Аладдин РД

Усиленная квалифицированная подпись и аутентификация

конференция
РусКрипто'2013

http://www.ruscrypto.ru/conference/

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

29 марта 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

с точки зрения применяемых технологий

Учетные записи и 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)

Аутентификация и электронная подпись

виды подписи	аутентификация	секрет (аутентификатор)
Простая	Да	Пароль
Усиленная неквалифицированная	Усиленная или Строгая	OTP или Закрытый ключ
Усиленная квалифицированная	Строгая взаимная	Закрытый ключ

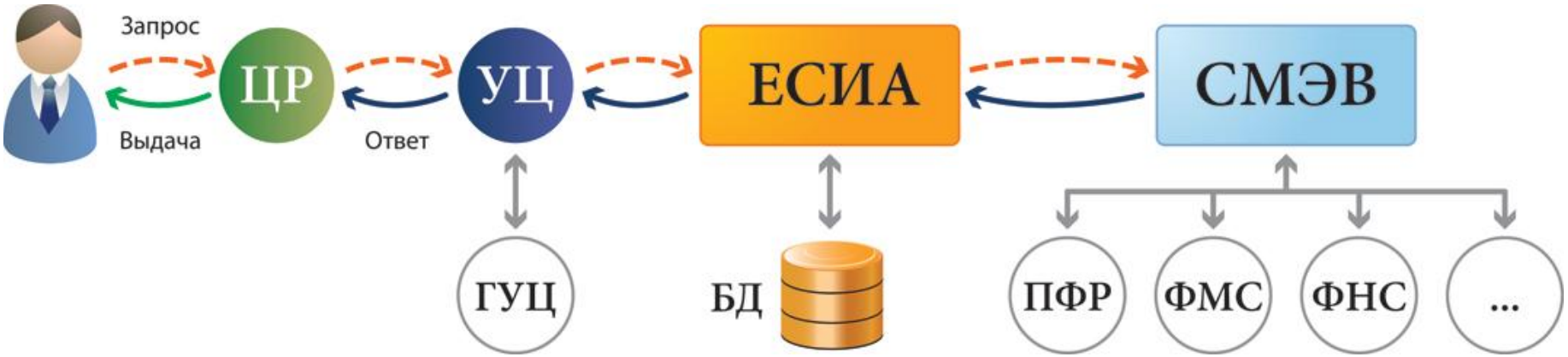
Основные процессы аутентификации

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 (собственно аутентификация)**		
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
2. Создание учетной записи в БД
3. Выпуск аутентификационных атрибутов (Credentials и токен)
4. Связывание этих атрибутов с пользователем
5. Делегирование прав
6. Определение политик доступа
7. Выдача токена (смарт-карта, USB-ключ) и Credentials

