В. А. Конявский

ИДЕНТИФИКАЦИЯ И ПРИМЕНЕНИЕ ЭЦП В КОМПЬЮТЕРНЫХ СИСТЕМАХ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Базовые положения

1. Информационное общество — это общество, в ВВП которого доля информационного производства (производства информационного продукта — электронных документов) заметна (т. е. составляет, по крайней мере, 10—15 %).

2. «Электронное правительство» — это информационная система (взаимодействующая совокупность информационных систем), обеспечивающая доверенное взаимодействие граждан и государства. Нельзя трактовать «электронное правительство» как социальную систему. Необходимо реализовывать социальные функции в технической системе.

3. Техническая система должна в первую очередь обеспечивать информационную поддержку отношений, возникающих в обществе, а не пытаться изменить их. Попытка изменить общественные отношения с мотивацией «так удобно вычислительному центру» кажется, как минимум, необоснованной.

4. В процессах информационного взаимодействия доверие — это базовая характеристика. Она обеспечивается технологией и **только** технологией.

5. Информационные технологии обеспечения доверия в технических системах существенно зависят от социально-экономических задач, решаемых с помощью технической системы, и возникающих при этом отношений.

Доверять можно только тому участнику взаимодействия, который, так или иначе, известен. Анонимному участнику взаимодействия доверять невозможно. Перед началом взаимодействия участник должен идентифицироваться и аутентифицироваться — проверить идентификацию.

Аутентификация — понятие относительное. Что-то одно можно аутентифицировать относительно чего-то другого, нельзя аутентифицировать что бы то ни было само по себе.

Таким образом, в процессе аутентификации участвуют не менее двух сторон. Если это стороны А и Б, то:

- А можно аутентифицировать относительно Б;
- Б можно аутентифицировать относительно А;
- Стороны А и Б можно аутентифицировать одну относительно другой — взаимно аутентифицировать.

Чем выше защищенность стороны, тем с большим основанием ей можно доверять. Незащищенной стороне можно только поверить, но проверить идентификацию можно только в том случае, если сторона защищена.

Если А — человек, а Б — одна из компьютерных систем информационного общества, то перечисленные выше варианты исчерпывают варианты аутентификации в информационном обществе.

Применение ЭЦП и авторизация граждан в системах электронного правительства

При анализе применимости тех или иных механизмов идентификации/аутентификации (ИА) для целей электронного правительства (ЭП) важен не столько выбор типа идентификатора, сколько обоснование того, какие именно услуги можно предоставить гражданину, идентифицировавшемуся тем или иным способом. Действительно, многие граждане уже имеют средства идентификации — ими могут быть любые банковские пластиковые карты, социальные карты, Универсальная электронная карта, USB-идентификаторы, TM-идентификаторы, отпечатки пальцев, номер мобильного телефона, логин и пароль e-mail и многое другое. Пользуясь идентификацией на основе этих средств, граждане получают немало услуг, и эти услуги зачастую весьма значимы. Можно управлять **своим** счетом, можно войти **к себе** домой или **к себе** на работу, можно открыть **свой** сейф, чтобы взять или положить **свои** документы.

Иначе дело обстоит тогда, когда гражданин обращается в госорганы. Здесь недостаточно идентифицироваться ключом от подъезда. Для того чтобы получить водительское удостоверение, диплом, зарегистрировать собственность, нужен паспорт. Информационные ресурсы в системах ЭП — государственные ИР, и своими для любого гражданина они являются лишь в части персональных данных.

Доступ к чему-то своему гражданин может осуществлять так, как хочет. Для изменения своих прав и волеизъявления — он должен предъявить паспорт.

Во втором случае более строгие методы авторизации применяются лишь по той причине, что волеизъявление и изменение прав могут оказать влияние не только на гражданина, выступающего в данный момент субъектом отношений, но и на многих других членов гражданского общества.

Для того чтобы идентифицироваться в платной справочной службе и узнать, во сколько и откуда отходит поезд, достаточно позвонить с частного телефона, номер которого определяется АОНом. А вот внести расписание движения поездов в компьютерную систему можно только в том случае, если оно заверено подписью должностного лица — иначе неприятностей не оберешься.

Эти два случая отличаются не содержанием данных, а направлением их движения — **из** системы или **в** систему.

