

**Вопросы юридической значимости
электронных медицинских документов и
защиты медицинских данных**

*Сабанов А.Г.,
ЗАО «Аладдин Р.Д.»*

Москва, 14.06.2012г.

Вопросы к обсуждению

1. Юридическая сила электронного документа
2. Что вносит трансграничность?
3. Каким медицинским электронным документам действительно нужно придавать юридическую силу?

Модель Единого пространства доверия

Создание правового
поля для юридически -
значимого
электронного
документооборота



Технологии обращения с
электронными записями,
документами и сообщениями,
позволяющие обеспечивать
их юридическую силу

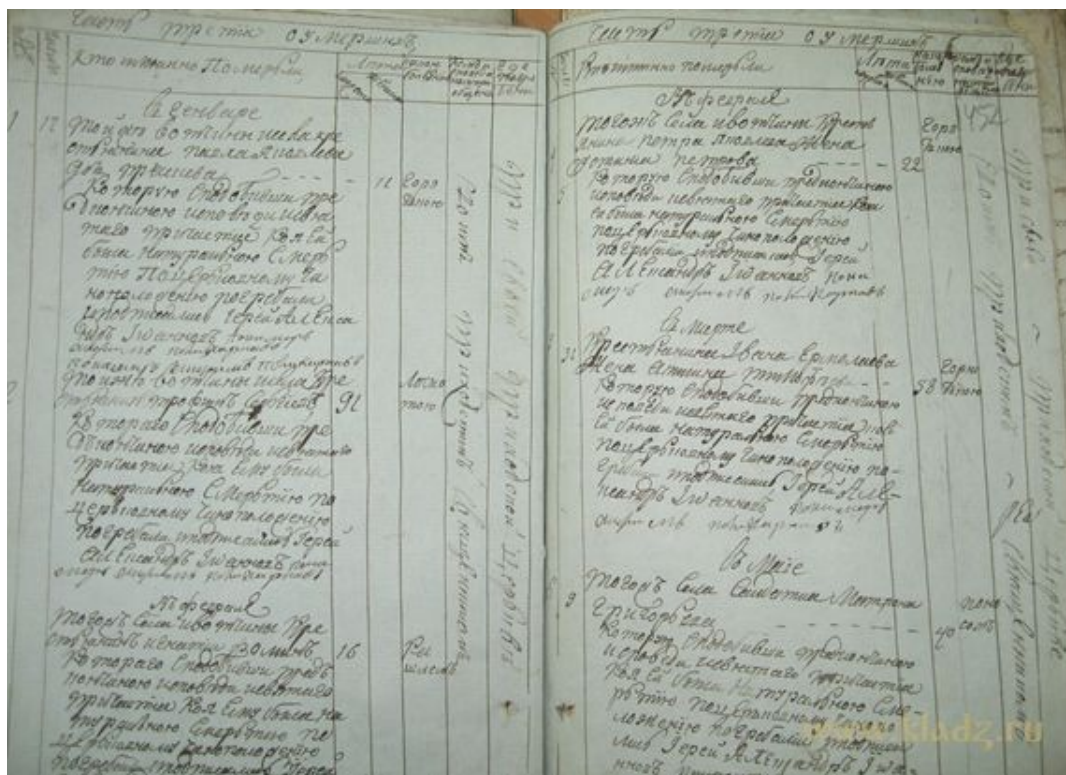
Организация
документирования,
передачи , хранения и
обработки
информации для
участников
информационного
взаимодействия и
операторов

