Аладдин РД

Технологии аутентификации: от LAN до Public Cloud

Алексей Сабанов,
Заместитель генерального директора ЗАО «Аладдин Р.Д.»

13 февраля 2013г.

Введение

- Согласно Федеральному закону №149-ФЗ обладатель информации, если иное не предусмотрено федеральными законами, вправе «разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа» (статья 6, пункт 2).
- Аутентификация является основным инструментом управления доступом пользователей (А.А.Грушо)
- Строгость идентификации и аутентификации пользователей должна соответствовать важности информации, к которой будет предоставляться доступ (ISO 27002:2005, раздел 11.5.2)

Терминология. Удаленная аутентификация

- **Идентификатор** – уникальная открытая (общеизвестная) метка, присвоенная субъекту для того, чтобы отличить его от других.
- **Процесс идентификации** – сравнение предъявленного субъектом идентификатора с эталонным, занесенным в базу при присвоении уникальной метки данному субъекту
- **Процесс аутентификации** – подтверждение ***подлинности*** идентификатора субъекта. Производится с помощью подтверждения владения секретом, изданным и выданным субъекту в процессе регистрации после тщательной проверки идентификаторов субъекта (после полной идентификации).

Идентификация и аутентификация

- Идентификация – процедура распознавания субъекта по его идентификатору. В процессе регистрации субъект предъявляет свой идентификатор информационной системе, которая проверяет его наличие в своей базе данных (LDAP-каталоге). Простейшим примером идентификатора является учетная запись, содержащая логин пользователя.
- Аутентификация – процедура проверки подлинности субъекта, проводимая, как правило, с помощью криптографических преобразований, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует.

Лучшая технология аутентификации – ЭЦП.

Идентификация и аутентификация

с точки зрения применяемых технологий

Аутентификаторы

Учетная запись пользователя	Секрет (аутентификатор)
Логин	Пароль
Логин	Одноразовый пароль (технология OTP)
Заданные поля сертификата X.509, сформированного удостоверяющим центром для доступа пользователя	Закрытый ключ (в терминах №1-ФЗ)

Угрозы

- Регистрация
  - «маскарад» – имитация конкретного пользователя
  - Отрицание регистрации
- Токены (аутентификаторы)
  - Программные и физические ключевые носители может быть украдены или дублированы
  - Известное (PIN) может быть раскрыто злоумышленником
  - Обладаемое (отпечаток пальца) может быть скопировано
- Протоколы аутентификации
  - Подслушивание
  - Имитация (заявителя, проверяющей стороны, доверяющей стороны
  - Перехват сеанса аутентифицированного пользователя (обращение от имени пользователя к доверяющей стороне с целью получения конфиденциальной информации или ввода ложной информации)
  - Обращение от имени доверяющей стороны к проверяющей стороне с целью получения конфиденциальной информации или ввода ложной информации

Прочие угрозы

- Случайные и/или намеренные ошибки при издании Credentials, связывании, делегировании прав, создании учетных записей
- Злонамеренное ПО, направленное на компрометацию токенов (аутентификаторов)
- Вторжение в системы пользователей, CSP или проверяющих сторон с целью получения цифровых удостоверений или токенов
- Угрозы компрометации токенов со стороны инсайдеров
- Социальный инжиниринг с целью раскрытия пользователем PINa, подглядывание
- Атаки, при которых обманутый заявитель использует небезопасный протокол, думая, что использует безопасный, либо сам преодолевает средства защиты (например, принимая сертификаты серверов, не прошедших проверку)
- Явный отказ пользователей, сознательно скомпрометировавших свои токены

Атаки на протоколы аутентификации

- Пассивное прослушивание
- Активные атаки
  - Угадывание пароля или PIN-кода
  - Воспроизведение
- Внесение изменений в канал аутентификации
  - перехват сеанса аутентифицированного пользователя
  - Имитация проверяющей стороны
  - «Человек посередине»

Основные процессы

1. Регистрация
2. Собственно аутентификация с помощью протоколов аутентификации
3. Валидация и управление цифровыми удостоверениями (Credentials)
4. Управление аутентификаторами (смарт-карты, USB-ключи)
5. Аудит

Основные процессы аутентификации

	процесс	критичность операции	сервер(С) или клиент(К)
1.	**Регистрация**		
1.1.	субъект ***предъявляет*** свои идентификаторы (удостоверения или ЭУ)	ошибки ввода данных	К
1.2.	ЦР ***проверяет*** предъявленные субъектом идентификаторы	ошибки проверки идент.	С
1.3.	ЦР ***создает*** учетную запись субъекта	ошибки ввода данных	С
1.4.	ЦР ***регистрирует/создает*** секрет (аутентификатор) и ***издает*** ЭУ	вероятность мала	С
1.5.	ЦР ***делегирует*** права доступа субъекта к другим ИС	вероятность мала	С
1.6.	ЦР ***выдает*** секрет и ЭУ на руки субъекту	вероятность мала	
2.	**Подтверждение подлинности**		
2.1.	Субъект ***хранит*** секрет и ЭУ	критичная операция	К
2.2.	Субъект ***предъявляет*** секрет и ЭУ доверяющей стороне (ДС)	вероятность мала	К
3.	**Валидация**		
3.1.	ДС ***проверяет*** цепочку сертификатов, срок и область действия ЭУ	вероятность мала	С
4.	**Принятие решения**		
4.1.	ДС ***принимает решение*** о результате аутентификации	вероятность мала	С

1. Регистрация (центр регистрации или УЦ)

1. Проверка идентификационных атрибутов личности
   1. В США предъявляют не менее 2 валидных документа
2. Создание учетной записи в БД
3. Выпуск аутентификационных атрибутов (Credentials и токен)
4. Связывание
5. Делегирование прав
6. Определение политик доступа
7. Выдача токена (смарт-карта, USB-ключ) и Credentials (закрытые ключи и сертификаты X.509, ключи шифрования, VPN,…)

О способах хранения секрета

- изданный ЦР на этапе 4 секрет субъект может хранить по-разному. Ст.10 Федерального закона 63-ФЗ: «ответственность за хранение ключа подписи лежит на его владельце». При массовом использовании ЭП к описанным процедурам будут привлечены разные слои населения, в т.ч., далекие от ИТ и ИБ. С другой стороны, действительно важные ресурсы и самый серьезный подход к изданию ключей подписи. В стандарте FIPS, а также стандартах и рекомендациях ЕС существует требование использования для формирования ключевой пары квалифицированной подписи только SSCD-устройств.
- В действующих на сегодня практике в регламентах УЦ зачастую отсутствует элементарное требование активации флага «неизвлекаемость закрытого ключа».
- В зависимости от способа хранения секрета (аутентификатора) появляется разделение на факторы, называемые *факторами аутентификации.*

Способы хранения секрета, уровни 1-2

Пароль можно:

- Запомнить
- Записать на бумагу
- Записать на электронный носитель

OTP можно:

- Хранить в бумажном блокноте (как это делал Штирлиц в 17-ти мгновениях весны)
- Записать на скретч-карту (как это делают до сих пор многие банки
- Сгенерировать по согласованному с сервером алгоритму с последующей процедурой синхронизации (пример – OTP-токен Аладдина, Васко…)