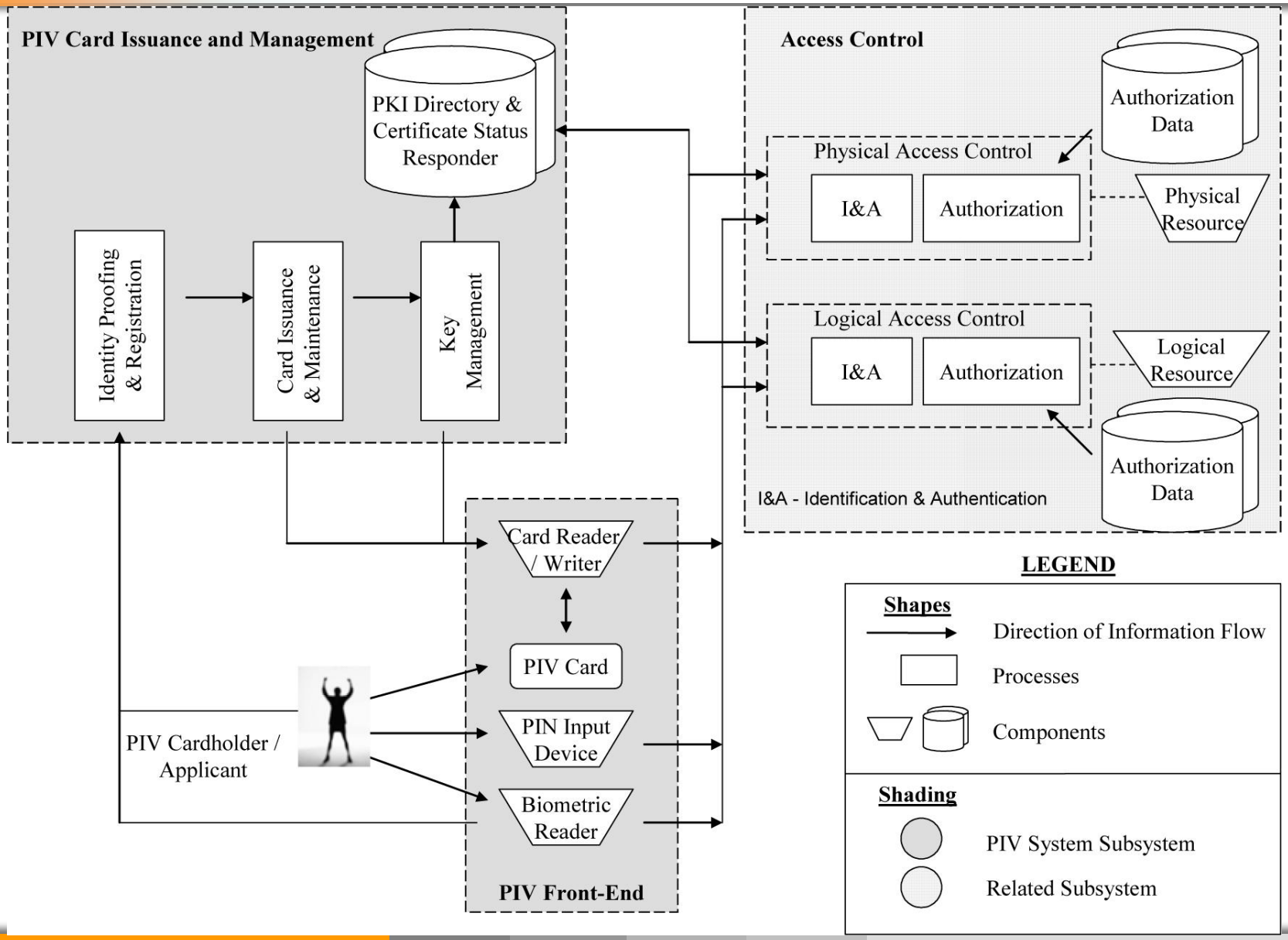
Способы хранения закрытого ключа

- Запись и последующее хранение в реестре компьютера
- запись на дискету или Flash-память
- 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.