Некоторые нерешенные вопросы

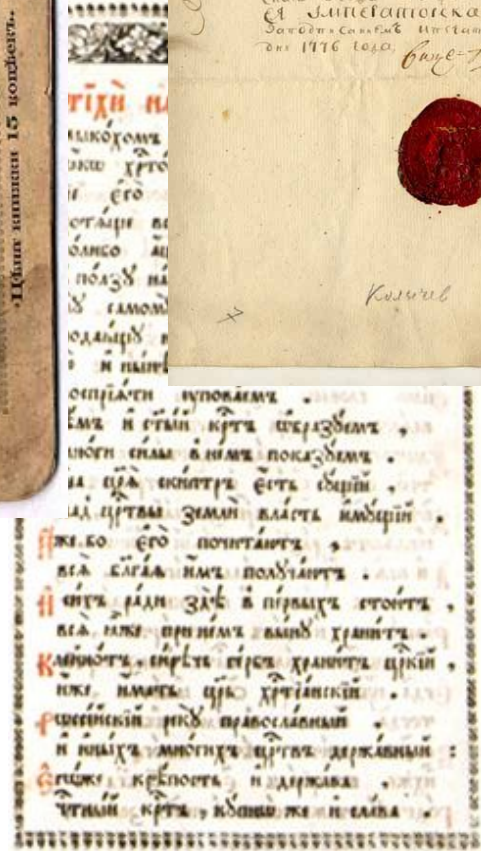
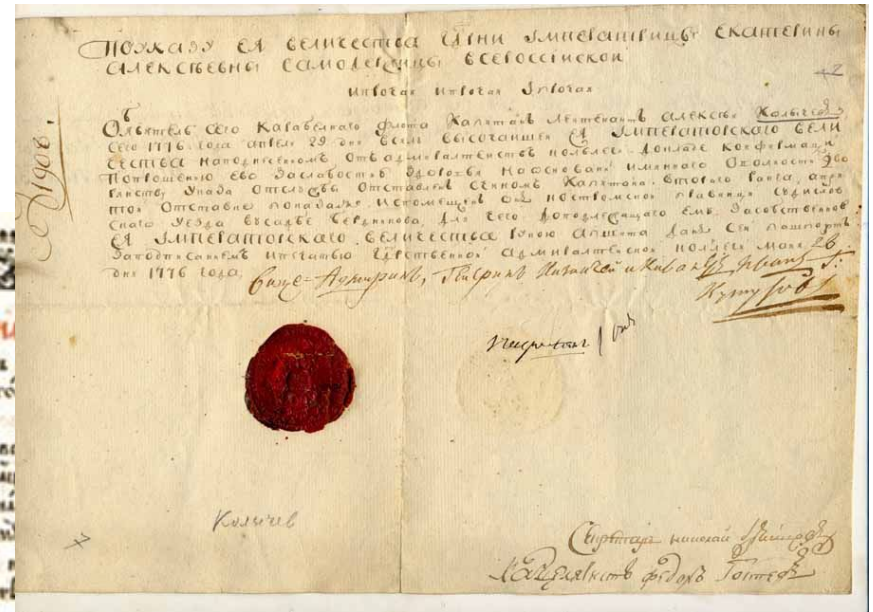
- Архитектура и сроки начала действия единой системы аккредитованных удостоверяющих центров во главе с корневым
- Выбор единого идентификатора гос.служащего, подтверждающего его полномочия (OID или что?);
- Кто и как будет отвечать за правильность построения инфраструктур доверия: полномочий, правомочий, юридически-значимых записей, подписей, времени, идентификационных и др. параметров доверия?
- Кто и когда правильно напишет и быстро утвердит регламенты и правила?
- Какова все же должна быть единая универсальная

Юридические факты

- "Священникам о приходских людях и о духовных детях иметь записные книги, кто, у кого в приходе, когда родился, и кто молитву давал, где который младенец крещен и кем, и кто восприемник и восприемница были, и от которых лет кто у кого исповедывался; аще кто, кем, где и при ком обручен; аще кто умереть, при смерти - онаго кто исповедовали приобщал, и кто тому, аще и отвне, свидетелем был»