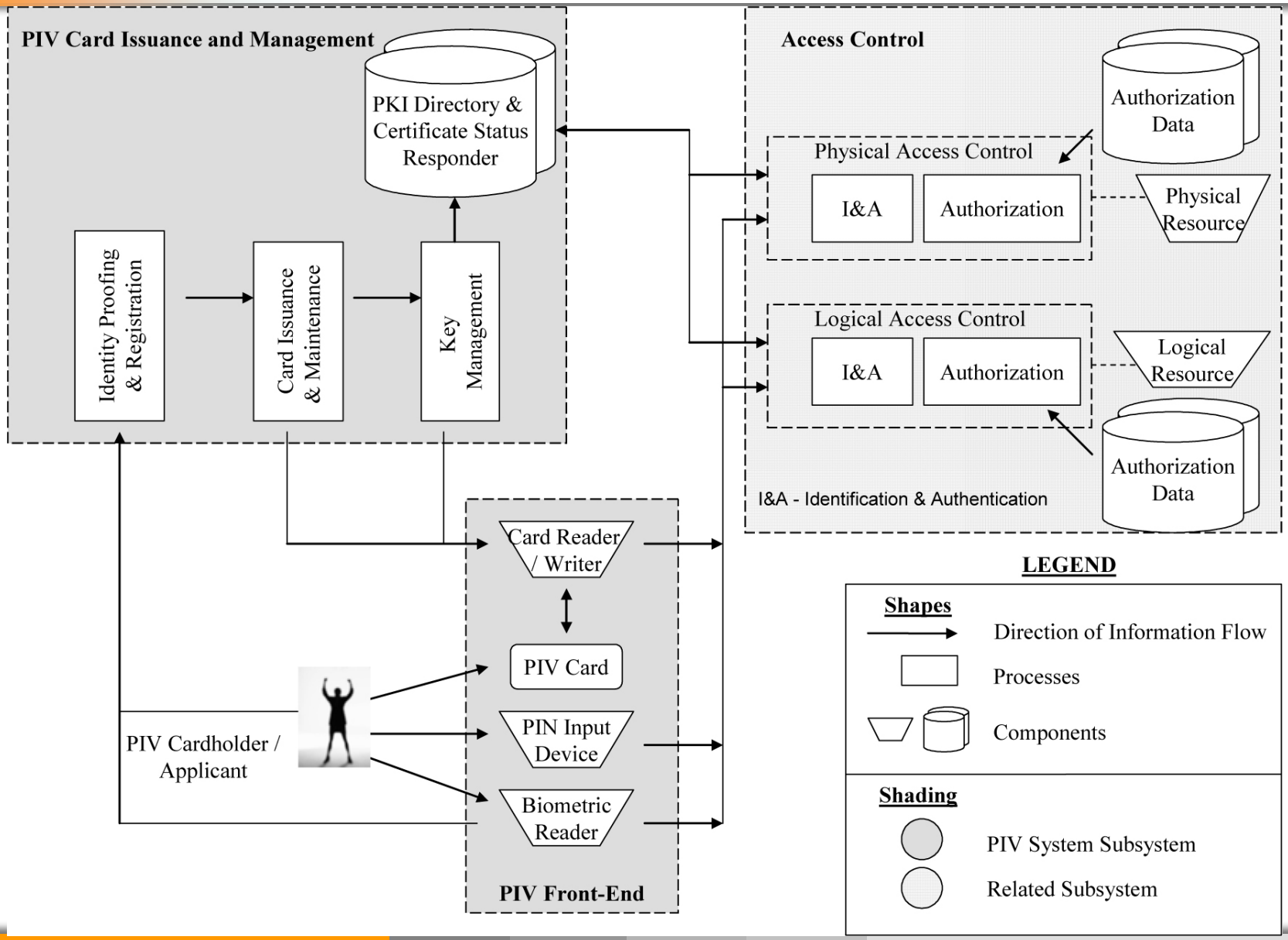
Способы хранения закрытого ключа

- Запись и последующее хранение в реестре компьютера
- запись на дискету
- запись на электронный носитель (USB-ключ, смарт-карту), например, в EEPROM, в лучшем случае – с взведенным флагом «Неизвлекаемость контейнера из носителя» при любых манипуляциях (введение PIN-кода юзера, PIN-кода администратора,….)
- генерация и гарантируемая неизвлекаемость в SSCD-устройстве.

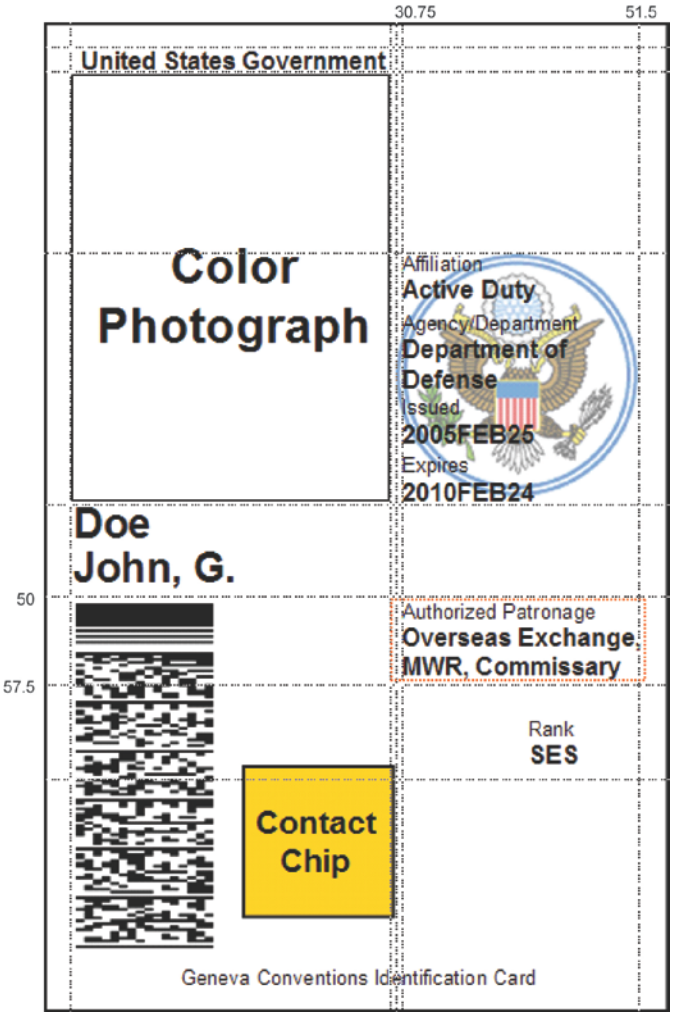
Пример Credentials из FIPS PUB 201-1

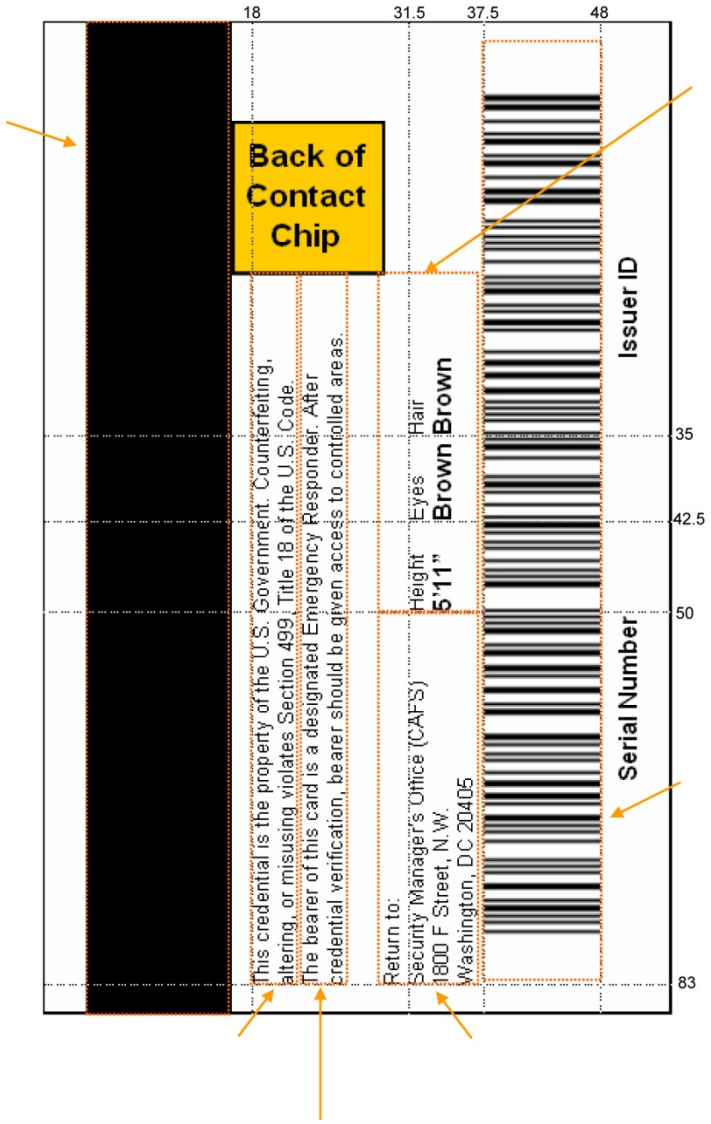
- Ключевая пара (открытый и закрытый ключи) и цифровой сертификат **аутентификации**
- Ключевая пара (открытый и закрытый ключи) и цифр. сертификат **электронной подписи**
- Ключевая пара (открытый и закрытый ключи) и цифровой сертификат для **управления ключами**
- Асимметричные или симметричные ключи **аутентификации смарт-карты** для СКУД
- Ключи для **системы управления жизненным циклом** смарт-карт