Только при установлении наличия и подлинности правоустанавливающих документов можно изменить **в** системе состав данных о собственности и персональных данных гражданина. Наличие тех или иных прав у одного человека существенно влияет на права других людей. Именно поэтому волеизъявление (понимаемое как изменение правоотношений), изменение прав и персональных данных фиксируются в информационной системе только при предъявлении документов, т. е. сведений, снабженных реквизитами, фиксирующими факты, в этих сведениях содержащиеся.

Подлинность подписи на бумаге устанавливается визуальными, приборными и криминалистическими методами. Цель — убедиться в достоверности волеизъявления гражданина.

В цифровом мире роль подписи выполняет криптографическое преобразование, которое называется ЭЦП — электронная цифровая подпись. При этом достоверность ЭЦП обеспечивается доверенной средой выполнения процедуры подписи, и поэтому достоверной ЭЦП является только та ЭЦП, которая устанавливается на доверенном компьютере. Недостаточно использовать сертифицированные средства ЭЦП, необходимо также, чтобы компьютер был доверенным. Это требование обеспечивается процедурами проверки правильности встраивания.

Компьютер может быть доверенным лишь в том случае, если осуществляется доверенная загрузка проверенной ОС и обеспечивается изолированность программной среды. Обычно для этого используется аппаратный модуль доверенной загрузки (АМДЗ) — сложное и недешевое изделие. Альтернативой является организация доверенного сеанса связи, т. е. проверенная ОС и минимальный набор ПО загружаются со специального носителя, гарантирующего целостность своего содержимого — средство обеспечения доверенного сеанса (СОДС). Цена такого решения в три раза меньше, чем при использовании АМДЗ.

Другие методы создания доверенной среды исполнения ЭЦП неизвестны.

Для нужд электронного правительства могут применяться различные методы ИА. Человек вправе сам выбрать, какой метод авторизации достаточен для того, чтобы просто, недорого и с достаточной надежностью получать данные **из** системы. Иначе обстоит дело с включением данных **в** состав системы ЭП. Источник этих данных должен быть зафиксирован, следовательно, они должны быть подписаны, значит, должны поступать **из** доверенной системы.

Из доверенной системы должны поступать:

- регистрационные данные и данные об изменении параметров регистрации (персональных данных);
- данные, содержащие волеизъявление граждан;
- данные об изменение прав;
- данные, содержащие сведения о юридических фактах.

Эти данные должны быть подписаны в доверенных системах или в доверенных сеансах.

Таким образом:

- если обеспечивается доверенное взаимодействие, то могут предоставляться любые услуги;
- если доверенное взаимодействие не обеспечивается, то могут предоставляться только те услуги, риски по которым

А) допустимы для системы ЭП

Б) приемлемы для гражданина.

Только в доверенной среде могут предоставляться услуги, связанные с:

- волеизъявлением граждан;
- управлением собственностью;
- управлением персональными данными.

Только в доверенной среде взаимодействуют с системами ЭП смежные подсистемы и должностные лица.

Отсюда вытекают инфраструктура аутентификации и требования к реализации входа на портал.

Инфраструктура аутентификации и требования к реализации входа на портал

Должностные лица используют компьютеры, снабженные АМДЗ, или используют СОДС.

АМДЗ или СОДС могут использовать и граждане, тогда они имеют полный доступ к услугам ЭП.

Во всех остальных случаях граждане регистрируются **на защищенных терминалах ЭП** (инфоматах, банкоматах, почте и т. д.).

При регистрации указывается выбираемый гражданином механизм идентификации и согласовывается тот перечень услуг, который может быть при этом получен.

Что надо сделать

Для реализации описанного подхода необходимо:

- перечислить все услуги электронного правительства гражданам;
- классифицировать их по принципам, описанным выше, т. е. разделить на услуги информирования и доверенные;

- попытаться услуги информирования классифицировать по степеням важности, с тем чтобы поставить в соответствие различным идентификаторам различные (пересекающиеся, и даже расширяемые) группы услуг;
- систему идентификации и аутентификации проектировать с учетом наличия доверенного взаимодействия и возможности предоставления различных наборов услуг гражданам, использующим различные методы авторизации, вплоть до полного набора услуг;
- исходя из такого подхода доработать модели нарушителя и угроз;
- для организации доверенного взаимодействия разработать пункты доступа в защищенном исполнении, а для наиболее активных категорий граждан предложить использовать технологию доверенных сеансов.