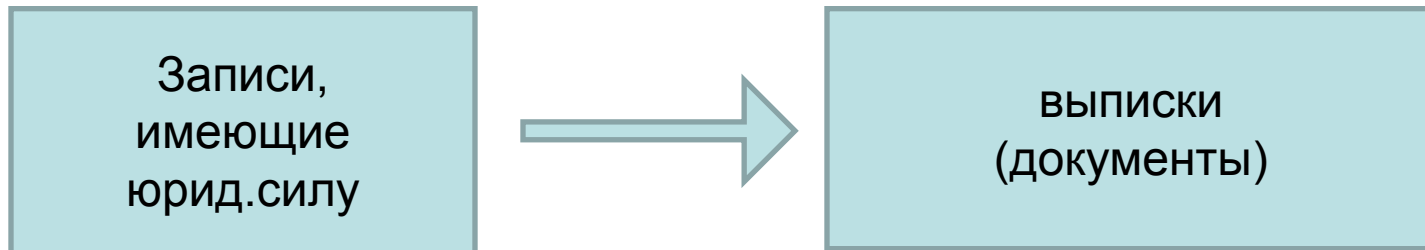


Бумажные документы, фиксирующие юридические факты



Нотариат

- **Нотариат** (от лат. notarius — писец, секретарь), система органов, в функции которых входит удостоверение сделок, оформление наследств. прав, **засвидетельствование документов** для придания им **юридической достоверности** и т.д. В СССР организация и деятельность. (БСЭ)
- **Нотариат** - правовой институт, носители которого - нотариусы -уполномочены государством **совершать и свидетельствовать юридические акты**, придавая тем последним значение актов **публичных**.(Брокгауз, Ефрон)
- **Нотариат** представляет собой систему государственных органов и должностных лиц, на которых возложено **удостоверение** бесспорных прав и фактов, **свидетельствование документов, выписок** из них, придание документам **исполнительной силы** (wikipedia.org)



Компоненты инфраструктуры юридической значимости **бумажного** документооборота

Законодательные и нормативно-правовые акты

Нотариат

Удостоверение беспорных прав

Свидетельствование документов

Придание документам исполнительной силы

Апостиль



Защитные элементы

Текст документа и собственноручная подпись

Защитные элементы печатей и штампов

Защитные элементы бланка документа

Технико-криминалистическая экспертиза документов

Защита печатей для бумажных документов

- Старинные печати

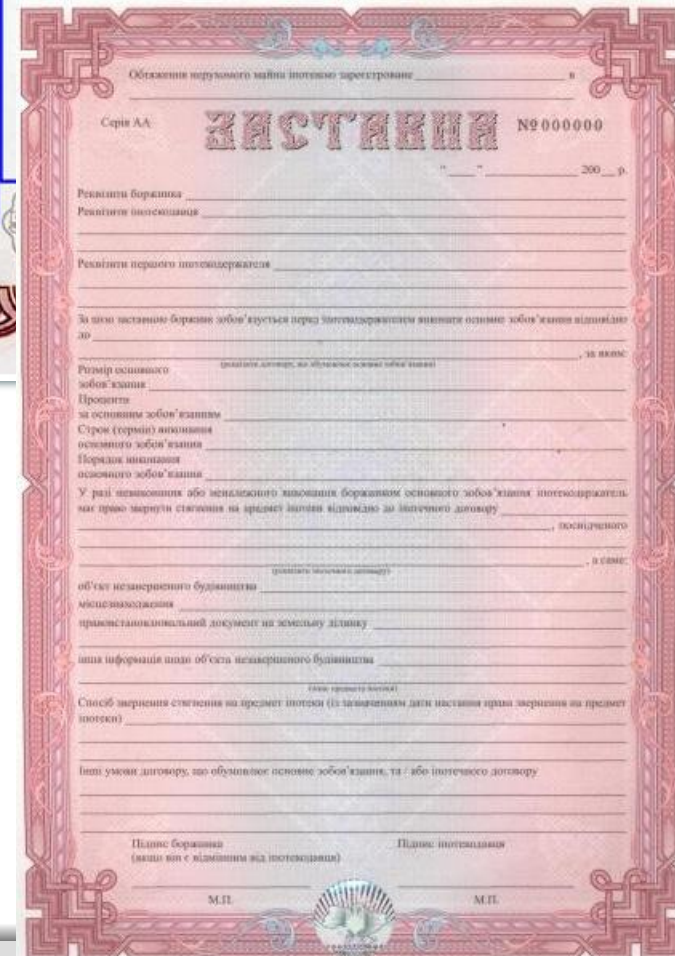


- Современные печати

- 1 ПЕЧАТЬ ИЗГОТАВЛИВАЕТСЯ**
на оборудовании с разрешающей способностью 2032 точки на дюйм
- 2 ТОНКИЕ ЛИНИИ**
толщина линий 0,8 мм
- 3 МИКРОТЕКСТ ЧЕРНЫЙ НА БЕЛОМ**
высота шрифта от 0,5 до 0,8 мм
- 4 МИКРОТЕКСТ БЕЛЫЙ НА ЧЕРНОМ**
высота шрифта от 0,5 до 0,8 мм
в микротексте указан номер сертификата печатеизготовителя, а также месяц и год изготовления.
- 5 РАСТРОВОЕ ПОЛЕ**
линиатура растра не менее 80 линий на сантиметр, т.е. в одном миллиметре длины должно быть не менее восьми точек растра.