Схема организации PIV федер. служб США

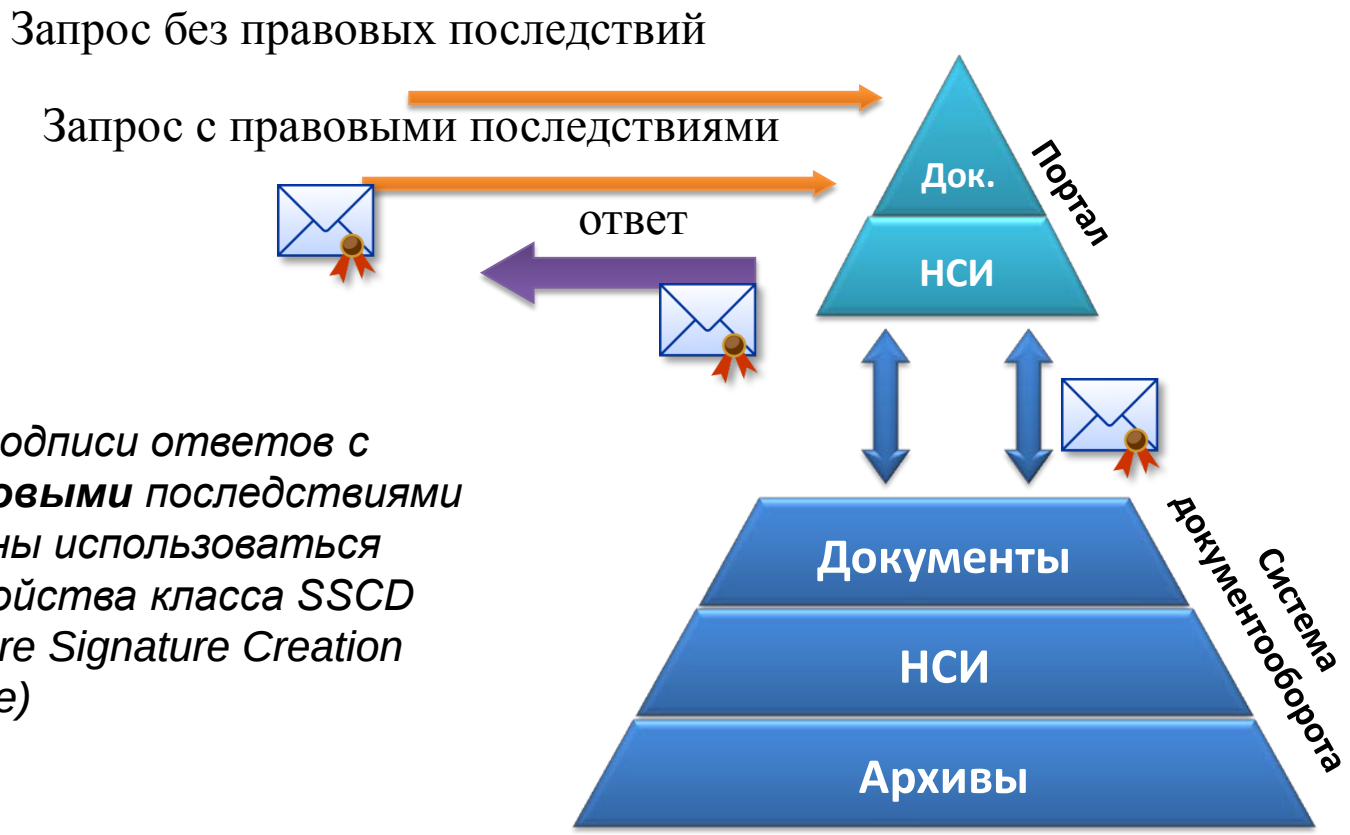


FIPS PUB 201-1: стандарт смарт-карты





Условная схема оказания госуслуг



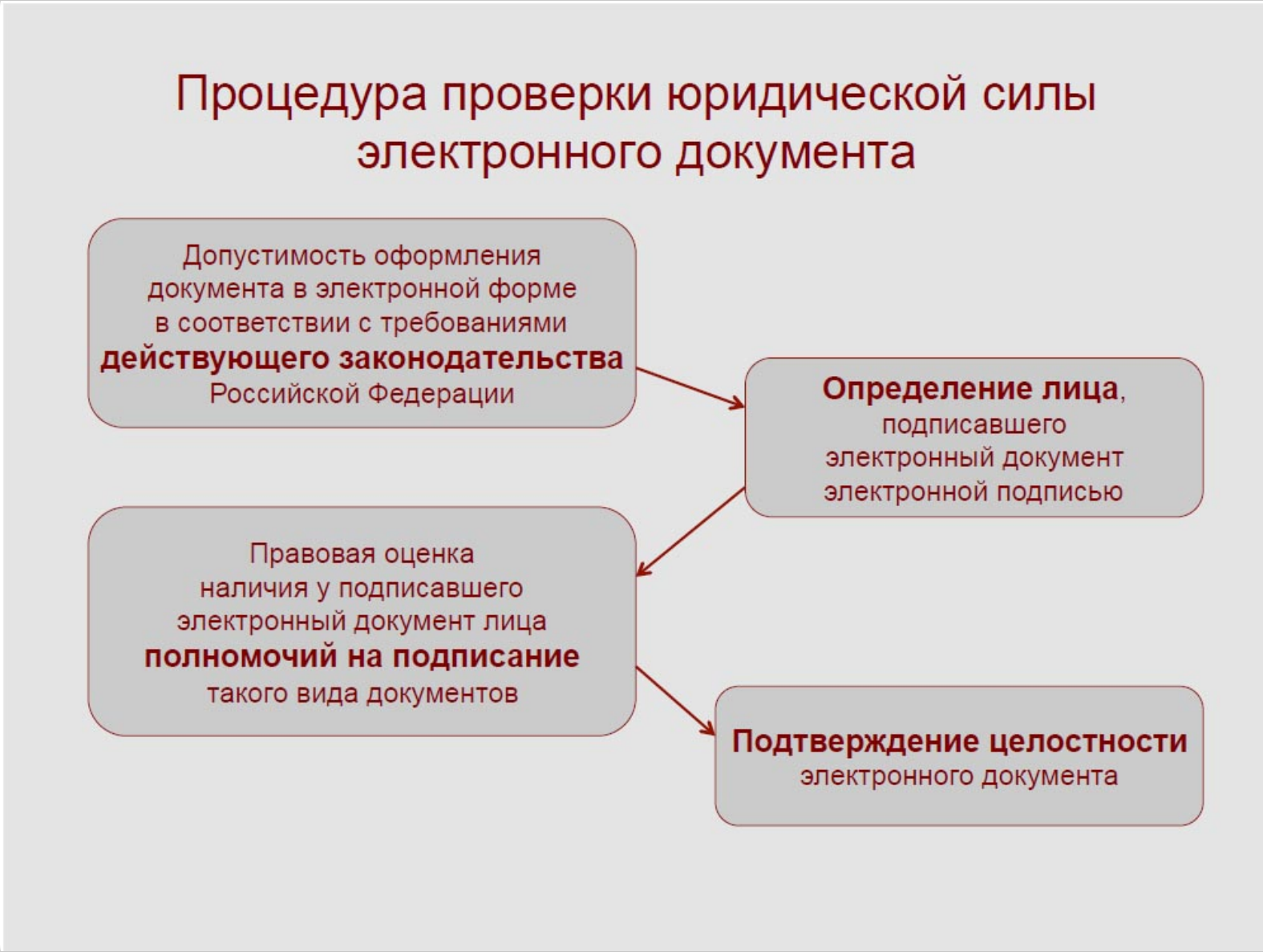
*Для подписи ответов с **правовыми** последствиями должны использоваться устройства класса SSCD (Secure Signature Creation Device)*

Юридическая значимость

Бланк и оформление документа

Постановление Правительства от 15.06.2009 №477 для бумажных документов в ФОИВ

Взгляд юриста: минимальный набор реквизитов



Юридическая сила эл.документа

- Инфраструктура и доверенные средства генерации, применения и проверки усиленной квалифицированной подписи (УКП);
- Развитая системы проставления меток доверенного времени, синхронизированного в каждом аккредитованном удостоверяющем центре с временем корневого УЦ;
- Поддерживаемая в актуальном состоянии с заданным интервалом времени (в часах) система реестров полномочий и правомочий владельцев УКП;
- Доверенные сервисы идентификации и аутентификации, строго регламентированные для каждого аккредитованного УЦ с регулярным внешним контролем порядка и правил выполнения основных процедур.

Технические проблемы хранилища

Проблемы архивного хранения электронных документов, обладающих юридической силой

- Устаревает сертификат X.509 (обычно 1 год);
- Заканчивается срок действия электронной подписи (1год 3 месяца, сейчас – максимум 3 года)
- Меняются криптографические алгоритмы (обычно 5-10 лет, ГОСТ 34.10.2002 – до дек.2012)
- Меняется формат представления электронных документов (Lexicon – Word, PDF,…)

Проблема истечения срока действия ЭП

- Решение задачи «в лоб»: RFC3029. При попадании электронного документа (ЭД) в архив выпускается квитанция (несколько Кб: док.база, статус проверки, время) о проверке подписи
- При попадании ЭД в архив электронная подпись снимается. Этот факт фиксируется, хранятся хеши документов. Гарантии. Доверенное хранилище.
- Применение специального вида подписи advanced (подпись с квитанцией): при попадании ЭД в архив вырабатывается TimeStamp + подпись уполномоченного лица

Что дают атрибутные сертификаты

- Разграничение ролевого доступа к документу. Пример (Юнизета): хранилище данных юр.лица. На предъявленный сертификат выпускается атрибутный сертификат доступа к документам архива на конкретный срок.
- Изготовление выписок из документа. Обеспечивается криптографическая связь с данными документа (обеспечение целостности), срок действия, возможность отзыва,….

