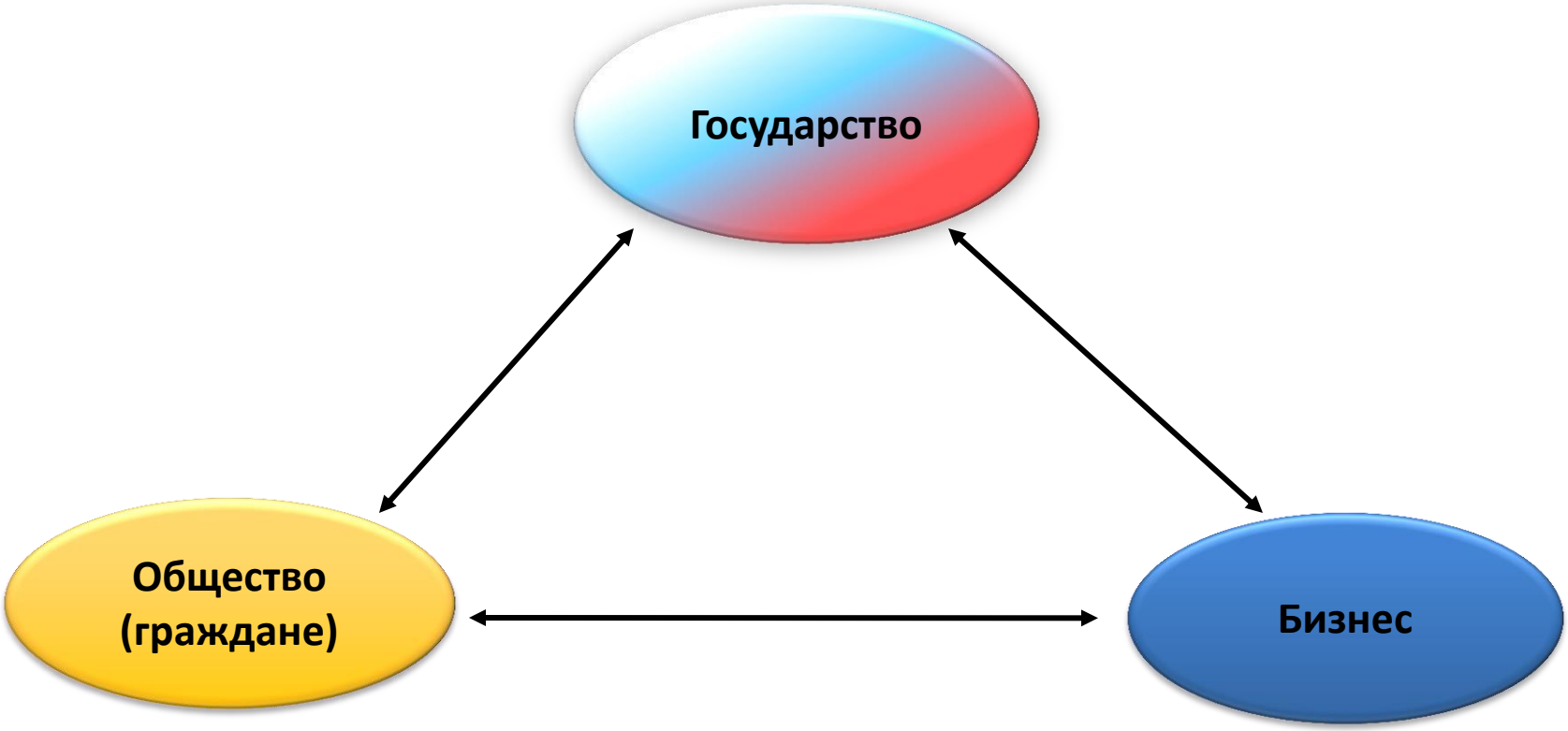
Анализ нормативно-правовой базы, отечественных и международных стандартов для развития защищенных сервисов на базе PKI

PKI-ФОРУМ РОССИЯ 2016 15-14 сеннтября СПб

14.09.2016

Сабанов А.Г.,
ген.дир.НП СОИБ,
Зам.ген.директора ЗАО Аладдин Р.Д.,
Академик МАС

Сферы обращения ЭП



Каждый гражданин в течение года обращается в те или иные органы государственной власти за получением услуг. В целом по оценкам экспертов, таких хождений в год около 300 миллионов только в органы государственной власти и органы муниципалитетов.

Виды электронного взаимодействия

Государство

Бизнес

Граждане

G2G	**B2G**	**C2G**
G2B	**B2B**	**C2B**
G2C	**B2C**	**C2C**

Методика определения "белых дыр" в НПА

1. Анализ бизнес-процессов в матрице видов электронного взаимодействия с позиций оценки рисков правовых последствий и вероятности их наступления.
2. Исследование регулирования собственно служб и основных функций участников PKI.
3. Анализ международных стандартов, руководств и рекомендаций, относящихся к PKI с точки зрения отсутствия подобных норм в РФ.
4. Рассмотрение задачи построения пространства доверия к электронным документам с правовыми последствиями

