицированным средством, которое только и можно применять для проверки.

3.3. Сертификаты: владельцы, изготовление, выдача пользователям

В принятом законе владельцем сертификата может быть только физическое (ст. 3), но не юридическое, лицо (в противоположность первоначальному проекту — ст. 6.1 [22]). По-видимому, обоснованием такой дискриминации юридических лиц послужило то, что при бумажном документообороте все документы подписываются исключительно физическими лицами, либо в личном качестве, либо в качестве полномочных представителей юридических лиц, поскольку последние существуют только виртуально (юридически) и реально ничего подписывать не могут. При этом упущено из виду, что электронный документооборот, который и призвана обслуживать ЭЦП, дает новые возможности по сравнению с бумажным, поскольку юридические лица в электронном мире существуют не менее реально, чем физические лица. Само по себе исключение юридических лиц из числа владельцев сертификатов не является критическим, поскольку простановка печати времени на документе (согласно ст. 4.1) обеспечивает действительность подписи должностного лица, даже если соответствующий сертификат утратил силу вследствие прекращения полномочий этого лица. Но вследствие такого исключения у удостоверяющих центров возникают проблемы при заверении сертификатов, которых мы коснемся ниже.

В законе проводится четкое разграничение между *изготовлением* сертификата (ст. 9.2) и *выдачей* его пользователям (ст. 6.4).

Сертификат на имя физического лица *изготавливается* удостоверяющим центром. Необходимые для изготовления сертификата ключи ЭЦП могут быть созданы участником информационной системы самостоятельно или по его просьбе удостоверяющим центром (ст. 5.1, 9.1). В последнем случае гарантируется тайна закрытого ключа. Для создания ключей ЭЦП должны использоваться только сертифицированные средства (ст. 5.2). Заметим, что в законе ФРГ об ЭЦП [23] также допускается создание ключей ЭЦП удостоверяющим центром, но закрытый ключ после передачи владельцу должен быть немедленно уничтожен.

В сертификат помимо необходимых по X.509 данных должны быть включены сведения об отношениях, при осуществлении которых ЭЦП будет иметь юридическое значение (ст. 6.1). В случае необходимости могут быть

указаны должность и квалификация владельца, а также иные сведения. Все сведения о владельце должны быть подтверждены документами (ст. 6.2).

Изготовленный сертификат включается в реестр удостоверяющего центра (ст. 6.3) и безвозмездно *выдается* пользователям (в том числе и владельцу) с указанием времени выдачи и его действительности. При этом он должен быть подписан ЭЦП уполномоченного лица удостоверяющего центра (ст. 6.4). Поскольку указанные данные непрерывно обновляются, то отсюда следует, что при каждой выдаче пользователю сертификат вместе с этими данными подписывается заново (может быть, даже разными уполномоченными лицами). В силу ст. 4.1 (поскольку указание времени выдачи и есть доказательство о времени подписания) подпись уполномоченного лица удостоверяет сертификат, даже если срок действия сертификата уполномоченного лица не покрывает весь период действия сертификата пользователя.

3.4. Удостоверяющий центр и уполномоченные лица

В первоначальной версии закона предполагалось, что у каждого удостоверяющего центра, как у юридического лица, имеется сертификат ключа подписи, которым он заверяет все издаваемые сертификаты (ст. 8.5 [22]). Этот сертификат, в свою очередь, издается уполномоченным государственным органом, который является корневым удостоверяющим центром для всех остальных и ведет единый государственный реестр таких сертификатов (ст. 8.6 [22]). Предложенная схема полностью вписывается в стандартную схему цепочек доверия PKI. Разумеется, уровень секретности закрытого ключа уполномоченного государственного органа вполне сопоставим с уровнем секретности “ядерного чемоданчика”, поскольку компрометация корневого сертификата приведет к компрометации всех остальных, что, конечно, является весьма существенным недостатком этой схемы. Заметим, правда, что закон ФРГ об ЭЦП [23] предусматривает именно такую схему. Но законодатель, по-видимому, руководствуясь демократической идеей минимизации государственного вмешательства, решил лишить уполномоченный государственный орган статуса корневого удостоверяющего центра. В результате этот орган лишь надзирает за деятельностью удостоверяющих центров, но по закону (не будучи удостоверяющим центром) сам не несет никакой ответственности (см. п. 3.5).

Вместо этого в принятом законе вводится институт уполномоченных лиц удостоверяющих центров. Это физическое лицо, обладающее закрытым ключом ЭЦП, предназначенным для подписывания от имени удостоверяющего центра (юридического лица) изготовленных последним сертификатов (ст. 6.4).