Нормативная база РФ, касающаяся темы ЕПД

- ФЗ от 10.01.2002г. № 1-ФЗ «Об ЭЦП» + №108-ФЗ
- ФЗ от 6.04. 2011г. № 63-ФЗ «Об электронной подписи»
- ФЗ от 27.07.2011г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»
- ПП РФ от 28.11.2011 г. N977 о создании ЕСИА
- ПП РФ от 09.02.2012г. N111 об ЭП для ФОИВ и МОИВ
- ПП РФ от 25.06.2012г. N634 об ЭП для получ. гос. услуг
- ПП РФ от 25.08.2012г. N852 об утв. правил исп. квалиф.ЭП
- Решение Правительства от 12.07.2011г. О видах ЭП для ФОИВ
- Приказ ФСБ №795 и 796 от 27.12.2011г.
- Приказы Минкомсвязи №250 от 05.12.2011, №107 и №108 от 13.04.2012
- Приказ ФНС от 17.12.2008г. №ММ-3-6/665
- ГОСТ Р ИСО/МЭК 15408, Р54582-2011, Р52447-2005, 9001-2008

Что такое Единое пространство доверия

- Приказ ФНС РФ от 17.12.2008 ММ-3-6/665: «Единое пространство доверия – структура, определяющая организационные границы, в пределах которых находятся только заслуживающие доверия удостоверяющие центры, а сертификаты ключей подписей, изготовленные ими, признаются всеми участниками информационного взаимодействия в границах структуры и на равных условиях».
- ГОСТ Р ИСО/МЭК 15408: «Доверие – основа для уверенности в том, что продукт или система ИТ отвечают целям безопасности».

ЕПД: техническая компонента

Единое пространство доверия - совокупность взаимосвязанных доверенных сервисов, развернутых на базе инфраструктуры открытых ключей

Доверенные сервисы

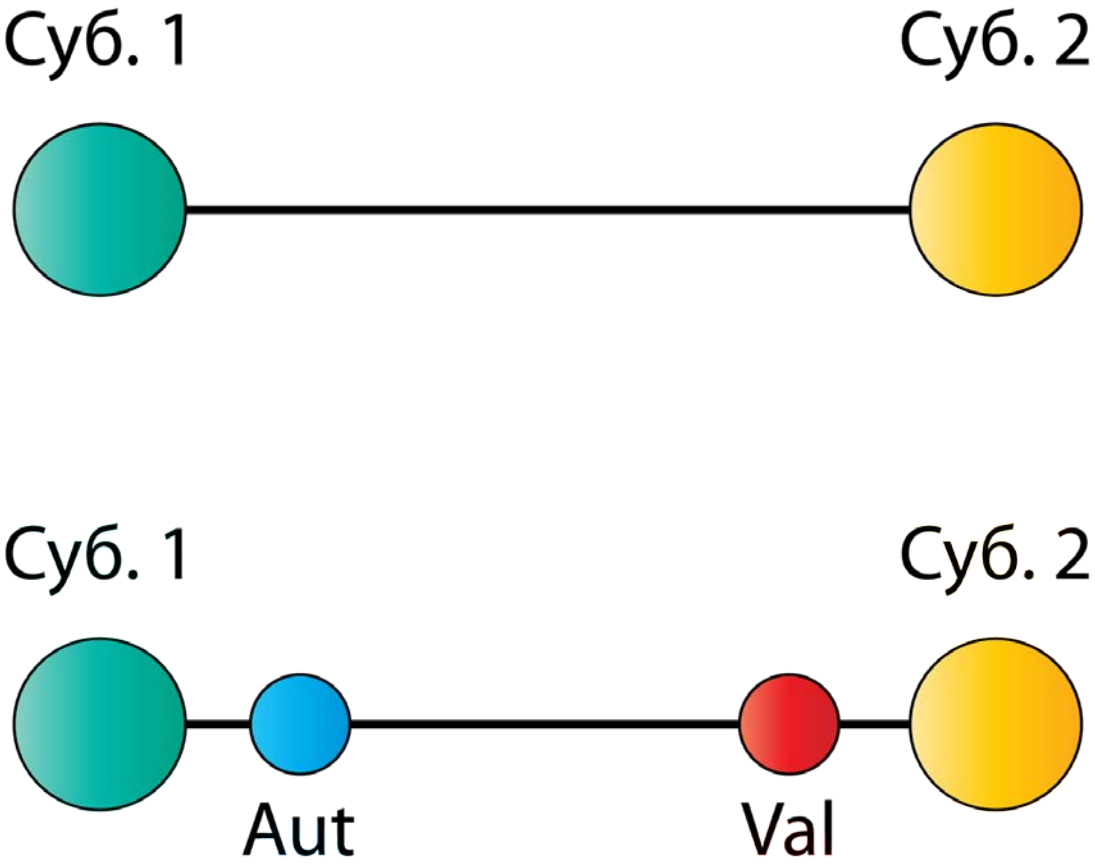
*Под **доверенными сервисами** будем понимать электронные сервисы, участвующие в создании, валидации, обработке, хранении электронных **подписей**, электронных **печатей,** меток **доверенного времени,** электронных **документов,** средств **доставки** и **заверения** электронных сообщений, разграничения и **управления доступом, аутентификации,** в том числе на на Web-сайтах, электронных **сертификатов** (в том числе атрибутных), актуальных **реестров** (ролей участников электронного взаимодействия, уполномоченных лиц и др.), сервисы **регистрации, документирования** и т.д.*

Нормативная база по аутентификации

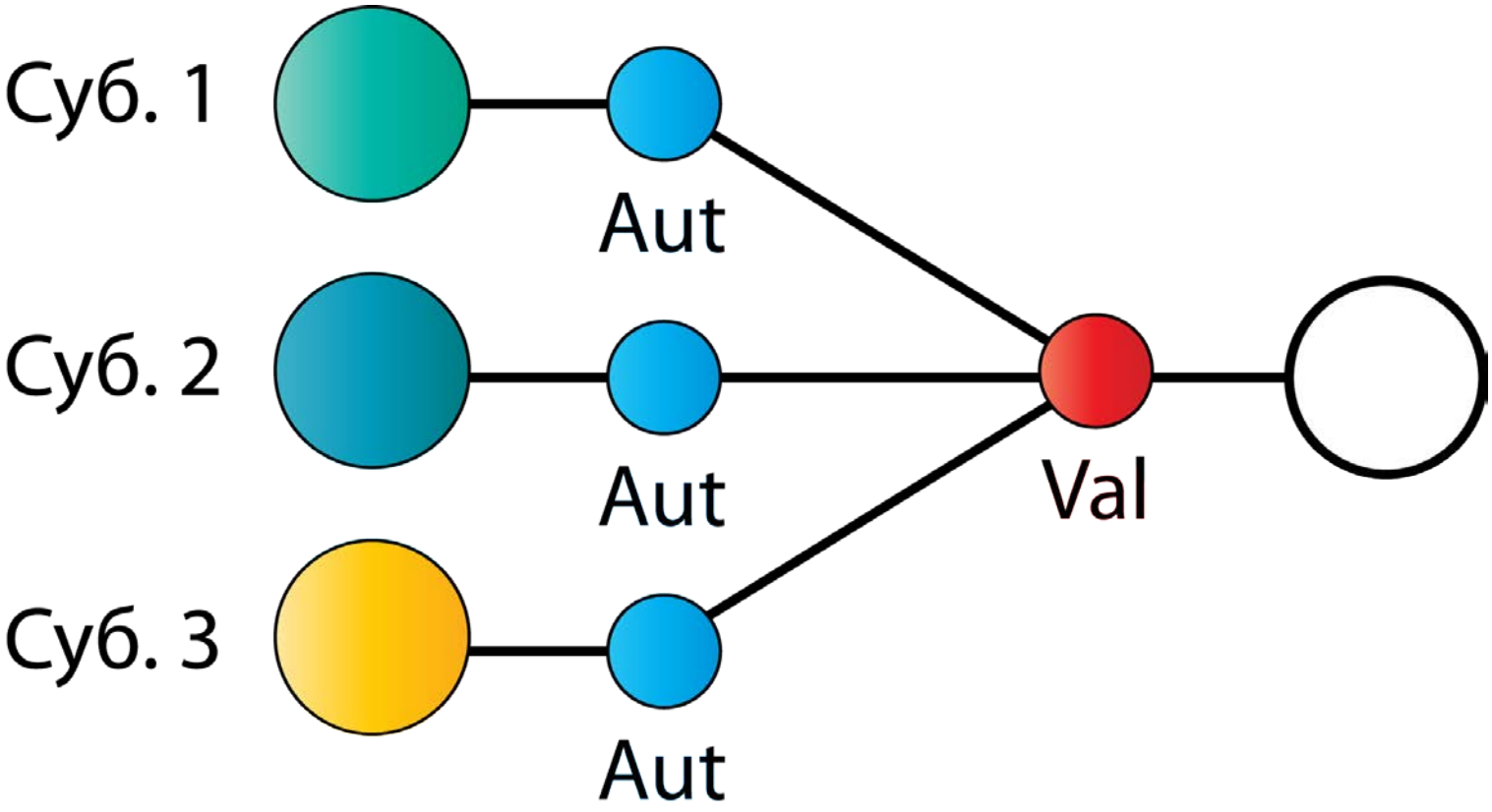
- Declaration on Authentication for Electronic Commerce 7-9 October 1998
- CWA 14365 Guide of use of Electronic Signature. Jan.2003
- OMB Memorandum M-04-04 E-Authentication Guidance for Federal Agencies December 16, 2003 & OMB Circular A-130 2003
- Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors. August 27, 2004
- ISO/IEC 10181-2, ITU-T Rec/x.811 Теоретические основы аутентификации. 2004
- NIST Special Publication 800-63 April 2006 (РД по использованию е-аутентификации)
- OECD Recommendation on Electronic Authentication/2007
- FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2006, FIPS PUB 201-2. March 2011
- ETSI draft SR 000 000 v0.0.2 Rationalized Framework for Electronic Signature Standardization August 2011 & ETSI TS 1, 103173,…
- European Commission. Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. Brussels, XXX COM (2012) 238/2.