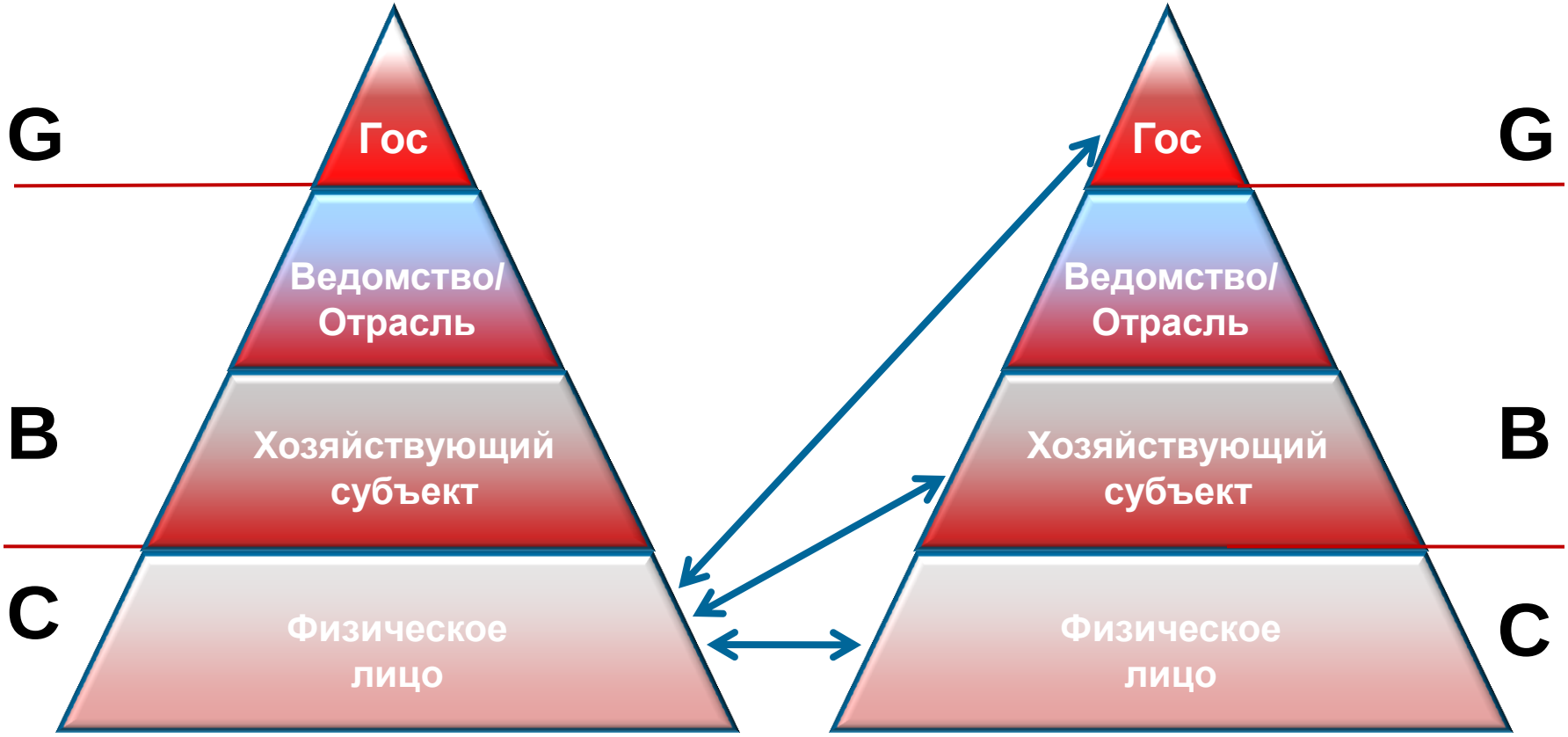
Текущее состояние

- Международные соглашения ЕЭС
- Три основных федеральных закона + отраслевые (о нотариате,….)
- Множество изменений в федеральных законах, АК, ГК, АПК, НК,..
- Приказы ФСБ России, ФСТЭК России и Минкомсвязи
- Методические материалы ФСТЭК и ФСБ России
- Отраслевая НПА (наиболее развита в КФС, имеются "продвинутые" требования в ФССП, ФНС,..)

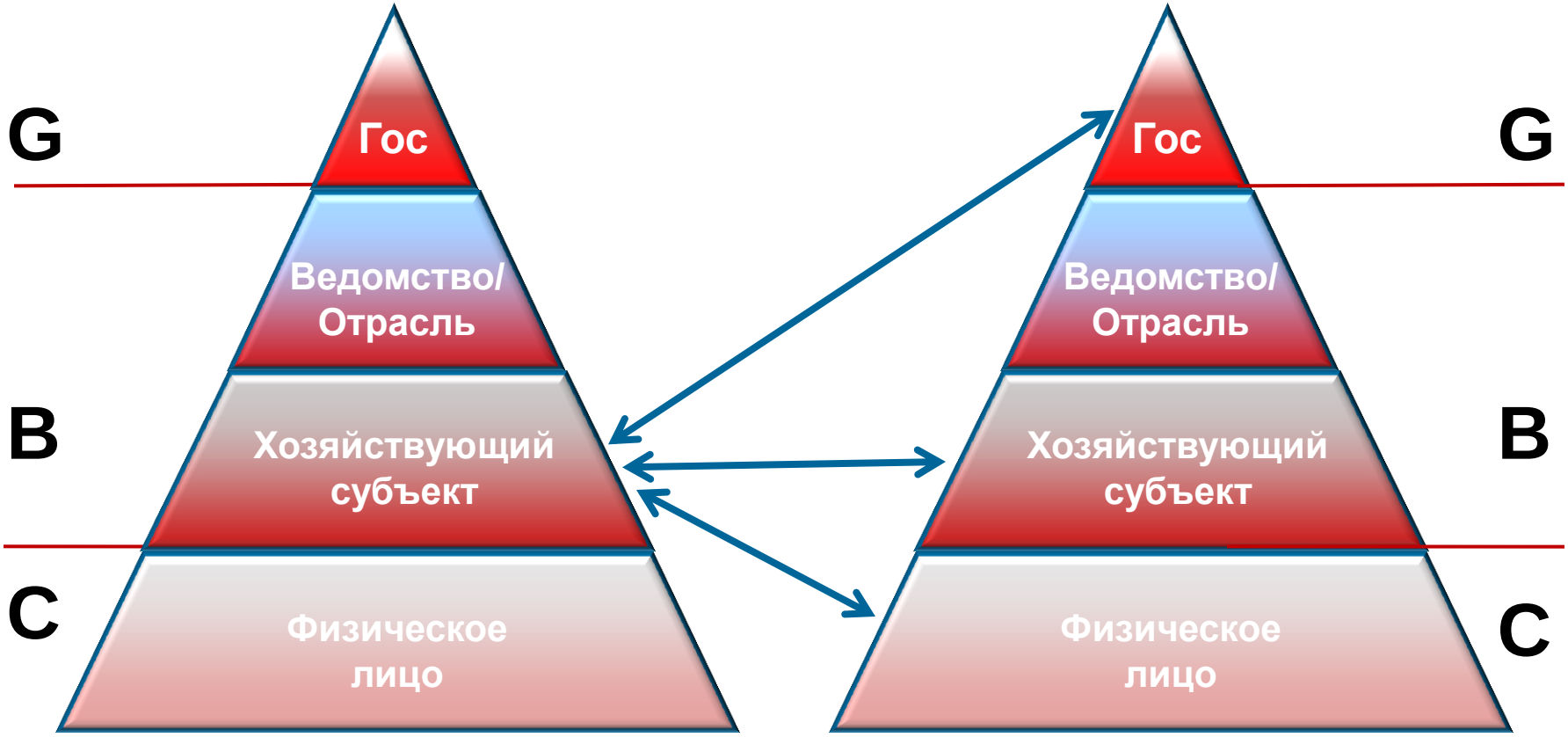
Методика определения "белых дыр" в НПА

1. Анализ бизнес-процессов в матрице видов электронного взаимодействия с позиций оценки рисков правовых последствий и вероятности их наступления.
2. Исследование регулирования собственно служб и основных функций участников PKI.
3. Анализ международных стандартов, руководств и рекомендаций, относящихся к PKI с точки зрения отсутствия подобных норм в РФ.
4. Рассмотрение задачи построения пространства доверия к электронным документам с правовыми последствиями