Про ЭЦП и принципы ее использования

ЭЦП использует ключ подписи (КП), который принципиально не должен быть никому известен, поскольку именно он обеспечивает свойства ЭлД, связанные с тем, что снабдить документ ЭЦП может только его автор или владелец.

Отсюда следует **принцип обеспечения сохранности КП**, который в сертификатах формулируется как аксиома («…при сохранении в тайне ключа подписи»).

Процедура ЭЦП всегда используется в некоторой системе, обеспечивающей целевую функцию обработки ЭлД, включающую снабжение и проверку ЭЦП в ЭлД. То есть это всегда подсистема системы более высокого уровня.

Со стороны подсистемы реализации ЭЦП вся остальная система является внешним окружением и потенциально враждебна с точки зрения сохранности КП. Попадание КП во враждебную среду эквивалентно его компрометации, и чем меньший интервал времени КП находится во враждебной среде, тем ниже вероятность неблагоприятного исхода.

Таким образом, можно сформулировать важный **принцип минимального присутствия КП в окружении**.

Потенциальная враждебность несертифицированного по параметрам безопасности внешнего окружения сертифицированных СКЗИ необходимо требует проверки правильности встраивания СКЗИ в компьютерную систему. Действительно, даже при использовании проверенных и сертифицированных СКЗИ возможна утрата и/или модификация критичной информации еще до СКЗИ. Этот принцип можно назвать **принципом правильности встраивания**. Контроль за соблюдением данного принципа осуществляет регулятор на основе имеющихся требований.

Принцип минимального присутствия в системе необходимо применять на протяжении всего жизненного цикла КП. Именно поэтому принцип минимального присутствия может быть реализован в полной мере лишь в том случае, когда ЭЦП реализована в отдельном устройстве, не имеющем общей памяти с окружением. При этом КП обрабатывается локально, не допуская перемещения информации о КП в другие части системы. Назовем такой подход **принципом локальной реализации**. Принцип локальной реализации предопределяет реализацию алгоритма ЭЦП в отдельном устройстве как предпочтительную. Следование принципу локальной реализации существенно уменьшает затраты на реализацию принципа правильности встраивания.

Вовне подсистемы реализации используется (отчуждается) ключ проверки (КПр) ЭЦП, который оформляется в виде, подтверждающем связь КП–КПр (в виде сертификата или иным образом).

Это следующий основополагающий принцип реализации ЭЦП – **принцип однозначной связи ключа подписи и ключа проверки**. Совместно с принципом обеспечения сохранности КП принцип однозначной связи КП и КПр обеспечивает целостность связи «человек – ключ подписи – ключ проверки».

Актуальна также проблема противодействия целевой компрометации КП. Суть состоит в необходимости обеспечить условия, при которых воздействие методами социальной инженерии (давление, подкуп, шантаж) не приводило бы к выделению КП из системы, его отчуждению и передаче третьи лицам. Проблема противодействия целевой компрометации решается изолированностью КП, его неизвлекаемостью из контейнера, в котором КП хранится. Действительно, в том случае, когда КП изолирован в отдельном устройстве, его отчуждение, передача третьи лицам невозможны. Тем самым снимается и нагрузка с владельца ЭЦП, который не может подвергаться внесистемным методам воздействия для компрометации ЭЦП. Таким образом, формулируется **принцип изолированности КП**[1].

Каждая ключевая система предполагает определенные ограничения по условиям применения ключей, при нарушении которых ключи могут быть скомпрометированы и/или само применение СКЗИ может быть поставлено под сомнение. Именно поэтому криптографические ключи должны применяться в соответствии с тем назначением, для которого они были выработаны, даже если технически возможно их гораздо более широкое применение. Конечно, это не означает, что ключи придется носить в связке, как папуасские бусы. Носитель криптографических ключей может быть один, но ключей на нем может храниться много. Конечно, при условии неизвлекаемости ключей, как и было описано выше.