Аутентификация – основа создания доверительных отношений при удаленном взаимодействии

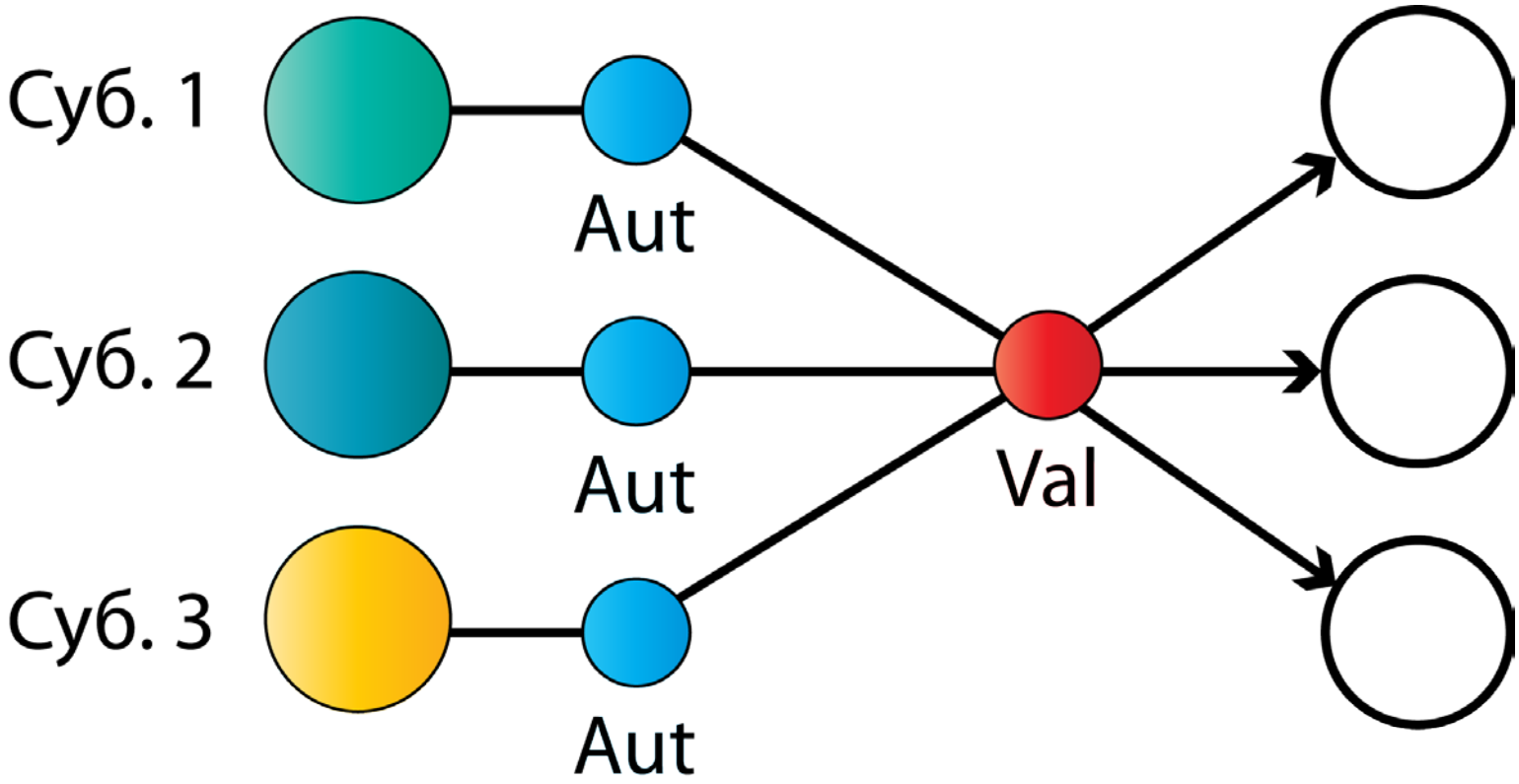
Отношения доверия



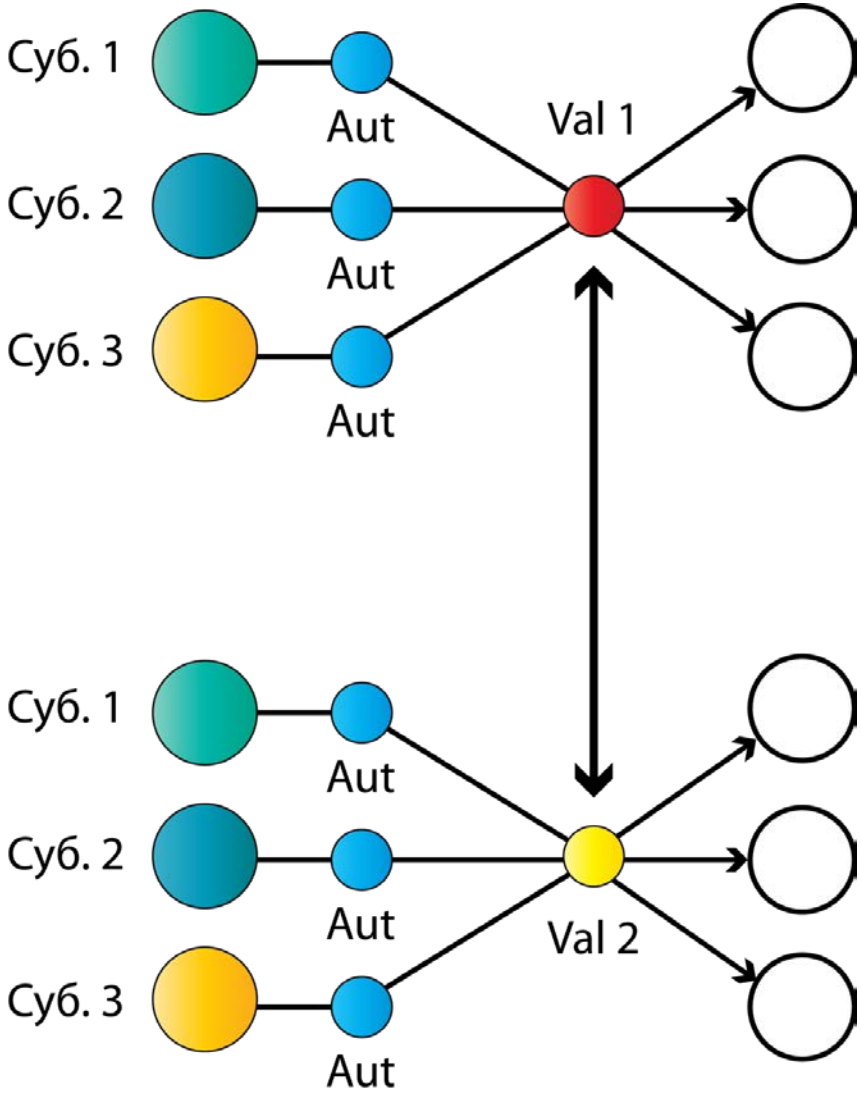
Система доверия



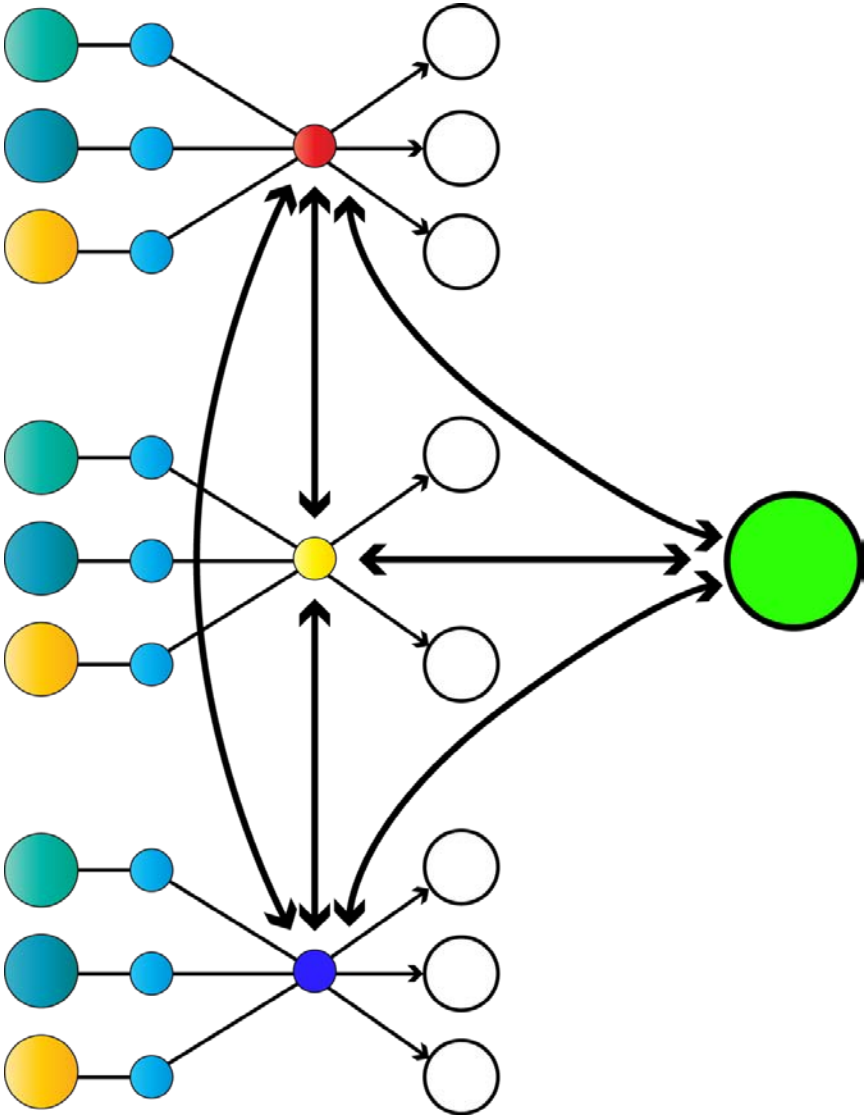