Защита бланков бумажных документов



Экспертиза документов в конфликтных ситуациях

- **Задачи технико-криминалистической экспертизы документов**
 - установление способа изготовления документа и его частей;
 - установление факта и способа внесения изменений в документ либо его части;
 - определение рода, вида документа;
 - установления первоначального содержания документа (выявление невидимых и слабовидимых текстов, выцветших, залитых, зачеркнутых, замазанных, вытравленных, подчищенных записей, текстов на сгоревших документах, текстов по вдавленным штрихам и др.);
 - определение возраста документа и последовательности выполнения его реквизитов.
- **Методики решения отдельных задач экспертизы документов**
 - Экспертиза документов с измененным содержанием
 - Установление технических приемов воспроизведения подписи
 - Установление последовательности выполнения реквизитов документа
 - Экспертиза бланков документов
 - Экспертиза денежных билетов и ценных бумаг
 - Экспертиза оттисков печатей и штампов
 - Экспертиза машинописных текстов

Система реквизитов очно-бумажного документооборота

Бланк
документа

The diagram shows a document form with 8 numbered requisites (circles) and their corresponding content:

- 4: Реквизиты ведомства (Department details)
- 5: г. Москва (City: Moscow)
- 16-00 (Time)
- Текст документа (Document text)
- В соответствии с Федеральным законом (In accordance with the Federal Law)
- 3: Директор (Director)
- 1: [Handwritten signature]
- 2: Иванов И.И. (Ivanov I.I.)
- 6: [Red circular stamp]
- 7: [Blue starburst stamp]
- 8: УПЛАЧЕНО пошлина 1 руб. (PAID stamp: stamp duty 1 rub.)

**Постановление
Правительства РФ
№ 477 от 15.06.09г.
«Об утверждении
Правил
делопроизводства
в федеральных
органах
исполнительной
власти»
(24 реквизита)**

Соответствие реквизитов очно-бумажного и электронного документов

Бланк документа

4 Реквизиты ведомства	5 г. Москва	16-00
Правовой статус	Место	Время
Текст документа		
В соответствии с Федеральным законом		
3 Директор	1 	2 Иванов И.И.
Полномочие	Подпись	Правомочие
6  	7 	8 УПЛАЧЕНО пошлина 1 руб.
Нотариальное заверение	Апостиль	Квитанция об оплате

Система реквизитов электронного документа

Бланк
документа

The diagram shows a form for an electronic document with the following fields:

- 4: Правовой статус
- 5: Место
- Время
- Текст документа
- В соответствии с Федеральным законом
- 3: Полномочие
- 1: Подпись
- 2: Правомочие
- 6: Нотариальное заверение
- 7: Апостиль
- 8: Квитанция об оплате

Служба
документирования
(ГОСТ 15489)

Служба
атрибутирования

е-архив

Доверенная третья сторона

ITU-T X.842

Удостоверяющий центр – основа электронного взаимодействия на технологии открытых ключей (PKI)

Система идентификации, авторизации -
управление доступом к отдельным частям ресурса ТТР

Служба доверенного времени – штампы времени (TSP) + GPS/Глонасс

Служба регистрации и ведения идентификаторов объектов – регистрация, публикация и сопровождение дерева идентификаторов объектов

Служба атрибутирования - базируется на рекомендациях RFC 3281. АА обеспечивает привязку внешне изданных сертификатов.

Служба заверения электронных сообщений – служба электронного нотариата (RFC 3029, RFC 2560, RFC 3161).

Служба документирования - Фактофиксирующая система, основанная на рекомендациях ГОСТ Р ИСО 15489-1-2007.

