Идентификация в области электронного правительства

В.А. Конявский
А.В. Чугринов

Базовые положения

- Информационное общество
  - общество, в ВВП которого заметна доля информационного продукта (10-15%)
- Электронное правительство
  - совокупность информационных систем, обеспечивающая доверенное взаимодействие граждан и государства
  - ЭП – не социальная система, социальные функции – в технической системе
- Техническая система
  - обеспечение поддержки общественных отношений, но не попытка изменить их
- Доверие
  - базовая характеристика процессов информационного взаимодействия, обеспечивается только технологией
- Информационные технологии обеспечения доверия в технических системах
  - существенно зависят от социально-экономических задач, решаемых с помощью технической системы, и возникающих при этом отношений

Доверие и аутентификация

- Доверять можно только известному участнику взаимодействия
- Доверять анонимному участнику взаимодействия нельзя
- Аутентификация относительна:
  - А можно аутентифицировать относительно Б
  - Б можно аутентифицировать относительно А
  - А и Б можно взаимно аутентифицировать
- Пример: А – человек, Б – компьютерная система информационного общества

Идентификация граждан в системах ЭП

- Имеющиеся у граждан идентификаторы:
  - банковские карты, социальные карты, УЭК, USB-идентификаторы, ТМ-идентификаторы, отпечатки пальцев, номер телефона и др.
- Услуги, доступные с помощью имеющихся идентификаторов:
  - управление **своим** счётом, доступ к **себе** домой и к **себе** на работу и др.
- Доступ к услугам государственных органов
  - с использованием паспорта
- В целом:
  - доступ к **своему** – по выбору гражданина
  - волеизъявление – паспорт

Направление движения данных

- Из системы:
  - доступ гражданина к своим данным не влияет на права других людей
  - аутентификация – по выбору гражданина
- В систему:
  - изменение прав у одного человека существенно влияет на права других людей
  - волеизъявление, изменение прав и персональных данных – только при предъявлении документов с подтверждающими реквизитами (пример – подпись)

Электронная подпись

- Электронный реквизит, подтверждающий подлинность и авторство электронного документа
- Достоверность электронной подписи обеспечивается доверенной средой выработки:
  - доверенный компьютер (доверенная загрузка ОС и изолированность программной среды)
    - аппаратный модуль доверенной загрузки
    - доверенный сеанс связи
  - сертифицированное СКЗИ
  - корректность встраивания

Включение данных **в** состав системы ЭП

- Источник данных должен быть зафиксирован – данные 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 изменении прав
  - данные, содержащие сведения о юридических фактах
- Эти данные должны быть подписаны в доверенных системах или в доверенных сеансах

Предоставление услуг

- Если обеспечивается доверенное взаимодействие, могут предоставляться любые услуги
- Если доверенное взаимодействие не обеспечивается, то могут предоставляться только те услуги, риски по которым:
  - допустимы для системы ЭП
  - 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

Инфраструктура аутентификации и требования к реализации входа на портал

- Должностные лица используют компьютеры, снабжённые аппаратными модулями доверенной загрузки (АМДЗ) или используют средства обеспечения доверенного сеанса связи (СОДС)
- Если АМДЗ или СОДС используют граждане, то они имеют полный доступ к услугам ЭП
- Во всех остальных случаях граждане регистрируются на защищённых терминалах ЭП (инфоматах и др.)
- При регистрации указывается выбираемый гражданином механизм идентификации и согласовывается перечень получаемых при этом услуг

Что надо сделать?

- Перечислить все услуги ЭП гражданам
- Разделить услуги на услуги информирования и доверенные
- Классифицировать услуги по степеням важности, с тем чтобы поставить в соответствие различным идентификаторам различные группы услуг
- Спроектировать систему ИА с учётом доверенного взаимодействия и возможности предоставления различных наборов услуг
- Доработать модели нарушителя и угроз
- Обеспечить граждан возможностью доверенного взаимодействия с ЭП (защищённые пункты доступа и СОДС)

Принципы использования ЭП

- Принцип сохранности ключа подписи (КП)
- Принцип минимального присутствия КП в окружении
- Принцип правильности встраивания
- Принцип локальной реализации алгоритма ЭП
- Принцип однозначной связи ключа подписи и ключа проверки
- Принцип изолированности ключа подписи
- Принцип многоконтурности реализации криптографических модулей
- Принцип связи ключей с условиями их применения
- Принцип связи КП с должностными обязанностями владельца ключа

Обеспечение доверия

- Доверие – фундаментальное понятие безопасности (защищённости)
- Доверие связано с человеком как с субъектом безопасности
- Две составляющие доверия:
  - возможность проверки
  - продолжительный положительный опыт

Возможность проверки ЭП

- В каких условиях хранились криптографические ключи?
- Правильно ли выполнено встраивание СКЗИ в ИС?
- Какому классу соответствует СКЗИ?
- Какой класс СКЗИ использовался для выработки ЭП?
- Является ли человек, подписавший документ, должностным лицом?
- Имеет ли право подписывать документы такого рода должностное лицо, подписавшее документ?
- Верна ли ЭП сообщения?
- Установлено ли авторство сообщения?
- Является ли данное сообщение документом?

Проблемы применения ЭП

- Ответы на вопросы – либо из знания устройства ИС абонента, либо из сертификата открытого ключа
- Можно ли по ЭП определить, в каких условиях она вырабатывалась?
  - нет
- Проблема проприетарности протоколов взаимодействия граждан с ЭП
  - открытые протоколы – цена доступа регулируется рынком
  - проприетарные протоколы – цена доступа устанавливается производителем
  - протоколы должны быть открытыми

Инфраструктура открытых ключей

- Иерархическая (удостоверяющие центры)
  - длинные цепочки сертификатов
  - порождение значительного непроизводительного трафика
  - создание абсурдных ведомственных и территориальных УЦ
  - отсутствие нормальной мотивации к доверию подписи
- Сетевая (сети доверия)
  - шире иерархической, включает её в себя
  - лишена недостатков иерархической

- В разных коммуникациях должны применяться разные механизмы аутентификации с возможностью выбора уместного механизма
  - нотариус и няня

Чего ждать?

- Изменение требований к СКЗИ
- Отказ от программных контейнеров, переход к аппаратным – появление новых, более эффективных СКЗИ
- Изменение структуры сертификата – новые требования к УЦ и ЕПД в целом
- Создание реестра должностных лиц
- Появление альтернативной PKI – PKI для гражданского общества

Спасибо за внимание! Вопросы?

В.А. Конявский
А.В. Чугринов