Домен доверия



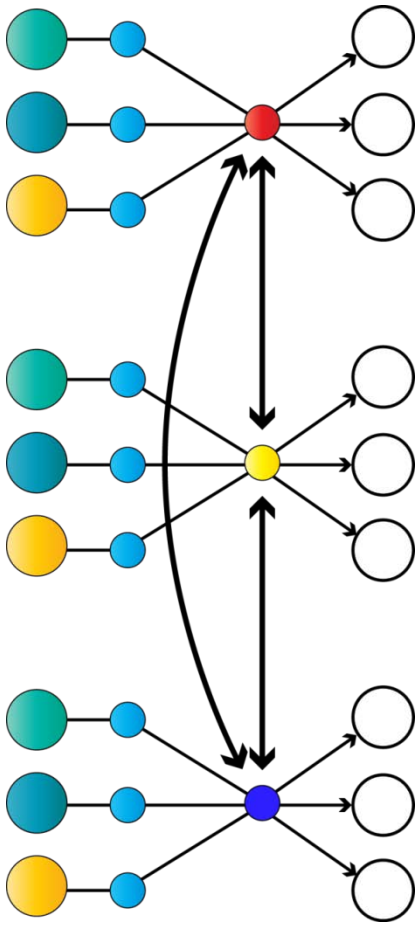
Пространство доверия AAA



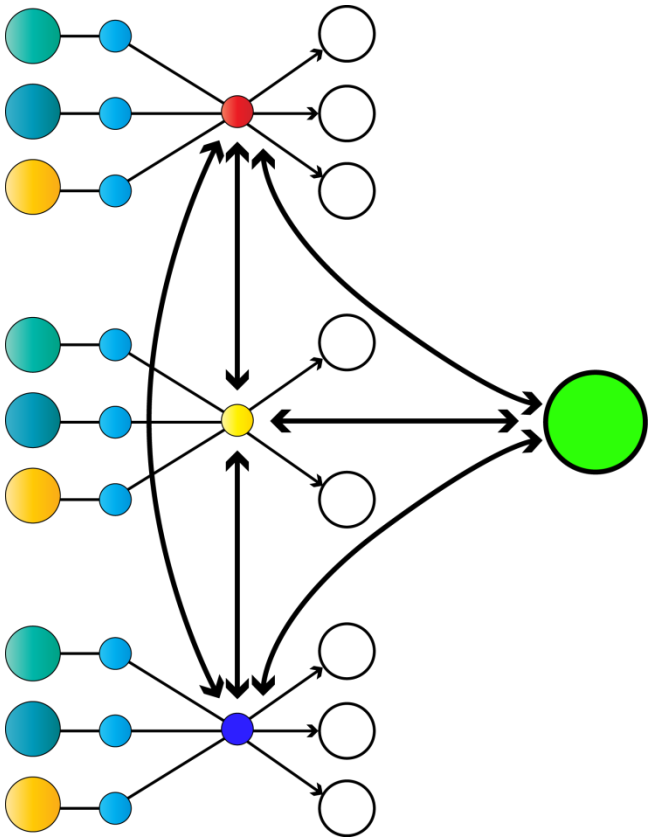
Мостовая схема



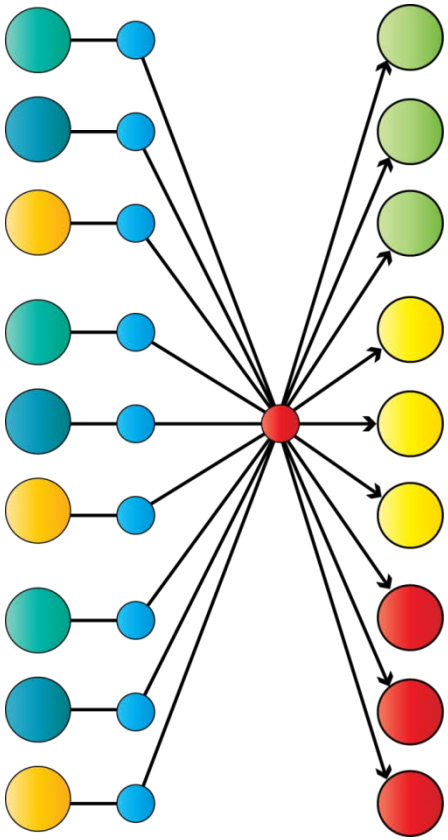
Модели формирования ЕПД



распределенная (сетевая)