Введение института уполномоченных лиц — логическое следствие исключения юридических лиц из числа владельцев сертификата. Оно плохо согласуется с международным стандартом X.509, описывающим формат сертификата. По этому стандарту подписать сертификат должно лицо,

идентификатор которого указывается в качестве изготовителя (поле Issuer). Но по закону удостоверяющий центр (как юридическое лицо) не владеет никакими сертификатами и не может ничего подписывать. Чтобы выйти из этого положения, в проекте российского профиля сертификата, предложенного компаниями “Новый Адам” и “Сигнал-Ком” [24], в поле Issuer указывается все-таки идентификатор удостоверяющего центра, а идентификаторы всех уполномоченных лиц в числе своих атрибутов полностью содержат все атрибуты этого поля. Это позволяет однозначно привязать уполномоченное лицо к своему удостоверяющему центру и дает возможность подписания им любого сертификата, изготовленного этим центром.

При прекращении полномочий уполномоченного лица или истечения срока действия его сертификата ЭЦП под всеми подписанными им сертификатами продолжают быть действительными (согласно ст. 4.1), поскольку в них указано время подписания (ст. 6.4). Поэтому нет необходимости в перекрытии периода действия выдаваемых сертификатов периодом действия уполномоченного лица, что было бы необходимо при отсутствии указания времени подписания.

Прежде чем использовать ЭЦП уполномоченного лица удостоверяющего центра, соответствующий сертификат ключа подписи необходимо представить (в том числе и в форме электронного документа) в уполномоченный федеральный орган (ст. 10.1).

В законе ничего не сказано, кем изготавливается и подписывается представляемый в уполномоченный федеральный орган сертификат уполномоченного лица в форме электронного документа (то, что он должен быть подписан, прямо указано в ст. 3). Следовательно, его может изготовить любой удостоверяющий центр, в том числе и тот, который представляет рассматриваемое уполномоченное лицо. Подписать же его может любое уполномоченное лицо удостоверяющего центра, изготовившего этот сертификат. Может ли само уполномоченное лицо подписать свой собственный сертификат? Формально нет, поскольку его сертификат еще не представлен в уполномоченный федеральный орган и не может использоваться для заверения сертификатов. Но в этом случае нельзя организовать конечную “цепочку доверия” (возможную только при наличии самоподписанных сертификатов), и закон становится полностью неработоспособным. Невозможность такой ситуации приводит к выводу, что это ограничение распространяется только на сертификаты общего назначения, выдаваемые пользователям. Сертификат уполномоченного лица имеет особый статус, поэтому уполномоченное лицо может само подписать свой собственный сертификат, представляемый в государственный реестр, тем более, что соответствующий бумажный сертификат подписывается им же и заверяется подписью руководителя и печатью удостоверяющего центра.

Ст. 13 и 14 закона регламентируют порядок приостановления и аннулирования сертификата. Информация об этом должна заноситься удостоверяющим центром в реестр сертификатов и выдаваться пользователям,

запрашивающим сертификат (согласно ст. 6.4). В законе ничего не говорится о списке отозванных сертификатов, который согласно X.509 должен вести удостоверяющий центр.

3.5. Уполномоченный федеральный орган

Уполномоченный федеральный орган не является удостоверяющим центром: он ведет единый государственный реестр сертификатов ключей подписи уполномоченных лиц удостоверяющих центров (ст. 10.2), но не изготавливает их (по крайней мере, в законе об этом ничего не сказано). Вообще ст. 10 об уполномоченном федеральном органе, если придерживаться ее буквы, по нашему мнению, полностью противоречит международным стандартам PKI и не позволяет организовать конечные цепочки доверия.

Уполномоченный федеральный орган выдает пользователям хранящиеся в реестре сертификаты уполномоченных лиц удостоверяющих центров (ст. 10.2), но в законе ничего не сказано о порядке выдачи. Скорее всего, имеется в виду такой же порядок, что для реестра сертификатов удостоверяющего центра (по аналогии со ст. 16.2), т.е. на хранящиеся в реестре сертификаты при их выдаче пользователям (вместе с данными о времени выдачи и действительности) ставится ЭЦП уполномоченного лица федерального органа. Из ст. 10.1 можно сделать вывод, что изготавливают эти сертификаты сами удостоверяющие центры (кроме них, это некому сделать). Остается непонятным, как в них увязать идентификаторы изготовителя и подписанта.