Участие пользователя в нескольких группах целевой деятельности предопределяет **принцип многоконтурности реализации криптографических модулей**, который связан с тем, что в одном аппаратном устройстве должно храниться несколько КП, должно быть реализовано несколько криптографических алгоритмов и должны присутствовать несколько технологически разных СКЗИ, например для аутентификации, канального шифрования, обновления ПО и т. д. В свою очередь, реализация принципа многоконтурности СКЗИ требует расширения принципа связи КП и КПр до **принципа связи ключей с условиями их применения.**

Еще один аспект применения ЭЦП можно проиллюстрировать следующим вопросом: «Является ли документом сообщение, подписанное подлинной ЭЦП»? Если исходить из того, что подлинность подписи обеспечивает юридическую значимость документа, то ответ будет положительным. Проверяем подпись, удостоверяемся в ее правильности и считаем сообщение документом. Но будет ли являться юридическим фактом закон, подписанный не подписью президента, а подписью владельца соседнего ларька? Несмотря на подлинность подписи, нет. Отсюда вытекает следующий фундаментальный принцип — **принцип связи КП с должностными обязанностями владельца ключа**. Этот принцип существенно отличается от предыдущих — он носит динамический характер (должностные полномочия изменяются во время жизни ключа), а все предыдущие — статический. Поэтому принцип связи КП с должностными обязанностями должен контролироваться не только при регистрации ключевой пары, а при всех основных транзакциях. Значит, в системе должен присутствовать Реестр должностных лиц, в котором отражается актуальное состояние должностных лиц, правомочий и полномочий.

Реализация сформулированных выше принципов позволяет гарантировать доверенную реализацию ЭЦП и, как естественное следствие, создавать предпосылки для реализации доверенного, защищенного, безопасного взаимодействия гражданина и компьютерных систем информационного общества.

Фундаментальным понятием безопасности (защищенности) является доверие. Это связано с человеком как субъектом безопасности. Любая защита, сколь бы надежной она ни была, не создаст ощущения безопасности, если человек ей не доверяет.

[1] Может показаться, что принцип изолированности нарушает права владельца КП, однако это не так. Вполне можно использовать КП, не зная его. Каждый может привести примеры множества вещей, которые он использует, не зная (или зная только частично), как они устроены.

И наоборот. Если человек доверяет плохому продукту, у него возникает ощущение безопасности. Но это в данном случае играет отрицательную роль — безосновательная успокоенность при реальной незащищенности обычно приводит к печальным последствиям.

Доверие обеспечивается доверием к технологии обработки, например применением ЭЦП или применением специальных каналов доставки. В подлинности купюры, получаемой в Сбербанке, можно не сомневаться, хотя ЭЦП она не содержит. Банкноты в руках рыночного торговца могут требовать проверки.

Да-да-нет-да

Доверие тем труднее обеспечить, чем выше уровень недоверия в обществе. Иногда для сделки достаточно только репутации участников, а зачастую недостаточно даже страхового полиса. Дальнейшие рассуждения мы приводим, исходя из существующего (здесь и сейчас) уровня недоверия.

Доверие обеспечивается двумя составляющими — возможностью проверки и продолжительным положительным опытом. Опыта (продолжительного положительного) применения ЭЦП пока нет. Сосредоточимся на возможности проверки. Для этого представим себе, что мы получили сообщение, подписанное ЭЦП некоторого должностного лица. Теперь мы должны ответить на ряд вопросов, вытекающих из приведенных выше принципов, а именно:

- в каких условиях хранились криптографические ключи,
- правильно ли выполнено встраивание СКЗИ в ИС,
- какому классу соответствует СКЗИ,
- какой класс СКЗИ использовался для выработки ЭЦП,
- является ли человек, подписавший документ, должностным лицом,
- имеет ли право подписывать документы такого рода должностное лицо, подписавшее документ.

Если ответы на все эти вопросы будут положительными, то только потом можно ответить на основную группу вопросов, а именно:

- верна ли ЭЦП под сообщением,
- установлено ли авторство сообщения.

И наконец, финальный вопрос, ради чего все и затеяно: «Является ли данное сообщение документом?»

Чтобы ответить на эти вопросы, нужно либо точно знать, как устроена ИС абонента, либо получить нужные сведения из сертификата открытой подписи.

Можно ли по ЭЦП определить, в каких условиях она вырабатывалась?

Нет.

Большинство популярных СКЗИ сертифицировано сегодня по двум классам — КС1, если они используются на незащищенном компьютере, и КС2, если они установлены на компьютере с сертифицированным электронным замком, обеспечивающим доверенность среды применения СКЗИ и контроль целостности СКЗИ, как минимум.

Получив сообщение, подписанное ЭЦП с помощью такой СКЗИ, невозможно определить, устанавливалась ЭЦП в доверенной среде или в недоверенной. Тем более нельзя установить, в какой среде хранились ключи, как они вырабатывались, не изменились ли за последнее время должностные обязанности лица, подписавшего сообщение, и т. д., и т. п.