Схемы применения ЭП. Физ.лицо



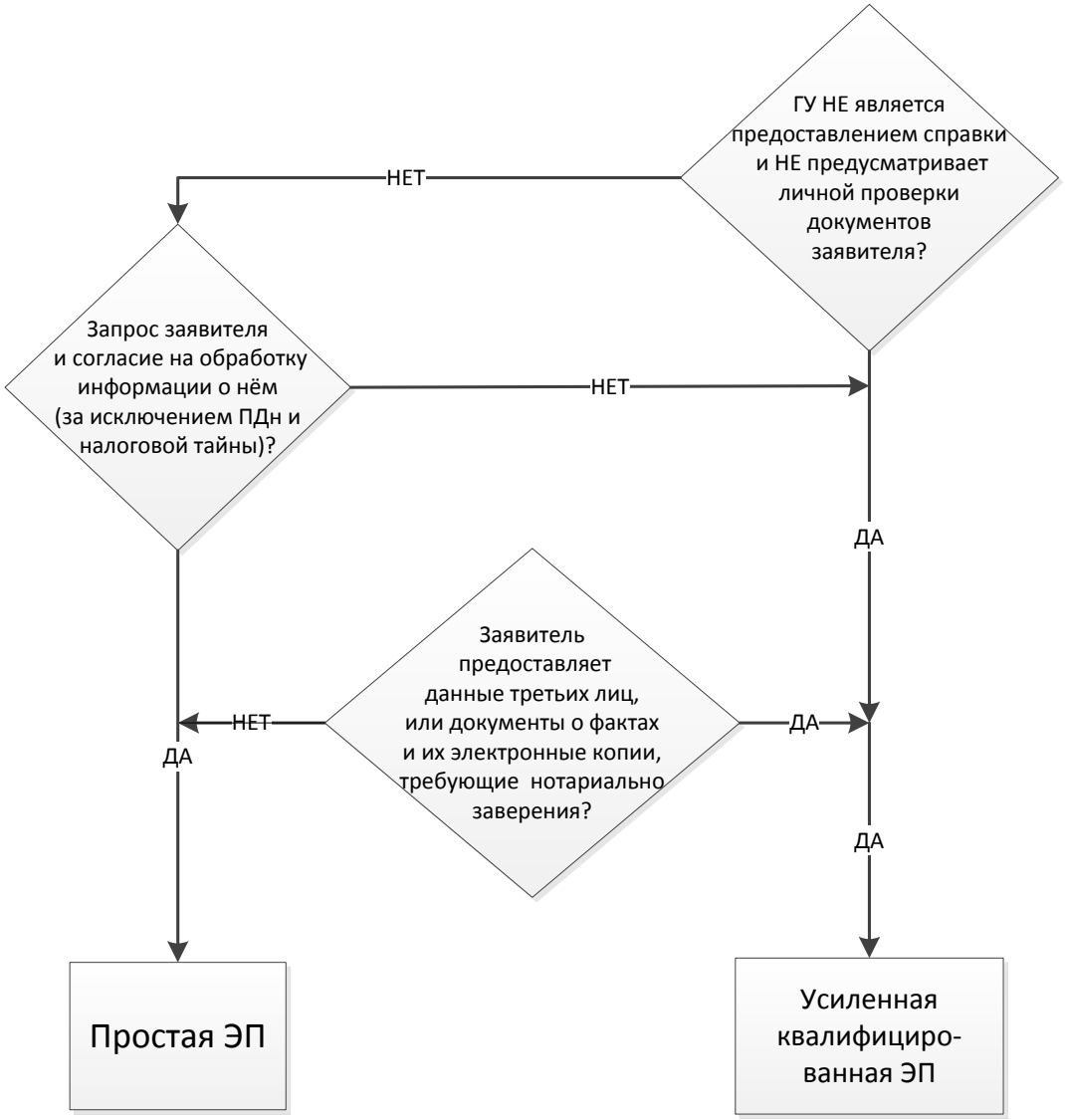
Схемы применения ЭЦП. Предприятие



Пример. Использование ЭП

Виды электронных документов, представляемых заявителями при обращении за предоставлением государственной или муниципальной услуги		Виды используемой электронной подписи		
		для справочной информации	взамен личного присутствия заявителя и предъявления им документа, удостоверяющего личность	в остальных случаях
1. Документы, заявителя	а) запрос заявителя	простая ЭП	простая ЭП	усиленная квалифицированная ЭП
	б) согласие заявителя на обработку информации о нем (за исключением ПДн, государственной и налоговой тайны)	простая ЭП	простая ЭП	усиленная квалифицированная ЭП
2. Документы с данными об ином лице, не являющемся заявителем		усиленная квалифицированная ЭП*	усиленная квалифицированная ЭП*	усиленная квалифицированная ЭП*
3. Документы от заявителя, удостоверяющие определенные юридические факты		усиленная квалифицированная ЭП*	усиленная квалифицированная ЭП*	усиленная квалифицированная ЭП*
4. Электронные копии документов, указанных в пунктах 2 и 3 настоящего документа, в следующих случаях:	а) если для предоставления услуг, требуется предоставление оригиналов или нотариально заверенных копий документов	усиленная квалифицированная ЭП	усиленная квалифицированная ЭП	усиленная квалифицированная ЭП
	б) нет условий подпункта "а" настоящего пункта	простая ЭП	простая ЭП	простая ЭП