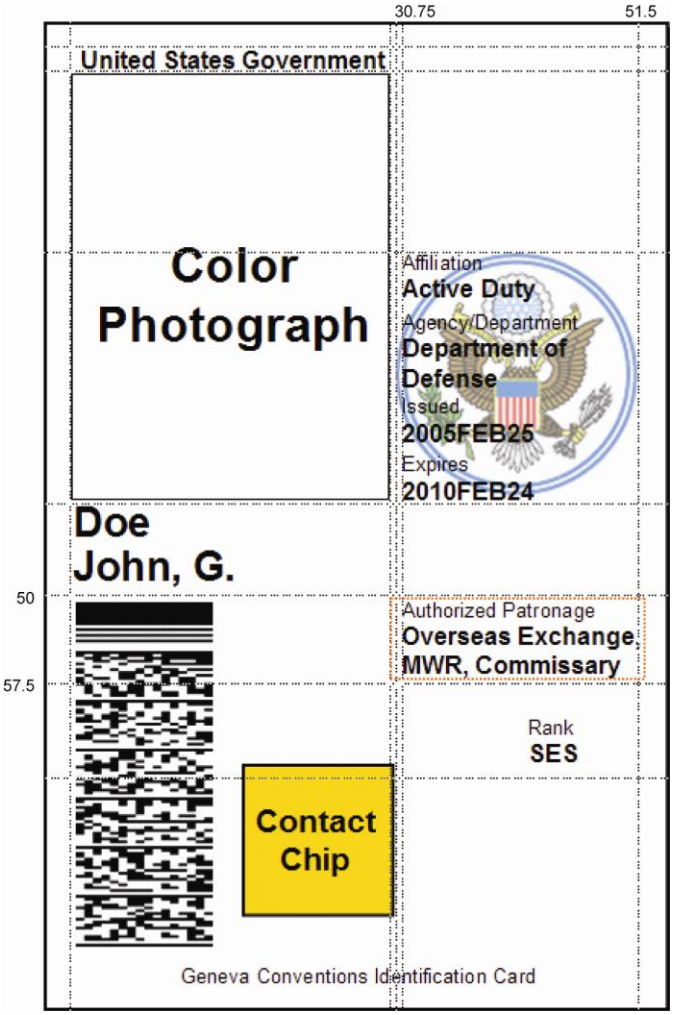
Пример Credentials из FIPS PUB 201-1

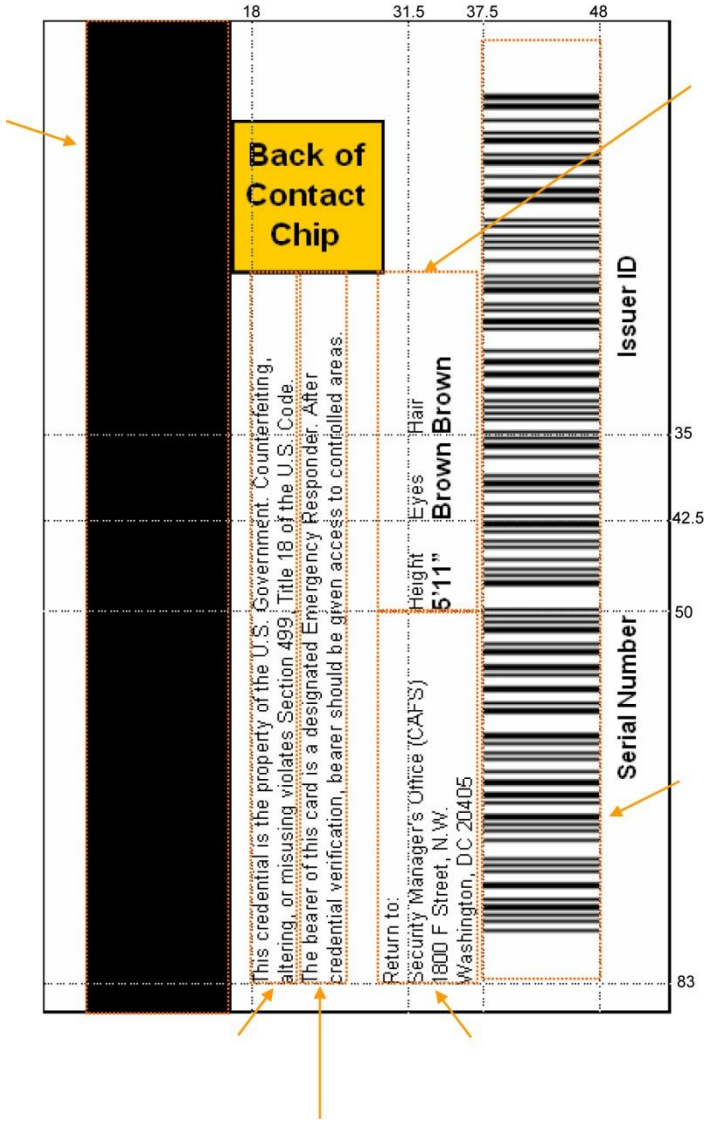
- Ключевая пара (открытый и закрытый ключи) и цифровой сертификат **аутентификации**
- Ключевая пара (открытый и закрытый ключи) и цифр. сертификат **электронной подписи**
- Ключевая пара (открытый и закрытый ключи) и цифровой сертификат для **управления ключами**
- Асимметричные или симметричные ключи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