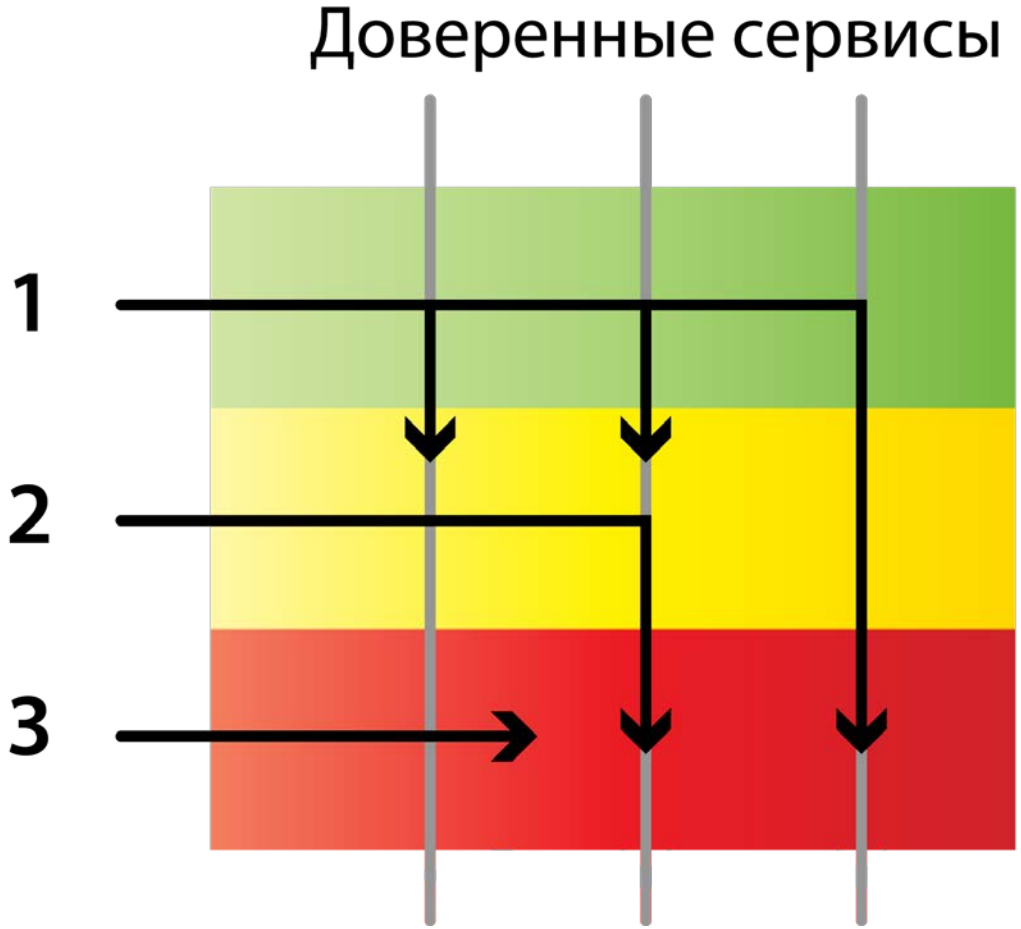
мостовая



централизованная

Уровни доверия AAA – часть ЕПД

Уровни Доверия AAA



Надежность аутентификации

- **Анализ рисков** → стандарты → безопасность → надежность → **качество**
- **Анализ надежности** (системы, состоящей из серверной и клиентской частей) → **соответствие требованиям** (в идеале – стандартам) → **качество**
- **Анализ процессов** → функциональная надежность → **качество**

Оценки надежности аутентификации

Надежность хранения аутентификатора: пароль- 0,43, закрытый ключ ЭП- 0,999

	процессы	минимум	макс.
1.	**Регистрация**		
1.1.	субъект ***предъявляет*** свои идентификаторы (удостоверения или ЭУ)		
1.2.	ЦР ***проверяет*** предъявленные субъектом идентификаторы	0,97	0,99
1.3.	ЦР ***создает*** учетную запись субъекта	0,99	0,999
1.4.	ЦР ***регистрирует/создает*** секрет (аутентификатор) и ***издает*** ЭУ	0,99	0,999
1.5.	ЦР ***делегирует*** права доступа субъекта к другим ИС	0,99	0,999
1.6.	ЦР ***выдает*** секрет и ЭУ на руки субъекту	0,9	0,999
2.	**Подтверждение подлинности**		
2.1.	Субъект ***хранит*** секрет и ЭУ	0,43	0,999
2.2.	Субъект ***предъявляет*** секрет и ЭУ доверяющей стороне (ДС)	0,99	0,999
3.	**Валидация**		
3.1.	ДС ***проверяет*** цепочку сертификатов ЭУ	0,99	0,999
3.2.	ДС ***проверяет*** срок действия ЭУ	0,99	0,999
3.3.	ДС ***проверяет*** действенность ЭУ	0,99	0,999
3.4.	ДС ***проверяет*** область действия	0,99	0,999
4.	**Принятие решения**		
4.1.	ДС ***принимает решение*** о результате аутентификации	0,99	0,999
		0,381	0,9801

Европейские требования к УЦ

- ЕС: уже несколько лет существует понятие **Trusted CA** – доверенный УЦ. Достаточно одной доверенной функции. Например, корректность проверки сертификатов ключей подписи (СКП). Все аккредитованные УЦ – Trusted

- **Qualified Trusted CA1** - *квалифицированный* доверенный УЦ = регламентированные процедуры не только с СКП, включая необходимый набор доверенных сервисов (см. первый слайд).

1. European Commission. Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. Brussels, XXX COM (2012) 238/2

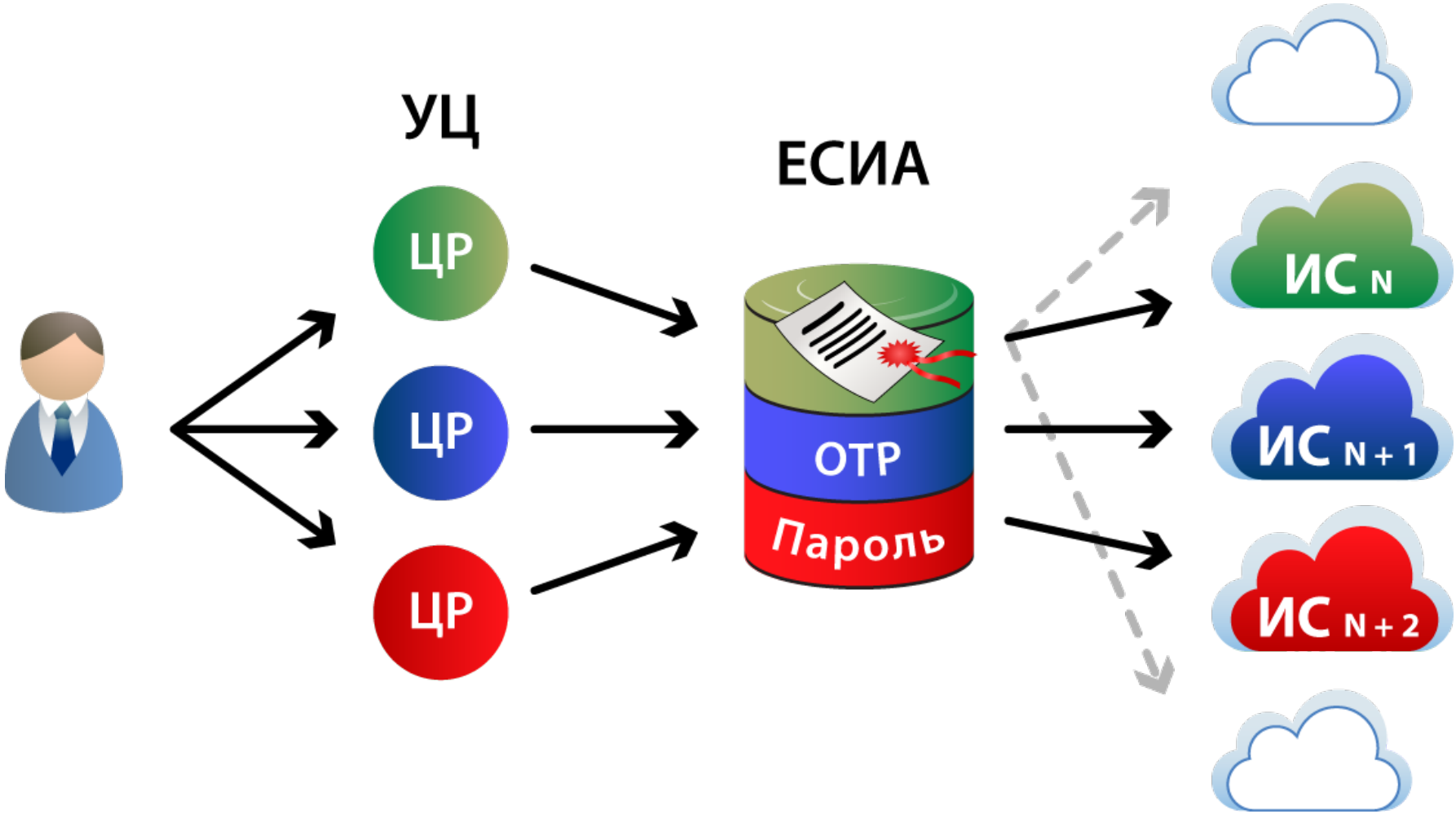
Переход к «облачным вычислениям»

- К настоящему времени вопросы информационной безопасности полностью не изучены
- Работа в «облаках» является зоной риска
- Выработаны только 2 понятных рекомендации:
  - Необходимо хранить данные в «облаке» только в зашифрованном виде
  - Обращать повышенное внимание на организацию аутентификации пользователей при доступе к облачным сервисам, аутентификация должна быть взаимной (двухсторонней: клиент-сервер) и строгой.