Пример. Бизнес-процесс

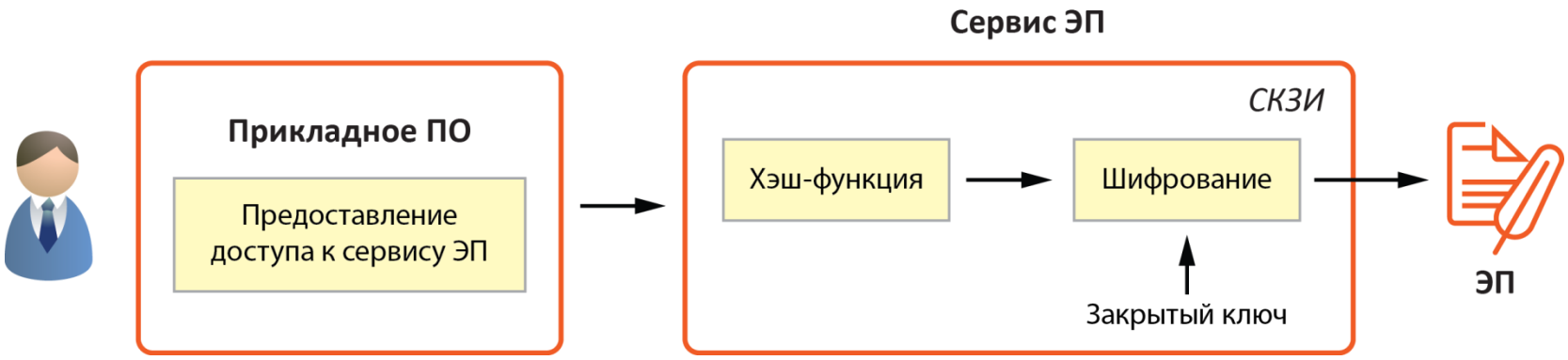


Пример. Госуслуги

- Заявка на гос.услугу. Сейчас используется простая подпись.
- Согласно ПП 789 от 13 августа 2016г. ответственность заявителя минимальна.
- Чем плоха простая подпись? Незащищенность. Если сертификат подделывают, то эккаунт любого гражданина, а еще страшнее, юр.лица, может быть вскрыт и использован в мошеннических целях.
- Несимметрия: чиновник обязан использовать УКЭП.

Что надо сделать? – Необходима дифференциация заявок по степени рисков наступления последствий. Четче определить, что такое госуслуга. Простая услуга – простая подпись, правовые последствия – УКЭП. С проверкой, действительно ли у обладателя заявки было желание и волеизъявление.

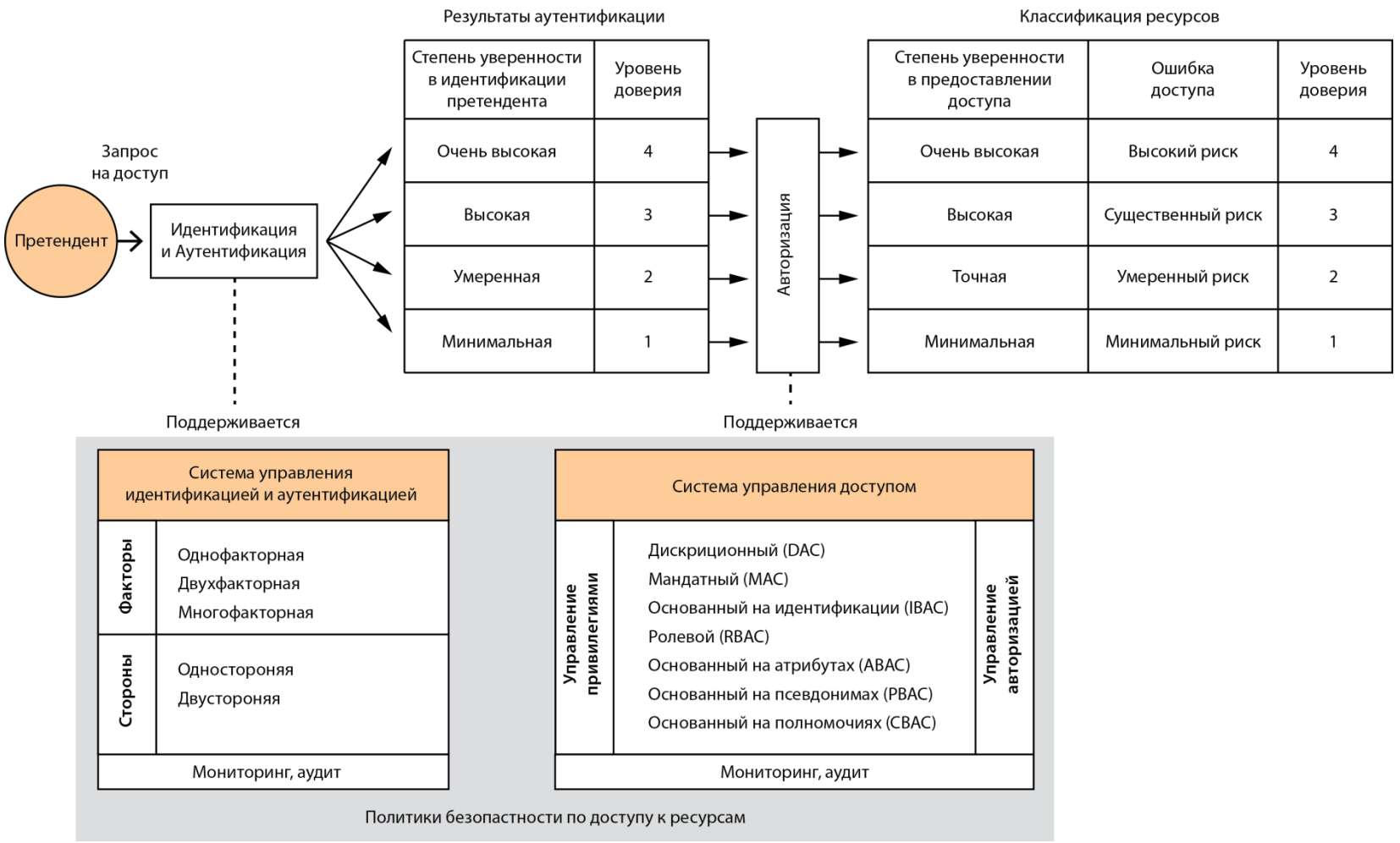
Один из вопросов. Что важнее?