Клиентское программное обеспечение

Организационный уровень

Операторы:

- Регламенты деятельности
- Договора
- Аудит

Участники информационного взаимодействия (клиентский уровень):

- Правила документирования информации в электронном виде
- Безопасные, но удобные условия применения электронной подписи

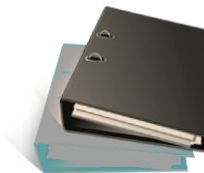
Правовой уровень

- Международные соглашения
- Законодательные и подзаконные акты
- Торговые обычаи
- Страховые механизмы
- Судебные процедуры

Иерархия нормативной базы

Международные документы

Конвенция о защите физических лиц при автоматизированной обработке ПДн
европейская спецификация MoReq (Model Requirements for the Management of Electronic Records),



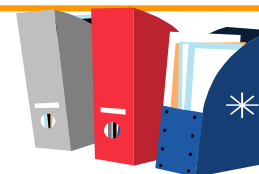
Законы РФ

63-ФЗ, 128-ФЗ, 184-ФЗ, 149-ФЗ, 210-ФЗ, ...



Подзаконные акты

(Госпрограмма «Информационное общество»)
ГОСТ Р 53898-2010 Системы ЭДО,
нормативная база ФСБ, ФСТЭК, РКН)



Отраслевая нормативная база



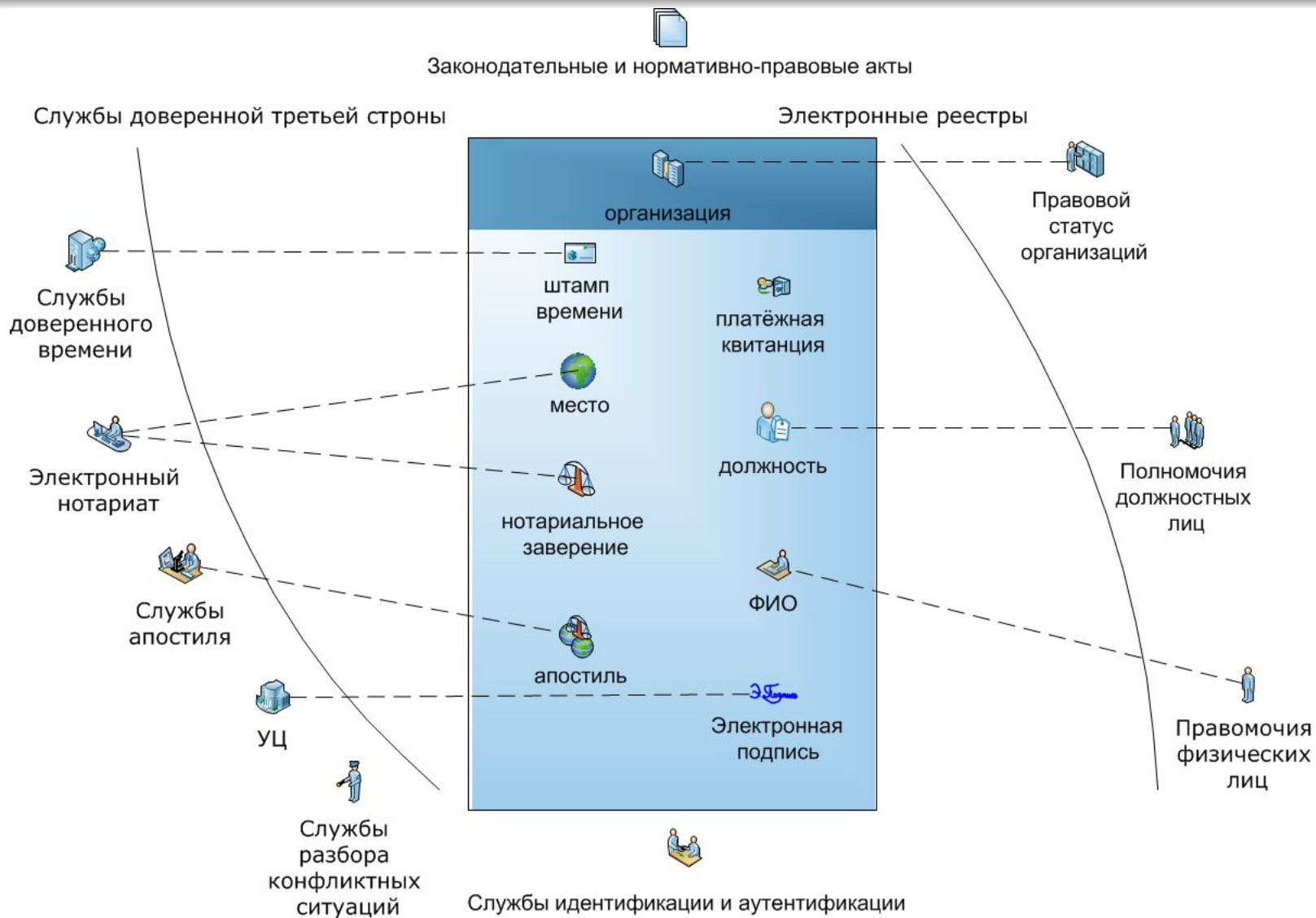
Нормативная база предприятия (приказы,
регламенты, распоряжения)