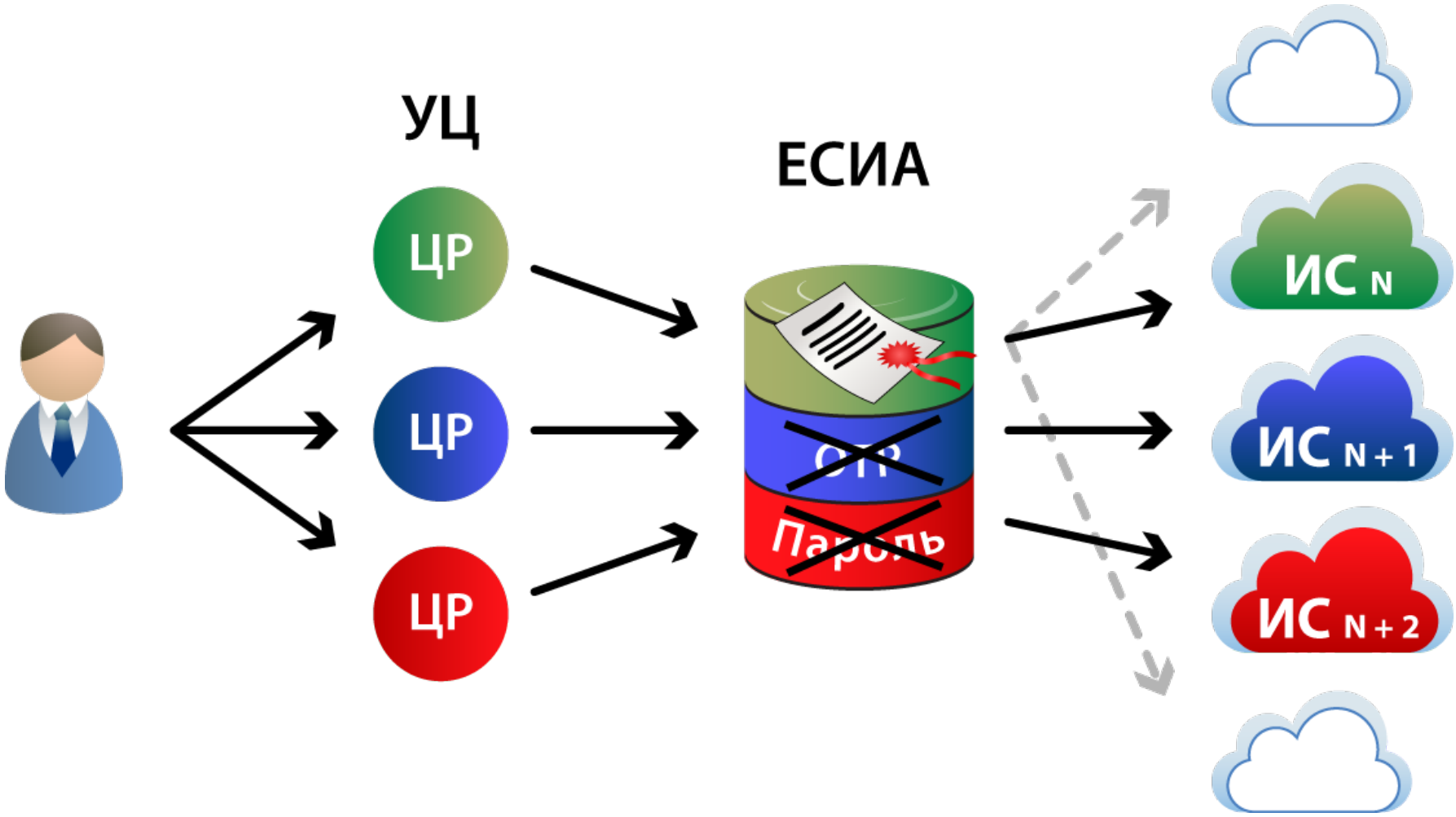
Задачи аутентификации для «облаков»

- Обеспечение удаленной регистрации;
- Безопасное ведение учетных записей пользователей;
- Обеспечение безопасного делегирования полномочий и доверия в облачные сервисы;
- Управление доверием при взаимодействии облачных сервисов;
- Контроль доступа в привязке к методу аутентификации пользователя, его роли и требований к уровню доверия в облаке;

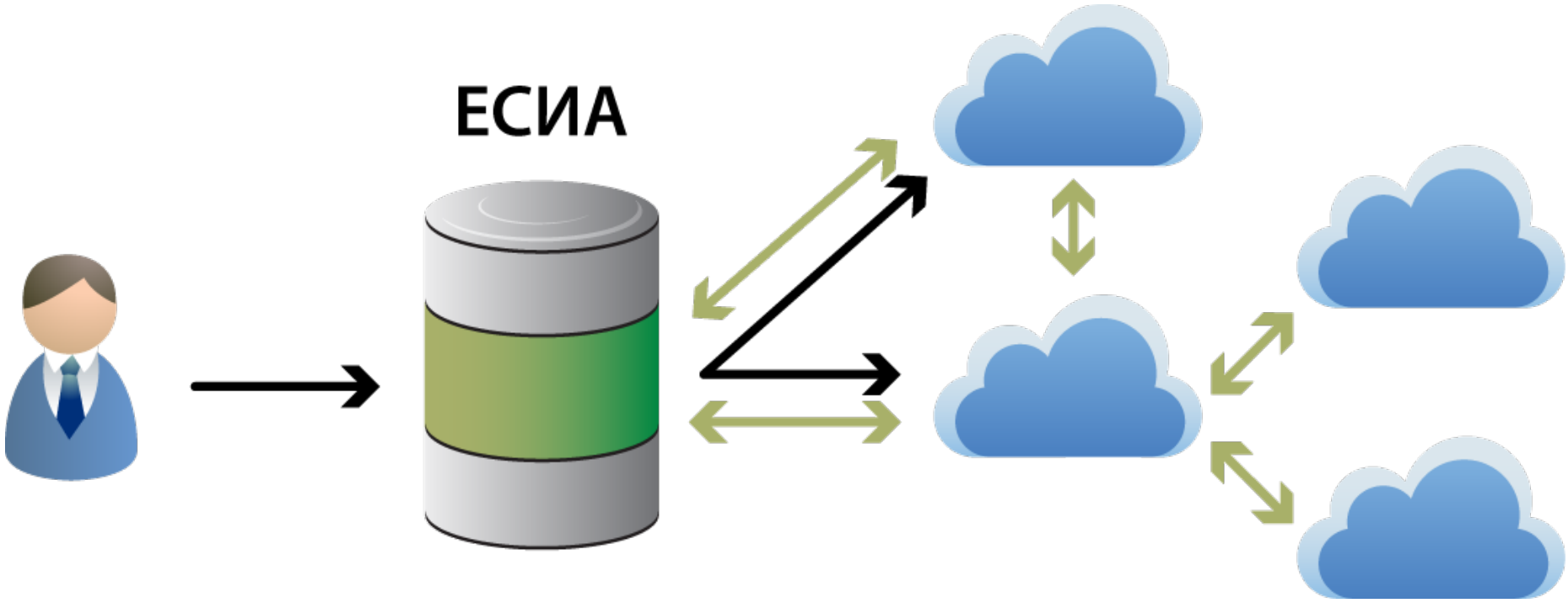
Регистрация к облачным сервисам



Регистрация к облачным сервисам



Доступ к облачным сервисам



Сервис аутентификации в ЕПД должен быть доверенным!

Спасибо за внимание!

a.sabanov@aladdin-rd.ru

Эволюция технологий

Микроконтроллеры для Java-карт (2007 – н.в.)

+ Быстрая периферия (USB-контроллер), драйвера в ОС

4

3

Смарт-карты (2000 – н.в.)

+ Разработаны для задач ИБ (secure by design)
+ Встроенная защищённая память
+ Общепринятые стандарты безопасности, аппаратно реализованы криптоалгоритмы
- Сложность расширения функционала, длительный цикл разработки и тестирования

2

Java-карты (2002 – н.в.)

+ Расширение функционала за счёт загрузки Java-апплетов
- Медленное взаимодействие с периферией

1

Микроконтроллеры общего назначения (1998 – н.в.)

- Не предназначены для задач ИБ (unsecure by design)
- Данные хранятся во внешней памяти, невозможность форм-фактора смарт-карты
- Программная реализация функций безопасности, алгоритмов шифрования
- Пропиетарная архитектура, нет стандартов

Примеры: iKey 1000, eToken R2, ruToken, Шипка

Важно: Есть факты взлома ключей, построенных на данной архитектуре (iKey1000)