Кроме того, на уполномоченный федеральный орган возложена обязанность вести реестр сертификатов уполномоченных лиц органов гос. власти и выдавать их (но опять-таки не изготавливать!) пользователям в таком же порядке, что и удостоверяющие центры (ст. 16.2). Отсюда следует, что при выдаче сертификаты подписываются ЭЦП уполномоченного лица федерального органа, т.е. он частично выполняет функции уполномоченного лица удостоверяющего центра. Остается непонятным, кто изготовит сертификат для него и должен ли этот сертификат быть внесенным в реестр сертификатов уполномоченных лиц удостоверяющих центров.

Очевидно, что этот сертификат имеет совершенно особый статус, близкий к статусу сертификата корневого удостоверящего центра в PKI, но не является таковым, поскольку его владелец сам не издает сертификаты, но только надзирает за издателями.

3.6. Проставление печати времени

При электронном документообороте очень важно удостовериться, когда именно был подписан документ. Согласно ст. 4.1 закона доказательства, определяющие момент подписания, играют существенную роль при признании ЭЦП равносильной собственноручной подписи. Первоначальная версия закона возлагала на удостоверяющий центр обязанность проставлять печать времени (timestamp) на подписанные ЭЦП документы по просьбе участников информационной системы (ст. 9.5 [21]). В принятом законе этот

пункт исчез. Возможно, эта обязанность подразумевается в числе иных связанных с использованием ЭЦП услуг (ст. 9.1).

3.7. Связь между электронным и бумажным документооборотом. Электронный нотариат

Электронный документооборот не может существовать изолированно от традиционного бумажного.

Например, при разрешении споров в суде стороны должны представлять бумажные документы. Поэтому должна существовать возможность получения бумажного эквивалента подписанного ЭЦП электронного документа. В первоначальной версии закона (ст. 9.7 [21]) на удостоверяющий центр возлагалась обязанность выдавать бумажную копию электронного документа, подписанного ЭЦП, сертификат которой им выдан, по требованию государственных органов и судов. В принятом законе этот пункт исчез. Возможно, эта обязанность подразумевается в ст. 9.1, как подтверждение подлинности ЭЦП.

И обратно, при электронном документообороте необходимо иметь электронные эквиваленты бумажных документов. В частности, при формировании комплекта документов заявки на участие в государственных конкурсных торгах поставщик обязан представить выданные сторонними организациями справки. Если для своих собственных документов поставщик может самостоятельно изготовить электронный эквивалент и подписать его своей ЭЦП, то справки сторонних организаций изначально существуют только в бумажном виде. Поэтому необходим “электронный нотариат”, в функции которого входило бы изготовление электронных копий бумажных документов и заверение их своей ЭЦП. Ст 19.1 принятого закона, по-видимому, относится к организации такого нотариата.

3.8. Техническая реализация закона

Чтобы закон действительно заработал, должна быть выстроена достаточно солидная инфраструктура. Необходимо создать уполномоченный федеральный орган, надзирающий за всеми удостоверяющими центрами, организовать систему сертификации удостоверяющих центров и средств ЭЦП. Должна быть выработана правовая регламентация электронного нотариата, без которого невозможно взаимодействие бумажного и электронного документооборотов. Но прежде всего нужно конкретизировать положения закона применительно к PKI, разработав соответствующий профиль X.509. Учитывая перспективы международного сотрудничества, было бы желательно этот профиль по возможности приблизить к профилю квалифицирующего сертификата (RFC 3039), на который ориентируется ЕС. Это значительно облегчит взаимное признание иностранных сертификатов в электронной форме и соответствующих ЭЦП.

Только потом возможны разработка и сертификация аппаратного и программного обеспечения средств ЭЦП, и развертывание сети удостоверяющих центров

В Германии, уже имеющей разветвленную инфраструктуру электронной коммерции, сначала в 1997 г. был принят технический закон об ЭЦП (не имеющей юридической силы), в соответствии с которым под государственным контролем была развернута сеть удостоверяющих центров, и только через 4 года оказалось возможным принять закон, по которому ЭЦП приравнивалась к собственноручной подписи.

Трудно предсказать, сколько времени потребуется России, учитывая почти полное отсутствие инфраструктуры и отмеченные расхождения с международными стандартами, на прохождение по достаточно сложному пути реализации закона.

4. Реализация правовых отношений в системе электронных государственных закупок средствами PKI

Реализация правовых отношений в электронном документообороте возможна только при условии, что этот путь пройден: в России имеются сертифицированные удостоверяющие центры, издающие сертификаты и выполняющие все прочие предусмотренные законом функции, и организован электронный нотариат.