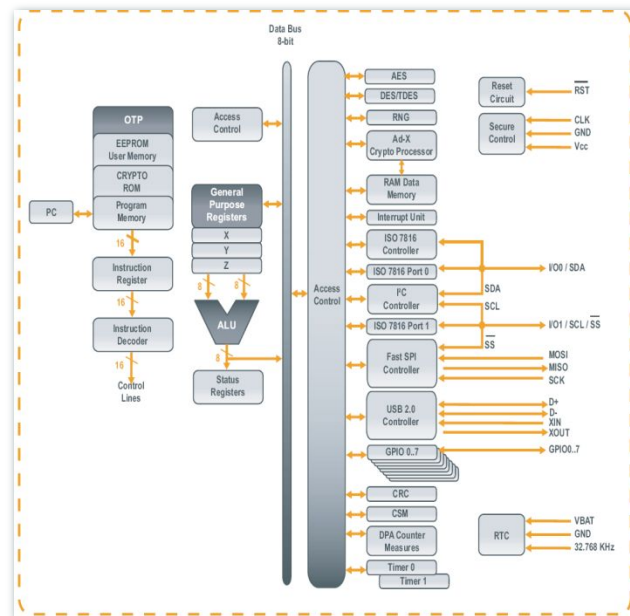
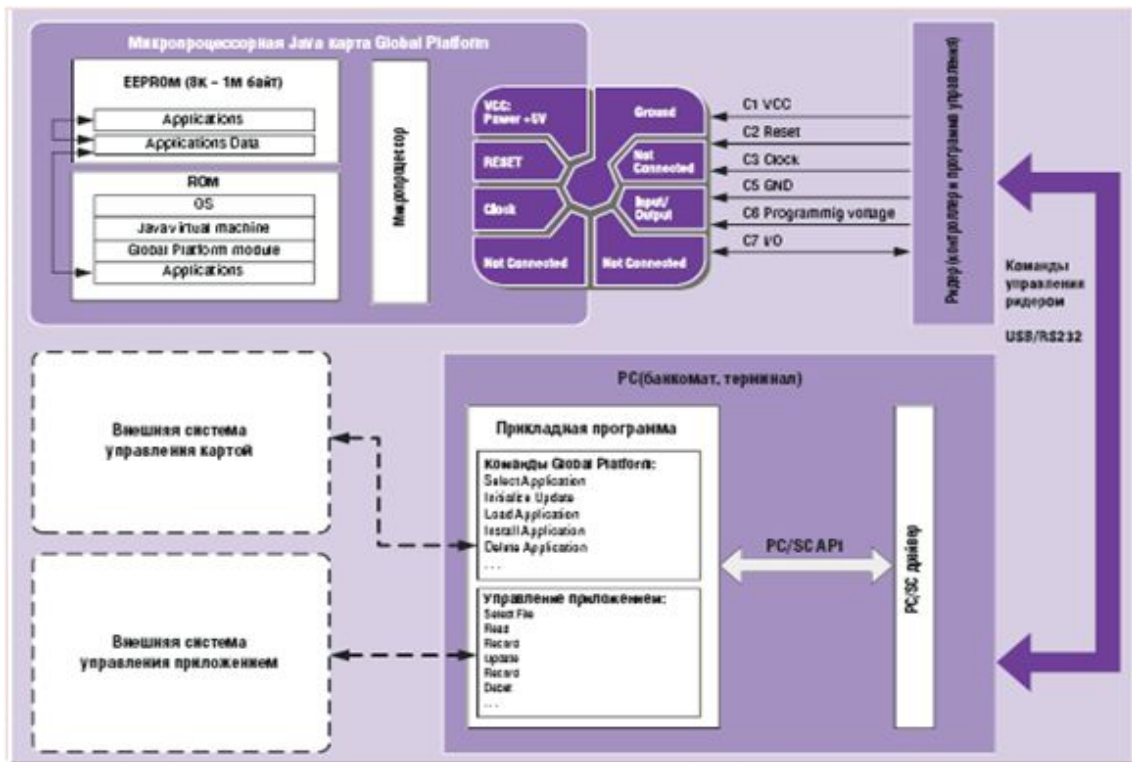
Элементы технологического уровня