Сертификат доступа

Сертификат проверки ЭП

Уровни доверия и риски



ISO/IEC 29146-2016

Методика определения "белых дыр" в НПА

1. Анализ бизнес-процессов в матрице видов электронного взаимодействия с позиций оценки рисков правовых последствий и вероятности их наступления.
2. Исследование регулирования собственно служб и основных функций участников PKI.
3. Анализ международных стандартов, руководств и рекомендаций, относящихся к PKI с точки зрения отсутствия подобных норм в РФ.
4. Рассмотрение задачи построения пространства доверия к электронным документам с правовыми последствиями

Иерархия нормативно правовой базы

Международные договоры

Конституция РФ

Федеральные законы

- Указы Президента РФ
- Постановления Правительства РФ
- Акты федеральных органов исполнительной власти, издаваемые в пределах их компетенции
- Акты органов местного самоуправления
- Локальные нормативные акты

Источники регулирования PKI

1. Федеральные законы.
2. Кодексы.
3. Подзаконные акты:
   a) Указы Президента
   b) Постановления Правительства
   c) Ведомственные приказы ФСБ России, ФСТЭК Росии, Минкомсвязи, Банка России,…

Метод решения: поиск в системе "Консультант+"

Основные термины PKI. **Инфраструктура открытых ключей**

- Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 17.06.2015) "Об утверждении государственной программы Российской Федерации "Информационное общество (2011 - 2020 годы)" – Приложение 3: "совершенствование **инфраструктуры электронного правительства** для реализации государственных функций в электронном виде..."
- Распоряжение Правления ПФ РФ от 11.10.2007 N 190р (ред. от 19.03.2010) "О внедрении защищенного электронного документооборота в целях реализации законодательства Российской Федерации об обязательном пенсионном страховании": Детализация конкретных действий участников Системы при использовании **инфраструктуры открытых ключей** определяется в Регламентах Удостоверяющих центров

Основные термины PKI. **Инфраструктура электронного правительства**

- ФЗ от 27.07.2010 N 210-ФЗ : Правила и порядок информационно-технологического взаимодействия информационных систем, используемых для предоставления государственных и муниципальных услуг в **электронной** форме, а также требования к **инфраструктуре**, обеспечивающей их взаимодействие, устанавливаются **Правительством** Российской Федерации
- ПП РФ от 08.06.2011 N 451 : Утвердить прилагаемое Положение об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме.
- ПП РФ от 21.07.2014 N 680: Минкомсвязи является госзаказчиком работ по формированию и обеспечению функционирования инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций (далее - инфраструктура взаимодействия), входящей в инфраструктуру электронного правительства

Основные термины PKI. **ДТС**

- Догововор о Евразийском экономическом союзе" (Подписан в г. Астане 29.05.2014) (ред. от 08.05.2015): "**доверенная третья сторона** " - организация, наделенная в соответствии с законодательством государств-членов правом осуществлять деятельность по проверке электронной цифровой подписи (электронной подписи) в электронных документах в фиксированный момент времени в отношении лица, подписавшего электронный документ"

- ПП РФ от 02.06.2008 N 418 (ред. от 01.07.2016) "О Министерстве связи и массовых коммуникаций Российской Федерации": 5.5.1. выполняет функции **доверенной третьей стороны** при обмене электронными документами в случаях, если ее участие в таком обмене предусмотрено международными договорами Российской Федерации

Основные термины PKI

Проверка валидности сертификата дано только в Приказе ФНС РФ от 17.12.2008 N ММ-3-6/665@ "Об утверждении Порядка ведения единого пространства доверия сертификатам ключей ЭЦП": Валидный СКП - сертификат, положительно прошедший все необходимые операции **проверки валидности**

Проверка цепочки сертификатов – 2 результата:

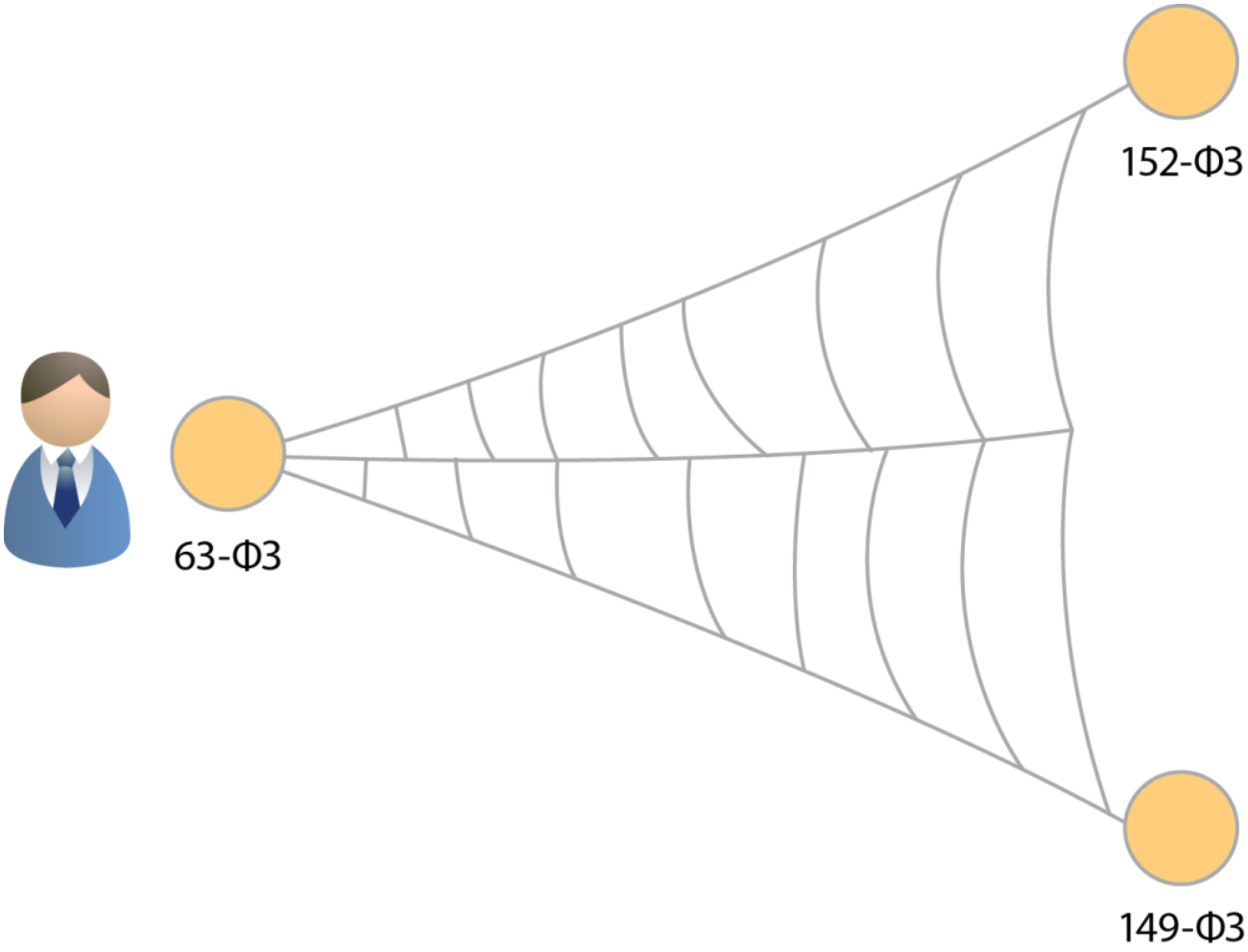
1)Приказ ФНС России от 14.01.2014 N ММВ-7-6/8@: **Цепочку** квалифицированных **сертификатов** ключей **проверки** электронной подписи (далее - КСКПЭП), начиная от КСКПЭП УЦ, непосредственно выдавшего юридическому лицу его КСКПЭП, и до корневого КСКПЭП, последнего в **цепочке сертификатов**, в соответствующие хранилища.