В [25] рассматриваются вопросы реализации системы электронных государственных закупок. В этой системе непосредственно участвуют следующие юридические лица:

- организатор электронных торгов (владелец сервера госзакупок);
- государственные заказчики;
- поставщики.

Предполагается, что все юридические лица — участники системы — обеспечены сертификатами ключей подписи, принадлежащими соответствующим уполномоченным должностным лицам. Там, где на бумажном документе должна быть собственноручная подпись должностного лица, на аналогичном электронном документе ставится ЭЦП этого лица, которая по закону равнозначна собственноручной. Следовательно, правильно подписанный электронный документ имеет такую же юридическую силу, что и бумажный.

Все юридически значимые действия участников подтверждаются электронными документами с их ЭЦП. При необходимости на документах проставляется отметка времени.

4.1. Публикация конкурсной документации госзаказчиком

Госзаказчик, желающий участвовать в системе электронных государственных закупок, должен предварительно зарегистрироваться на сервере госзакупок и получить права доступа (имя и пароль пользователя).

Права доступа должен знать только оператор госзаказчика, производящий удаленное редактирование конкурсной документации на сервере. Оператор, вообще говоря, не является должностным лицом, но только техническим работником и не может подписывать документы от имени госзаказчика. Зная права доступа, оператор может редактировать материалы конкурсов, принадлежащих только своему госзаказчику.

С каждым конкурсом, объявленным госзаказчиком, на сервере связаны два комплекта документов: рабочий (открытый для редактирования оператором по защищенному протоколу https, гарантирующему защиту от подделки и конфиденциальность) и опубликованный (открытый для всеобщего обозрения в Интернет по протоколу http). Непосредственно редактировать опубликованный комплект оператор не может. Первоначально у конкурса имеется только рабочий комплект. Для публикации рабочего комплекта необходимы полномочия (ЭЦП) соответствующего должностного лица. После публикации оператор может продолжать редактировать рабочий комплект, но при этом опубликованный комплект не меняется: для публикации выполненных изменений вновь требуется ЭЦП должностного лица.

В процессе редактирования оператор заполняет поля полученных с сервера форм и отправляет их на сервер. Сервер на этом основании автоматически генерирует некоторые конкурсные документы (на первом этапе реализации системы мы ограничимся автоматической генерацией только приглашения к участию в конкурсе). Остальные документы госзаказчик готовит самостоятельно и отправляет их на сервер, указывая в соотвествующих полях имена файлов.

Когда рабочий комплект готов к опубликованию, оператор запрашивает у сервера сводный документ, в котором отражены все данные, введенные при редактировании рабочего комплекта (значения всех полей, а также имена и даты всех отправленных файлов). Этот сводный документ подписан ЭЦП сервера, чтобы гарантировать неизменность рабочего комплекта. Любое изменение оператором рабочего комплекта после подписания сервером сводного документа аннулирует эту подпись.

Сигналом к публикации является отправление на сервер сводного документа, дополнительно подписанного ЭЦП должностного лица госзаказчика, уполномоченного для совершения этого действия. Сервер, получив подписанный сводный документ, проверяет, на месте ли *обе* подписи и не было ли изменений после подписания сервером, и публикует рабочий комплект (рис.8). Такая процедура гарантирует, что опубликованный комплект полностью соответствует подписанному госзаказчиком сводному документу, т.е. опубликовано именно то, что хотел опубликовать госзаказчик.