Схема организации PIV федер. служб США

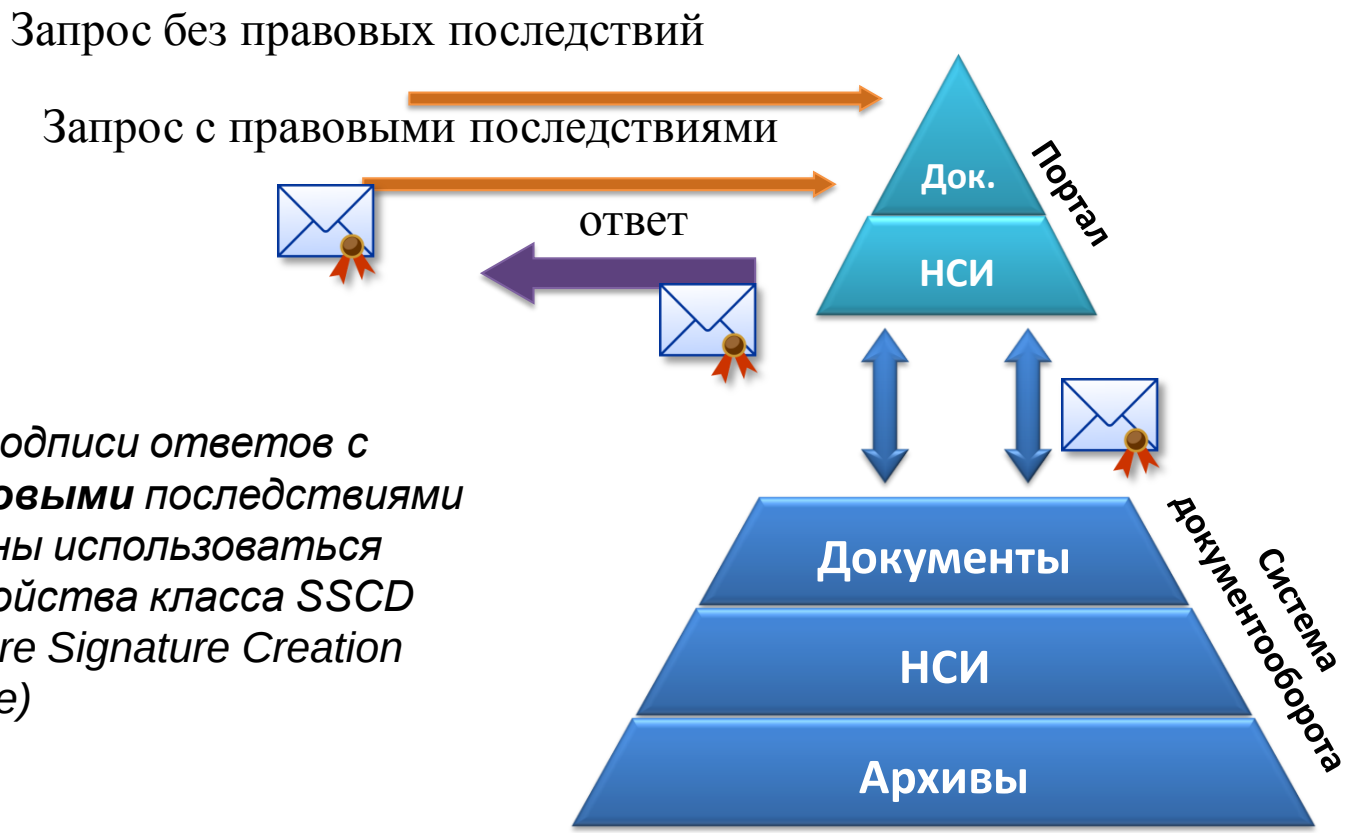


FIPS PUB 201-1: стандарт смарт-карты





Условная схема оказания госуслуг



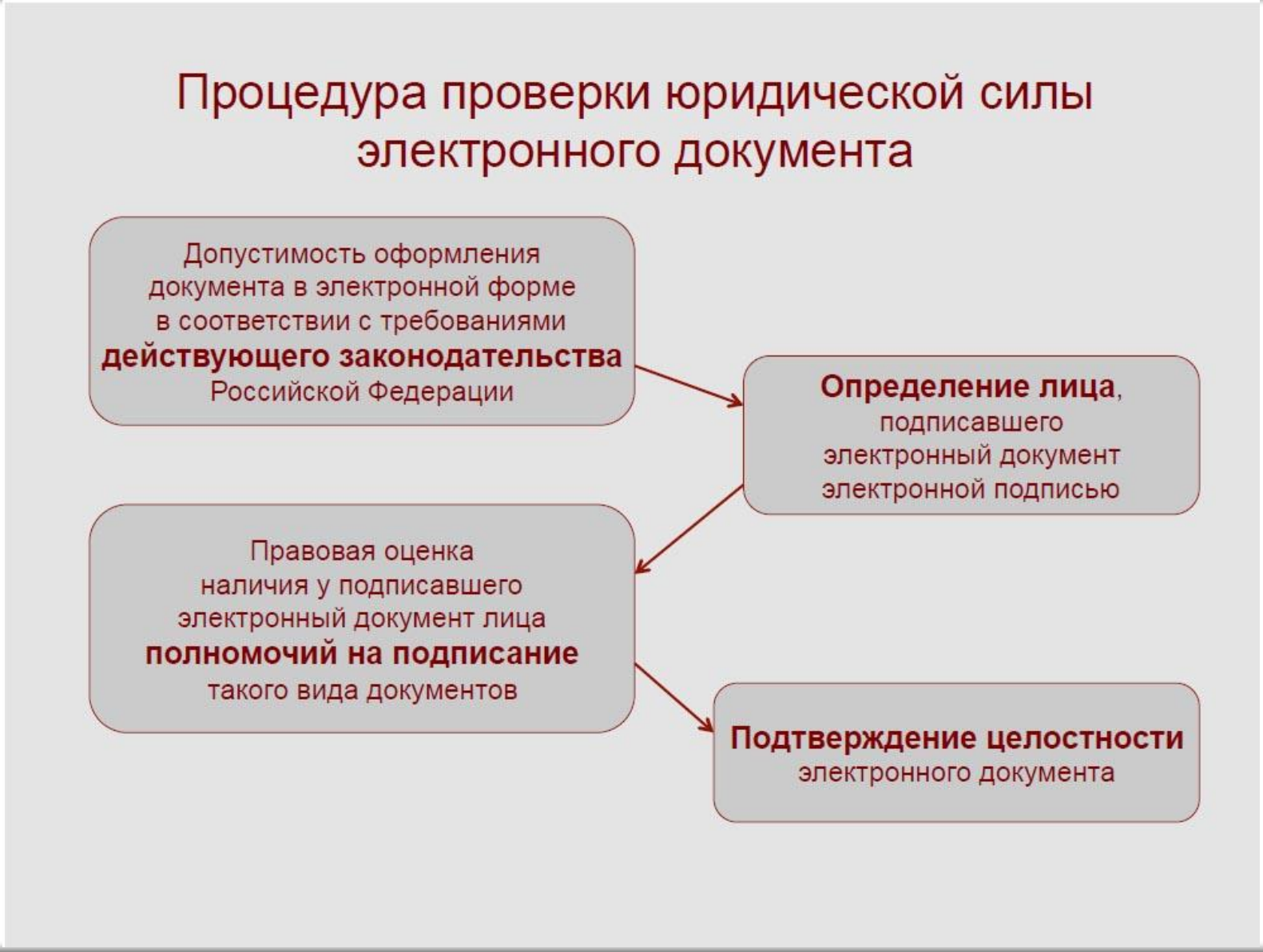
*Для подписи ответов с **правовыми** последствиями должны использоваться устройства класса SSCD (Secure Signature Creation Device)*

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

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

Перспективы развития нормативной базы

- ФСБ России отвечает только за криптографию;
- ФСТЭК создает нормативную базу, в том числе по аутентификации, с оговоркой «в целях защиты информации некриптографическими методами»:
  - В апреле появится проект «Требований к средствам двухфакторной аутентификации» и шесть профилей защиты на основе ГОСТ Р ИСО/МЭК 15408-2.
  - Готовятся и собственно технические требования к аутентификации, но опять же с оговоркой «в целях защиты информации некриптографическими методами»
- Минкомсвязи готовит нормативные документы по развитию пространства доверия. Имеется версия проекта закона «О внесении изменений в отдельные законодательные акты Российской Федерации» от 01.02.13

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.*

Сервис аутентификации в ЕПД должен быть доверенным!

Спасибо за внимание!

a.sabanov@aladdin-rd.ru