Ответ на вопрос подзаголовка однозначен: «Нет».

Проблема проприетарности

ИС информационного общества создаются для оказания услуг гражданам, для снижения нагрузки (временной, эмоциональной, коррупционной) на граждан, связанной с их взаимодействием с государством.

С системами граждане взаимодействуют, явно или неявно используя те или иные протоколы. Протоколы могут быть общеизвестные, открытые, а могут быть проприетарные, фирменные, нераскрываемые.

В первом случае цена доступа регулируется рынком. Во втором она становится практически налогом (скорее, сбором) с населения в пользу одной компании.

Протоколы должны быть открытыми.

Инфраструктура открытых ключей

Применение ЭЦП обеспечивается специальными средствами и технологиями, которые в совокупности называются PKI — Public Key Infrastructure, инфраструктура публичных ключей. В российской традиции применяется аббревиатура ИОК — инфраструктура открытых ключей.

Известно два типа ИОК — иерархическая и сетевая. Иерархическая основана на идеологии «цифровых паспортов». Она поддерживается системой удостоверяющих центров (УЦ). Сертификат ЭЦП в этом случае представляет собой КПр владельца ЭЦП с дополнительными реквизитами, подписанный подписью УЦ, которая содержит открытый ключ УЦ верхнего уровня, подписанный… и т. д. По цепочке сертификатов, дойдя до «корневого УЦ», можно удостовериться, что ключ корневого УЦ подписан уполномоченным лицом уполномоченного федерального органа (УФО). Можно ли при этом поверить, что волеизъявление действительно было? Наверное, можно. Если, конечно, к этому моменту не будет принято решение о расформировании УФО, передачи его функций другому федеральному органу, а человек, ранее бывший уполномоченным лицом бывшего УФО, не перешел на другую работу.

Заметим, что цепочка сертификатов может быть очень длинной, а общее решение будет положительным, если положительны все проверки, т. е. решения по каждому сертификату цепочки объединяются союзом «И».

Этим объясняются недостатки иерархической системы: порождение значительного непроизводительного трафика, создание абсурдных ведомственных УЦ и даже УЦ отдельных организаций, а также отсутствие нормальной мотивации к доверию ЭЦП. Практически это воплощенная в технике идея недоверия — поверить можно только тогда, когда все без исключения единогласно это подтверждают. А «моя хата — с краю».

В случае сетевой системы используется не идеология «цифровых паспортов», а идеология «отпечатков пальцев», как идиома поручительства — «я ручаюсь, что этот открытый ключ принадлежит именно тому, чье имя указано в сертификате». Если среди множества таких «отпечатков» пользователь обнаруживает «отпечаток» знакомого ему человека, у него появляются основания доверять подписи под документом. Объединение по «ИЛИ» значительно сокращает непроизводительный трафик. Удостоверить принадлежность открытого ключа человеку может другой человек, убежденный в этой принадлежности.

Сетевая система лишена недостатков иерархической. Более того, в качестве ряда «отпечатков» могут использоваться подписи УЦ. Таким образом, сетевая система ИОК шире иерархической и включает ее в себя. Обратное неверно.

В России используется иерархическая система.

Это происходит потому, что PKI в нашей стране получает распространение через государственные институты к общественным, а не наоборот.

В разных коммуникациях должны применяться разные механизмы аутентификации. При обращении, например, к нотариусу нас будут в первую очередь интересовать официальные подтверждения его полномочий и квалификации, а его — наш паспорт, а при найме няни для ребенка для нас будут иметь значение рекомендации конкретных людей, а не нотариуса. Человек имеет право сам определять, в какой роли он выступает в каждом конкретном случае. В случае с

инфраструктурой открытых ключей должна быть предоставлена возможность выбора уместного и удобного способа взаимодействия.

Чего ждать?

1. Изменения требований к СКЗИ.

2. Отказа от программных контейнеров, переход к аппаратным, что повлечет за собой появление новых, более эффективных СКЗИ.

3. Изменения структуры сертификата, и, соответственно, новых требований к УЦ и ЕПД в целом.

4. Создание реестра должностных лиц с актуализацией полномочий и правомочий.

5. Появление альтернативной PKI – PKI для гражданского общества.

Ожидаемые изменения перечислены в порядке предполагаемой реализации.