2)Приказ Росстата от 07.07.2011 N 313 (ред. от 21.05.2012): Отпечаток **сертификата** (thumbprint) - **цепочка** из 20 байт (хэш-код), уникально идентифицирующая тот или иной **сертификат**. Отпечаток **сертификата** предназначен для упрощения идентификации **сертификатов** отправителя, получателя, подписанта в программных продуктах, использующих СКЗИ

Основные термины PKI

- Удостоверяюзий центр определен в №63-ФЗ
- Сервер каталогов – нет результатов в системе "Консультант+"
- Репозиторий – нет результатов
- Сервер архивного хранения – нет результатов
- Служба доверенного времени – нет результатов
- Доверенное время – нет результатов
- Сертификат доступа – нет результатов

В России более 5350 федеральных законов, непосредственно PKI касается только №63-ФЗ



Вывод

Необходим федеральный закон или несколько законов, регулирующих правоотношения государства, бизнеса и личности при удаленном электронном взаимодействии. Основные задачи:

- Уточнение порядка и правил оказания государственных услуг в зависомости от наступления правовых последствий с учетом рисков для участников бизнес-процессов
- Решение проблемы повышения доверия к электронному взаимодействию и электронным документам, имеющим правовые последствия (идентификация и аутентификация участников, метки доверенного времени, валидация сертификатов доступа и проверки электронной подписи, проверка полномочий подписантов и т.д.)
- Определение основ создания простарнства доверия к электронным документам с правовыми последствиями
- Формулирование прав, обязанностей и ответственности участников удаленного электронного взаимодействия.

Зачем нужна система доверия

- Противодействие неуклонному росту мошенничеств и злоумышленных действий
- Необходимость полноценной замены бумажных документов электронными. Для бумажных документов имееется система доверия и криминалистическая экспертиза, для электронных пока такие механизмы не утверждены
- Отсутствие требований к доверенным сервисам (кроме УЦ) на уровне законов и подзаконных актов. Например, выбор технологий и средств ИА отдан на откуп владельцам ИС
- Актуальность проблем доверия в мире год из года растет (eIDAS -EC, USA Strategy, e-Authentication Австралия,…)