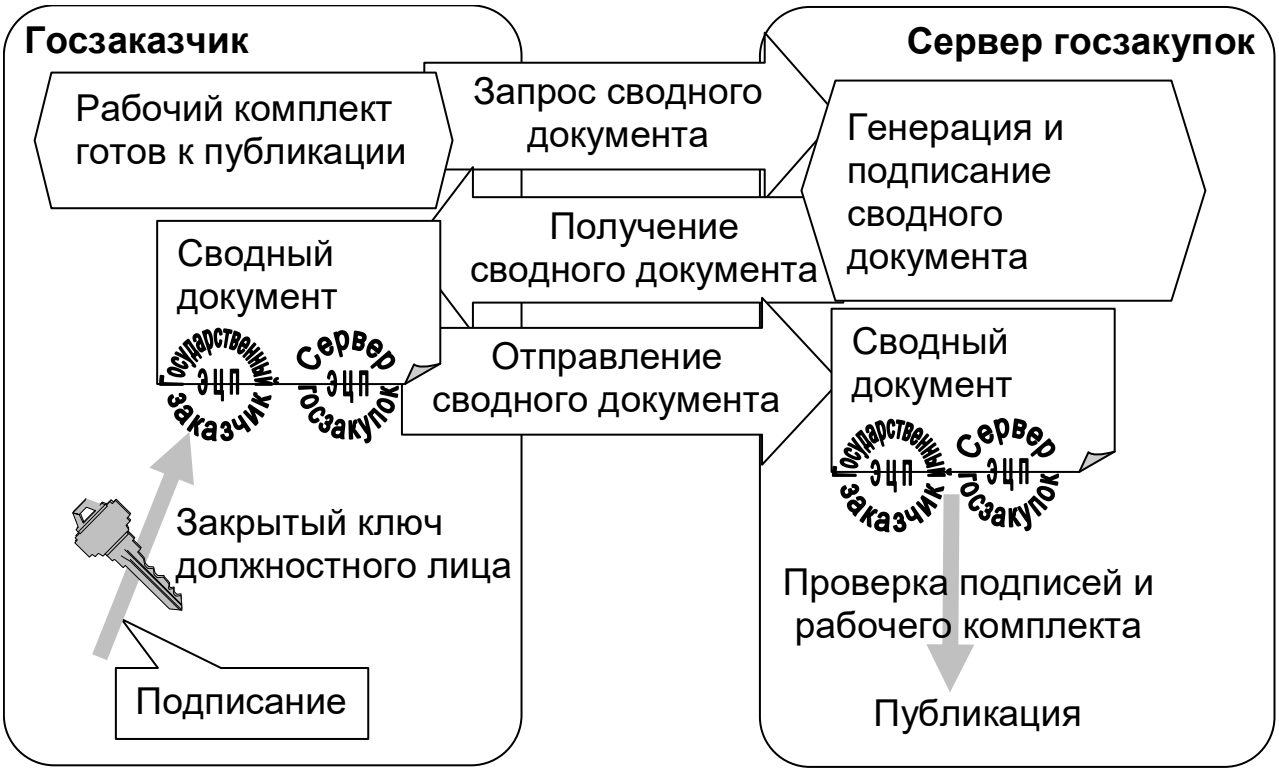

Рис. 8. Публикация рабочего комплекта.

4.2. Подача заявки поставщиком

На первом этапе реализации системы электронных государственных закупок поставщик своими средствами готовит документы на основе опубликованных на сервере образцов. При необходимости они подписываются ЭЦП поставщика. В комплект входят и документы третьих сторон. Эти последние документы, как правило, изначально существуют только в бумажной форме. Чтобы они могли участвовать в электронной системе, их необходимо преобразовать в электронную форму и заверить ЭЦП электронного нотариуса.

Организация электронного нотариата, вероятно, будет запаздывать. Поэтому на начальной стадии эксплуатации системы электронные документы третьих сторон можно и не включать в электронный комплект заявки, допуская электронный комплект *наряду* с традиционным бумажным. Затем, по мере развития инфраструктуры ЭЦП, предстоит, разумеется, отказаться от бумажного документооборота и полностью перейти на электронный.

При подаче электронной заявки необходимо обеспечить ее секретность. Никто не должен иметь возможность прочитать заявку до момента вскрытия заявок. С другой стороны, поставщик не должен иметь возможность заблокировать прочтение присланной им заявки, если он от нее не отказался до обусловленного срока, поскольку это налагает на него определенные обязательства.