- Доверенная третья сторона
- Учетные системы
- Инфраструктура документирования информации
- Инфраструктура мониторинга правовых статусов
- Инфраструктура актуальности правомочий юридических и физических лиц
- Инфраструктура мониторинга полномочий
- Инфраструктура валидации
- Служба определения места события
- Служба доверенного времени

Основные компоненты ЮЗЭДО



Персональное средство электронной идентификации



Назначение – персонально - адресное взаимодействие и запуск приложений для работы с различными устройствами обслуживания

Доверенный процесс – аппаратно программное окружение обеспечивает безопасную загрузку, инсталляцию и запуск любого из востребованных приложений, а виртуальная Java-машина, - безопасное исполнение этих приложений во взаимодействии с различными устройствами обслуживания

Отличительные качества

Решение позволяет объединить весь спектр оказываемых услуг с возможностями безопасного комплексного использования и интеграции.

Исполняемое в различных форм-факторах (USB-ключ, смарт-карта, микро SD или SIM), такое устройство обладает огромным инновационным потенциалом. Ее отличительная особенность - мультиаппликативность.

Архитектура используемой аппаратно программной среды обеспечивает простое и **надежное исполнение различных механизмов безопасности:**

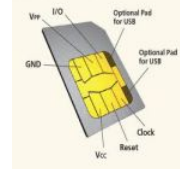
- многофакторная аутентификация клиента на основе криптографии с открытым ключом и цифровых сертификатов;
- электронная подпись в соответствии с ГОСТ Р 34.10-2001;
- хранение ключей пользователя в неизвлекаемом виде;
- возможность установления защищенного логического соединения с сохранением сессии и шифрованием информации.

Является средством криптографической защиты информации (СКЗИ), сертифицированным ФСБ России

Эксплуатационные качества

С точки зрения пользователя:

- работает крайне просто
- и одинаково во всех приложениях



С точки зрения оператора - надежное исполнение всех операций, а именно:

- распознавание субъекта (идентификация);
- проверки подлинности субъекта (аутентификация);
- адресный контроль (мониторинг), включая протоколирование всех действий субъектов при их доступе к ресурсам информационной системы (аудит);
- предоставления субъекту определенных прав (авторизация);
- адресное управление доступом субъектов к ресурсам системы (администрирование).



Защищенное рабочее место пользователя



- Является ключевым элементом концепции доверенного электронного взаимодействия. Его основу должен составлять интегрированный модуль безопасности (embedded Trusted Security Module).
- С его помощью осуществляется контроль доступа и целостности ресурсов вычислительной платформы.
- Загрузка операционной системы и доступ к ресурсам компьютера выполняется только после осуществления процедур аутентификации.

TSM - работа на этапе загрузки



- взаимодействует с идентифицирующими устройствами
- располагается в SPI Flash на материнской плате компьютера
- вызывается на исполнение BIOS после прохождения процедуры Power On Self-Test (POST).