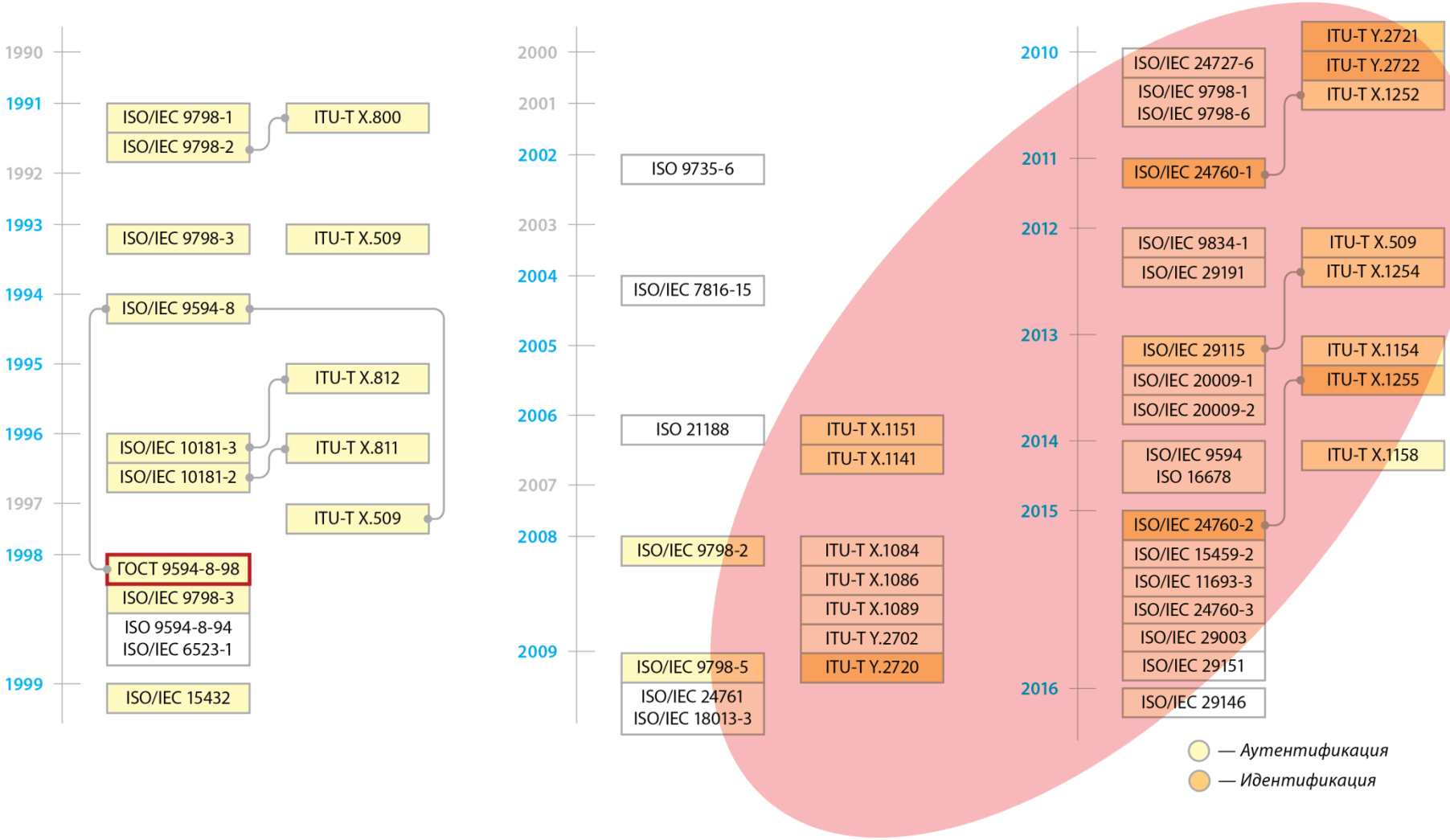
Некоторые актуальные задачи

1. Приблизить 63-ФЗ к Regulation 910/2014 ЕС или разработать новый ФЗ. Определить статус и требования к доверенным сервисам инфраструктуры использования ЭЦП, штампов времени, OCSP, DVCS как сервиса валидации ЭП, е-архивы, е-выписки, средства гарантированной доставки, защищенные Web-сервисы…
2. Ввести сертификаты доступа (сертификатф аутентификации).
3. Реакция УЦ на отзыв сертификата должна быть не 8 часов, а считанные минуты.
4. Определить, что такое "доказательства момента подписания"(достаточно иметь доказательства выполнения проверки ЭП ,когда сертификат был еще действителен)
5. Определиться со ст. 7 федерального закона 63-ФЗ и иностранными ЭП: если иностранная подпись неквалифицированная, то наличие действующей квитанции валидации или цепочки из них придает иностранной подписи статус квалифицированной? П.1.,ст.7 говорит о признании иностр.ЭП, но ни в одном акте не сказано, как это реализовать технически
6. Атрибутные сертификаты, связанные не только с сертификатом открытого ключа, а с абстрактными данными - это самоактуализируемые выписки из реестров, фактический аналог отсоединенной ЭП, которую можно отозвать (е-лицензии, е-сертификаты на товары и т.д.)
7. В PKI авторство и неотрекаемость от ЭП определяется исключительно фактом единоличного владения и управления закрытым ключом. Норму возможности передачи закрытого ключа необходимо исключить из 63-ФЗ. Риски: возможность копирования закрытого ключа при использовании современных СКЗИ пока не исключены, если закрытый ключ будет скопирован, возможны судебные разбирательства, которые могут зайти в тупик.

Методика определения "белых дыр" в НПА

1. Анализ бизнес-процессов в матрице видов электронного взаимодействия с позиций оценки рисков правовых последствий и вероятности их наступления.
2. Исследование регулирования собственно служб и основных функций участников PKI.
3. Анализ международных стандартов, руководств и рекомендаций, относящихся к PKI с точки зрения отсутствия подобных норм в РФ.
4. Рассмотрение задачи построения пространства доверия к электронным документам с правовыми последствиями

Международные стандарты



История обновлений X.509

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.509	1988-11-25	
2.0	ITU-T X.509	1993-11-16	7
3.0	ITU-T X.509	1997-08-09	7
3.1	ITU-T X.509 (1997) Technical Cor. 1	2000-03-31	7
3.2	ITU-T X.509 (1997) Technical Cor. 2	2001-02-02	7
3.3	ITU-T X.509 (1997) Technical Cor. 3	2001-10-29	7
3.4	ITU-T X.509 (1997) Technical Cor. 4	2002-04-13	17
3.5	ITU-T X.509 (1997) Technical Cor. 5	2003-02-13	17
3.6	ITU-T X.509 (1997) Technical Cor. 6	2004-04-29	17
4.0	ITU-T X.509	2000-03-31	7
4.1	ITU-T X.509 (2000) Technical Cor. 1	2001-10-29	7
4.2	ITU-T X.509 (2000) Technical Cor. 2	2002-04-13	17
4.3	ITU-T X.509 (2000) Technical Cor. 3	2004-04-29	17
4.4	ITU-T X.509 (2000) Technical Cor. 4	2007-01-13	17
5.0	ITU-T X.509	2005-08-29	17
5.1	ITU-T X.509 (2005) Cor. 1	2007-01-13	17
5.2	ITU-T X.509 (2005) Cor. 2	2008-11-13	17
5.3	ITU-T X.509 (2005) Cor. 3	2011-02-13	17
6.0	ITU-T X.509	2008-11-13	17
6.1	ITU-T X.509 (2008) Cor. 1	2011-02-13	17

Методика определения "белых дыр" в НПА

1. Анализ бизнес-процессов в матрице видов электронного взаимодействия с позиций оценки рисков правовых последствий и вероятности их наступления.
2. Исследование регулирования собственно служб и основных функций участников PKI.
3. Анализ международных стандартов, руководств и рекомендаций, относящихся к PKI с точки зрения отсутствия подобных норм в РФ.
4. Рассмотрение задачи построения пространства доверия к электронным документам с правовыми последствиями

Юридическая сила

- Юридическая сила электронного документа (ЭД) может быть опредедена как способность ЭД вызывать правовые последствия [на основе ГОСТ Р 7.0.8 – 2013]

Юридическая значимость

- Юридическая значимость документа – свойство документа выступать в качестве подтверждения деловой деятельности либо событий личного характера [ГОСТ Р 7.0.8 – 2013]