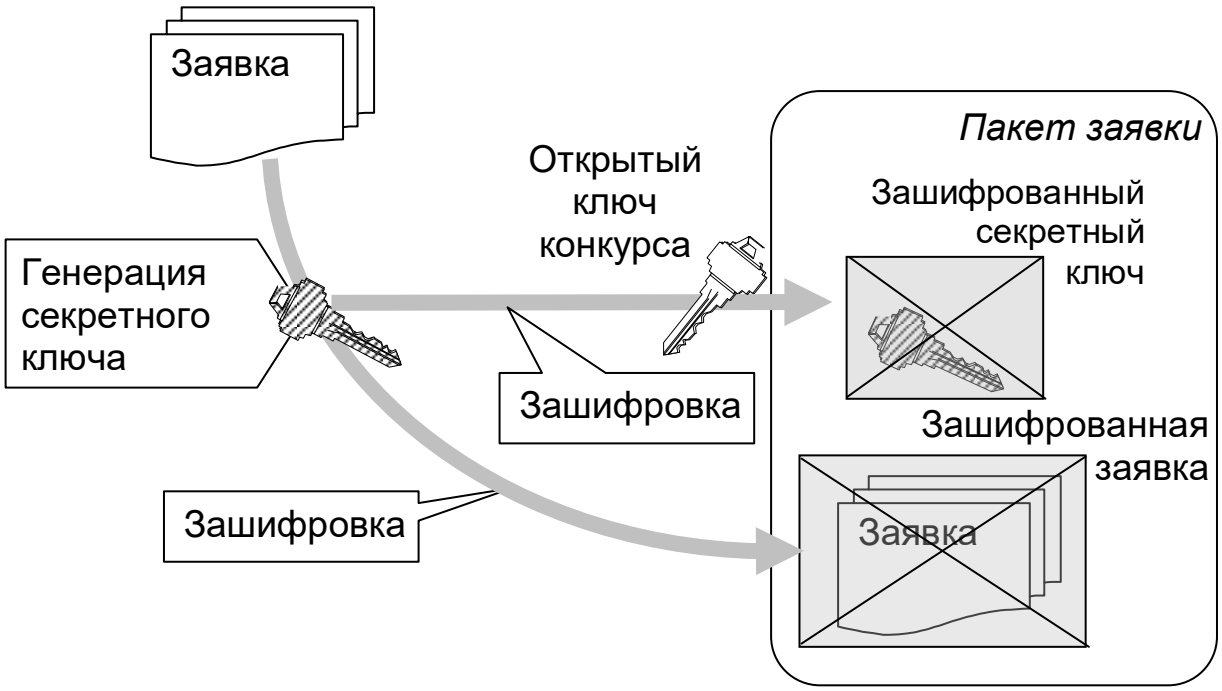

Рис. 9. Шифрование заявки.

Можно предложить следующий механизм обеспечения секретности до момента вскрытия заявок, обеспечивающий такой же уровень надежности, что и ЭЦП. Для каждого конкурса доверенный удостоверяющий центр по просьбе сервера госзакупок изготавливает асимметричную ключевую пару (ключи конкурса). Закрытый ключ конкурса удостоверяющий центр сохраняет в тайне до момента вскрытия заявок. Открытый ключ конкурса передается серверу для зашифровки поступающих заявок.

Подготовив комплект документов заявки, поставщик архивирует его и пересылает на сервер госзакупок по защищенному протоколу https (обеспечивающему конфиденциальность и целостность). Никто посторонний не может ни перехватить, ни изменить передаваемую заявку. В ответ сервер присылает поставщику квитанцию о приеме заявки, подписанную ЭЦП сервера и снабженную печатью времени. В квитанции содержится идентификатор, присваиваемый каждой поступившей заявке, который используется поставщиком при посылке исправлений или при отказе от заявки. Получив комплект заявки, сервер “на лету” генерирует секретный симметричный ключ и шифрует им принятый комплект. Вместе с комплектом заявки сохраняется и секретный ключ, зашифрованный посредством открытого ключа конкурса. Сам же секретный ключ уничтожается сразу после зашифровки. Возможна следующая модификация предложенной схемы: генерация секретного ключа и шифрование заявки выполняются на стороне поставщика с помощью специализированных средств, обеспечивающих

немедленное уничтожение секретного ключа. На сервер пересылается уже зашифрованные заявка и секретный ключ. Такой вариант исключает всякие сомнения в том, что секретный ключ, посредством которого зашифрована заявка, известен персоналу сервера госзакупок. В этом случае открытый ключ конкурса должен быть опубликован в конкурсной документации.

Исправления заявки подписываются, архивируются и шифруются точно так же, как и сама заявка. Отказ от заявки, включающий ее идентификатор, должен быть подписан ЭЦП поставщика, чтобы он имел юридическую силу и для предохранения от злоумышленников. В ответ на исправления или отказ сервер присылает квитанцию, подписанную ЭЦП сервера.

На заявке, исправлениях, отказе и всех квитанциях, возвращаемых сервером, ставится отметка времени.

Зашифрованные заявки и исправления (вместе с зашифрованными секретными ключами) хранятся на сервере. Вообще говоря, нет никакой необходимости хранить их в защищенном хранилище.

Прочитать заявку, хранящуюся на сервере, не может никто (в том числе и персонал сервера), не знающий закрытого ключа конкурса, тайна которого известна только доверенному удостоверяющему центру. Недостатком предложенной схемы является отсутствие государственных стандартов на асимметричное шифрование (в отличие от ЭЦП и симметричного шифрования). Поэтому программные средства, реализуюшие эту схему, не могут быть сертифицированы. Также не вполне ясно, входит ли услуга по хранению в тайне закрытого ключа конкурса в число иных связанных с использованием ЭЦП услуг, которые может предоставлять удостоверяющий центр (ст. 9.1 закона об ЭЦП). Если удостоверяющий центр не возьмется за предоставление такой услуги, то придется для этого создавать специализированную структуру. Главное — отделить ответственность за сохранение тайны заявок от ответственности за их прием, которую несет сервер госзакупок.