Функциональные качества

- TSM невозможно обойти при любых режимах загрузки компьютера, в том числе и при загрузке с отчуждаемых носителей
- его невозможно извлечь без нарушения физической целостности материнской платы,
- вне заводских условий извлечь TSM из компьютера невозможно
- в режиме «Пользователь» ПО модуля исчезает из адресного пространства и не может быть атаковано



Эксплуатационные преимущества

- нет необходимости в осуществлении организационных мероприятий по контролю его физической целостности
- без средства аутентификации пользователя компьютер просто не работает

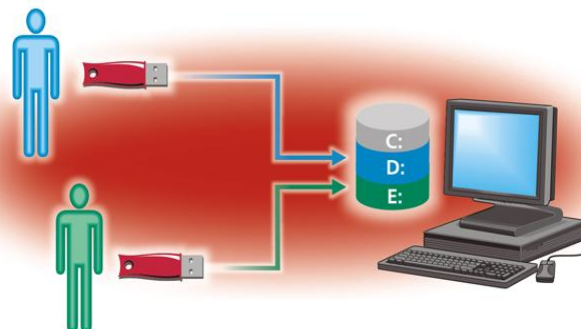
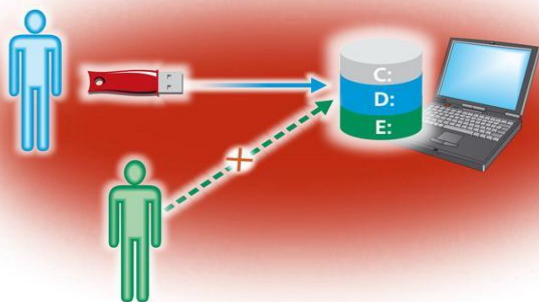


Аутентификация при доступе к зашифрованным данным

- **Персональная система шифрования** данных на дисках (Secret Disk)
- **Шифрование данных на серверах** (Secret Disk Server)
 - Управление доступом
 - Для файл-серверов и серверов приложений
- **Защита конфиденциальной информации и персональных данных:**
 - защита системного раздела;
 - защита пользовательской информации от несанкционированного доступа;
 - соответствие закону по защите персональных данных (152-ФЗ)
 - прозрачная работа для пользователя

Как это работает

- Для доступа к защищённым дискам каждый пользователь использует свое идентифицирующее устройство
- С его помощью пользователь может создавать так называемые защищённые (секретные) диски с зашифрованным содержимым
- Поддерживается три типа защищённых дисков: разделы жёсткого диска, съёмные диски (USB-диск, ZIP и др.) и виртуальные диски.
- Виртуальные диски представляют собой логическое устройство, воспринимаемое операционной системой как обычный диск. Всё содержимое виртуального диска хранится в файле на одном из доступных дисков (раздел жёсткого диска или съёмный диск).



Главная задача – администрирование

- Главная задача – **создание надежного связующего элемента (звена) между пользователями, их средствами идентификации и многочисленными приложениями**
- Постановлением Правительства РФ от 28 ноября 2011 г. № 977 предполагается создать федеральную государственную информационную систему «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА). Ввод в эксплуатацию указанной системы запланирован в апреле 2012 г. Построение такой системы в масштабах государства - архи сложная задача.
- Организация правильной работы в масштабах страны и в масштабах отрасли (здравоохранение) – весьма серьезная технологическая задача.
- **Нерешенный вопрос:** взаимодействие доверительных сервисов, транслирование доверия, надежное разделение доступа, аутентификация

Что надо заверять подписью

История болезни в электронном виде – общая задача

- Эпикриз (врачебной комиссии, выписной, посмертный)
- Результаты обследования
- Анализы
- Назначения
- Операции
- Ежедневные дневники (после тяжелой операции, 1 раз в 10 дней- этапный?, 1 раз в 15 дней – ВК (лечащий врач, зав.отделением, зам.гл.врача по экспертизе))
- ...

Назначения

- Лист назначений подписывает лечащий врач и мед. сестра, исполняющая назначения
- Если более 5 препаратов или наркотические препараты – подписывает лечащий врач, мед.сестра и заведующий отделением

Спасибо за внимание!

a.sabanov@aladdin-rd.ru