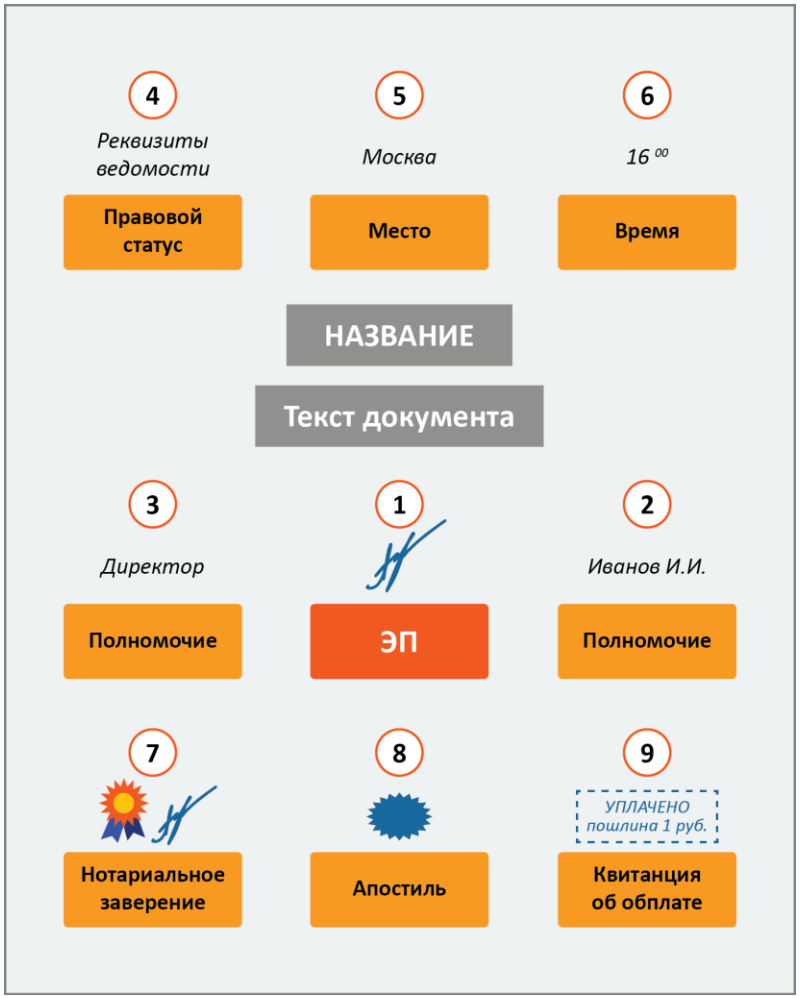
Юридическая сила электронных документов

Проверка юридической силы документа состоит из этапов:

- Допустимость оформления документа в электронной форме в соответствии с требованиями действующего законодательства Российской Федерации;
- Определение лица, подписавшего электронный документ электронной подписью;
- Правовая оценка наличия у подписавшего электронный документ лица полномочий на подписание такого вида документов;
- Подтверждение целостности электронного документа.

Переход на безбумажный оборот

Аналогия с бланком бумажного документа



Постановление Правительства от 15.06.2009 №477 для бумажных документов в ФОИВ (24 реквизита)

Минимальный набор сервисов безопасности

- Аутентификация
- Электронная подпись
- Метка доверенного времени (RFC 3161 «Time-Stamp Protocol (TSP)»
- Валидация сертификата ключа проверки подписи (RFC 2459)
- Проверка полномочий подписанта

Сервис аутентификации

- обеспечение доказательства подлинности предъявленного идентификатора (ISO/IEC 10181-2:1996, 9798-3:1998);
- доказательство принадлежности аутентификатора, с помощью которого производится доказательство подлинности, конкретному объекту (ISO/IEC 24760-2: 2015);
- аутентификация сторон – подтверждение того, что взаимодействующая сторона является той, за которую себя выдает (ISO 29115: 2013).

Сервисы безопасности: подпись

- аутентификация источника данных – подтверждение подлинности источника полученных данных (ISO 7498-2);
- обеспечение целостности данных, означающее, что данные не были модифицированы или уничтожены неавторизованным образом (ISO 7498-2);
- невозможность отрицания авторства – сервис защиты от отрицания автором факта создания или отправления им сообщения (ISO/IEC 13888-1).

Пример отличий. Подпись

Собственноручная подпись	Цифровая подпись
Не зависит от подписываемого текста, всегда одинакова	Зависит от подписываемого текста, разная для различных текстов
Неразрывно связана с подписывающим лицом, однозначно определяется его психофизическими свойствами, не может быть утеряна	Определяется секретным ключом, принадлежащим подписывающему лицу, который может быть утерян владельцем
Неотделима от носителя (бумаги), поэтому отдельно подписывается каждый экземпляр документа	Легко отделима от документа, поэтому верна для всех его копий
Не требует для реализации дополнительных механизмов	Требует дополнительных механизмов, реализующих алгоритмы её вычисления и проверки
Не требует создания поддерживающей инфраструктуры	Требует создания доверенной инфраструктуры сертификатов открытых ключей
Не имеет срока давности	Имеет ограничения по сроку действия

Зарубежный опыт применения электронного документооборота

- Тенденция распространения электронных документов в практике государственного управления является общемировой. Успех внедрения электронных документов и электронного документооборота обеспечивается наличием государственной политики и ее законодательного обеспечения.
- Анализ опыта подчеркивает необходимость участия в процессах внедрения электронного документооборота архивных служб, которые прямо заинтересованы в обеспечении контроля жизненного цикла электронных документов.
- Зарубежный опыт указывает на то, что полностью отказаться от документов на бумажном носителе в современных условиях невозможно. В течение обозримого периода времени бумажные документы и электронные документы будут сосуществовать параллельно, причем в массовом порядке.
- Часть документов по-прежнему будет создаваться и храниться только на бумажных носителях, которые позволяют гарантированно сохранять информацию на протяжении нескольких столетий.

Модель Единого пространства доверия

Создание правового поля для юридически - значимого электронного документооборота

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

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

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
- Инфраструктура управления ключами и сертификатами
- Инфраструктура идентификации и аутентификации

Единое пространство доверия (ЕПД)

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

Принципы построения ЕПД:

- Должна обеспечиваться совместимость ИТ-решений и сервисов всех компонентов ЕПД
- Сервисы безопасности должны быть выстроены по уровням доверия.
- Уровень доверия цепочки взаимодействия должен определяться уровнем доверия самого слабого звена.

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.*

Спасибо за внимание!

Международные соглашения

- Договор о Евразийском экономическом союзе. Астана. 29 мая 2014г.
- Решение Евразийской экономической комиссии от 23 ноября 2012г. N 95 "О мероприятиях, направленных на обеспечение взаимного признания электронной цифровой подписи в рамках Таможенного союза и Единого экономического пространства в целях исполнения Соглашения о государственных (муниципальных) закупках".
- Решение Евразийской экономической комиссии от 17 декабря 2013г. N 302 "Об утверждении плана мероприятий по вопросу взаимного признания электронной цифровой подписи, изготовленной в соответствии с законодательством одного государства – члена таможенного союза и единого экономического пространства (Республики Беларусь, Республики Казахстан или Российской Федерации) другим государством – членом Таможенного союза и Единого экономического пространства (Республикой Беларусь, Республикой Казахстан или Российской Федерацией) в целях исполнения соглашения о государственных (муниципальных) закупках от 9 декабря 2010 года".