Схема, аналогичная предложенной, использована в системе государственных электронных торгов Австралии (Commonwealth Electronic Tender System) [26] — одной из стран, лидирующих в области электронизации госзакупок.

4.3. Вскрытие заявок

Когда настает момент вскрытия заявок, сервер (или его персонал) получает у доверенного удостоверяющего центра закрытый ключ конкурса и расшифровывает им секретные ключи хранящихся на сервере заявок, а посредством их и сами заявки (рис. 10). Поставщик, если он вовремя не отозвал заявку, никак не может воспрепятствовать ее вскрытию и безнаказанно отказаться от своих обязательств.

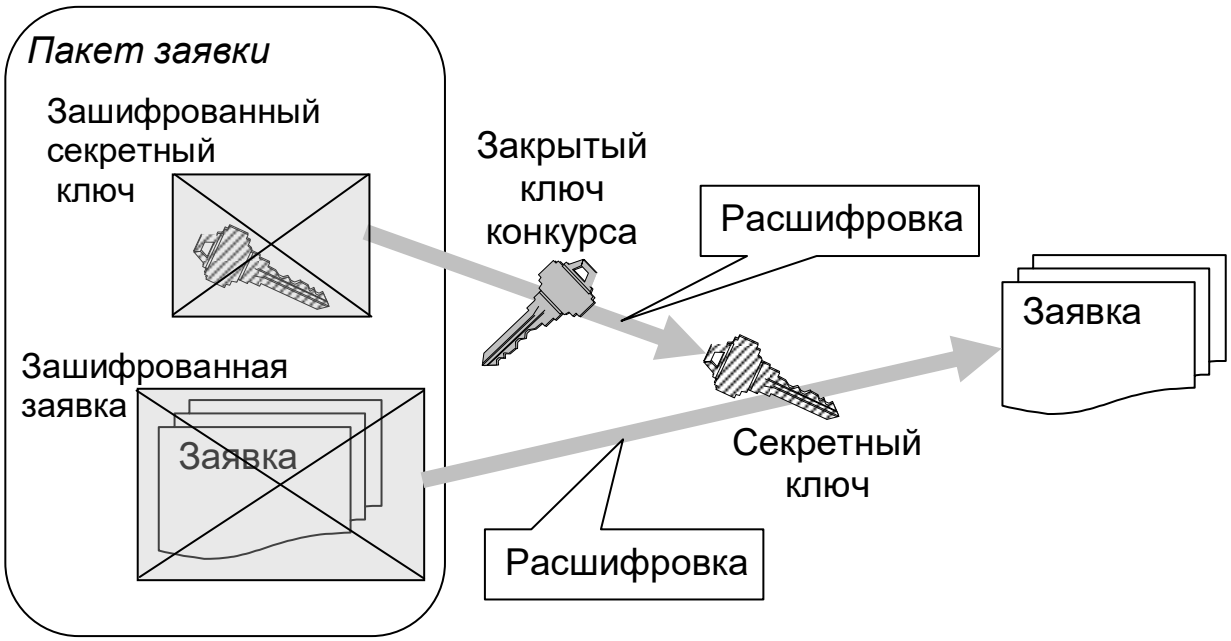

Рис. 10. Вскрытие заявки закрытым ключом конкурса.

5. Заключение

Нельзя не признать, что вступление в силу российского закона об электронно-цифровой подписи является одним из ключевых обстоятельств, позволяющих с оптимизмом оценивать перспективы построения в России системы электронных государственных закупок. Однако и вопросов новый закон породил немало. Часть из них была так или иначе затронута в данной работе.

Среди неупомянутых вопросов наиболее острые — о конкретике отношений между строящейся системой госзакупок и удостоверяющими центрами. Когда появятся первые удостоверяющие центры, действующие в соответствии с законом об ЭЦП? В какой степени их возможности будут отвечать запросам системы государственных закупок? Потребуется ли образование специализированного корпоративного удостоверяющего центра госзакупок? Хочется верить, что ответы на эти вопросы удастся получить уже в текущем, 2002 году.

Определенный оптимизм вселяют уже состоявшиеся первые шаги в направлении технической реализации закона об ЭЦП. Так, 14 марта 2002 г. на сервере российской компании "Новый Адам", специализирующейся на разработке защищенных информационных систем, появился документ "Состав сертификата открытого ключа ЭЦП" [24], содержащий проект профиля российского сертификата. В преамбуле документа говорится: «В настоящее время силами двух компаний — "Новый Адам" и "Сигнал-КОМ" начаты работы по согласованию структуры и формата полей сертификата, удовлетворяющего положениям статьи 6 Закона об ЭЦП и максимально соответствующего международному стандарту X.509 и Рекомендациям RFC

2459, RFC 3039. Данный вариант документа передан на согласование в ФАПСИ».

* * *

С рукописью настоящей работы ознакомились Г.Т.Артамонов, М.М.Горбунов-Посадов, Д.А.Корягин, С.М.Муругов, А.П.Полежаев. Авторы выражают им свою глубокую признательность за проявленный интерес и множество полезных замечаний.

Авторы чрезвычайно благодарны А.Б.Виссарионову, Н.В.Нестеровичу и В.И.Смирнову за всестороннее обсуждение процедуры электронного вскрытия конвертов с конкурсными заявками.

Литература

1. *Н.В.Нестерович, В.И.Смирнов.* Конкурсные торги на закупку продукции для государственных нужд. — М.: Инфра-М, 2000. — 360 с.
2. *М.М.Горбунов-Посадов, А.В.Ермаков, Д.А.Корягин, Т.А.Полилова.* Предпосылки развертывания электронных торгов для государственных нужд. Препринт ИПМ им. М.В.Келдыша РАН, 2001, № 38. — 16 с.
3. Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». Российская газета. № 6, 12 января 2002 г. — http://www.rg.ru/oficial/doc/federal_zak/1-fz.shtm
4. *В.Столлингс.* Криптография и защита сетей: теория и практика. М: Вильямс. 2001. Пер. с англ. — 669 с.
5. *А.Ростовцев, Е.Маховенко.* Введение в криптографию с открытым ключом. М: Интерлайн. 2001. — 335 с.
6. *R.Rivest, A.Shamir, L.Adleman.* A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21 (1978), pp. 120-126.
7. *M.J.B.Robshaw, Yigun LisaYin.* Elliptic Curve Cryptosystems. RSA Laboratories Technical Note. June 27 1997. — http://www.rsasecurity.com/rsalabs/ecc/elliptic_curve.html
8. ГОСТ Р 34.10-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.
9. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры формирования и проверки электронной цифровой подписи.
10. Federal Information Processing Standards Publication (FIPS PUB) 186, Digital Signature Standard, 18 May 1994.
11. *W.Diffie, M.E.Hellman.* New directions in cryptography. IEEE Transactions on Information Theory, 22 (1976), pp. 644-654.
12. ITU-T Recommendation X.509 (1997 E): Information Technology — Open Systems Interconnection — The Directory: Authentication Framework, June 1997.
13. Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459). — http://www.ietf.org/rfc/rfc2459.txt

14. Public-Key Infrastructure (X.509) (pkix) Charter. — http://www.ietf.org/html.charters/pkix-charter.html

15. DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities. L 13, 19.1.2000, p.12-20. — http://europa.eu.int/ISPO/ecommerce/legal/documents/1999_93/1999_93_en.pdf

16. Internet X.509 Public Key Infrastructure Qualified Certificates Profile (RFC 3039). — http://www.ietf.org/rfc/rfc3039.txt

17. S/MIME Mail Security. http://www.ietf.org/html.charters/smime-charter.html

18. *A.Freier*, *P.Karlton*, *P.Kocher*. The SSL Protocol. Version 3.0. Internet Draft. Netscape Communication Corporation. Nov 18 1996. — http://home.netscape.com/eng/ssl3/draft302.txt

19. The TLS Protocol Version 1.0 (RFC 2246). — http://www.ietf.org/rfc/rfc2246.txt

20. Secure Electronic Transaction (SET) Specifications. Version 1.0. May 31 1997. — http://www.setco.org/download/set_bk3.zip

21. IP Security Protocol. http://www.ietf.org/html.charters/ipsec-charter.html

22. Проект закона “Об электронной цифровой подписи”. — http://www.netoscope.ru/documents/2000/08/04/32.html

23. German Digital Signature Law. Translated by Christopher Kuner. — http://www.kuner.com/data/sig/digsig4.html

24. Состав сертификата открытого ключа ЭЦП. — http://www.adam.ru/Pki/cert.phtml

25. *М.М.Горбунов-Посадов, А.В.Ермаков, Д.А.Корягин, Т.А.Полилова.* Программное обеспечение государственных закупок. Препринт ИПМ им. М.В.Келдыша РАН, 2001, № 46. — 16 с.

26. Commonwealth Electronic Tender System. — http://www.tenders.gov.au/aboutus/index.html