Аладдин РД

О формировании единого пространства доверия в Российской Федерации

Алексей Сабанов,
Заместитель генерального директора

18 сентября 2012г.

План презентации

1. Что такое Единое пространство доверия (ЕПД)
2. Доверенные сервисы на базе PKI
3. Качество доверенных сервисов
4. Аутентификация – основа доверия при удаленном взаимодействии
5. Вопросы надежности аутентификации
6. Анализ потенциальных возможностей построения ЕПД
7. Заключение
8. Предложения в проект меморандума конференции

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 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».
- Определение: ***ЕПД - 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** 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.*

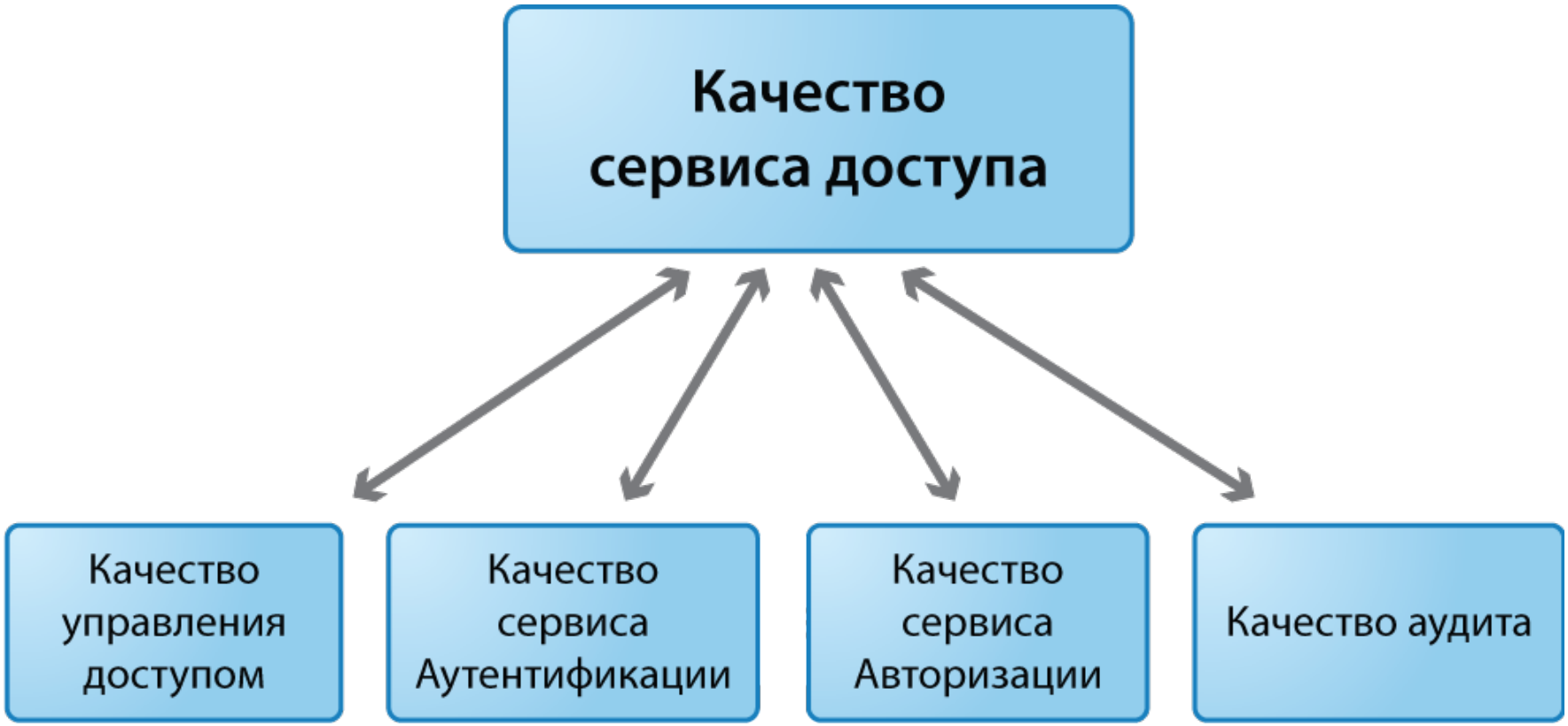
Качество доверенных сервисов

- ГОСТ Р ИСО 9000-2008: качество (*quality*) - степень соответствия совокупности присущих характеристик некоторым требованиям.

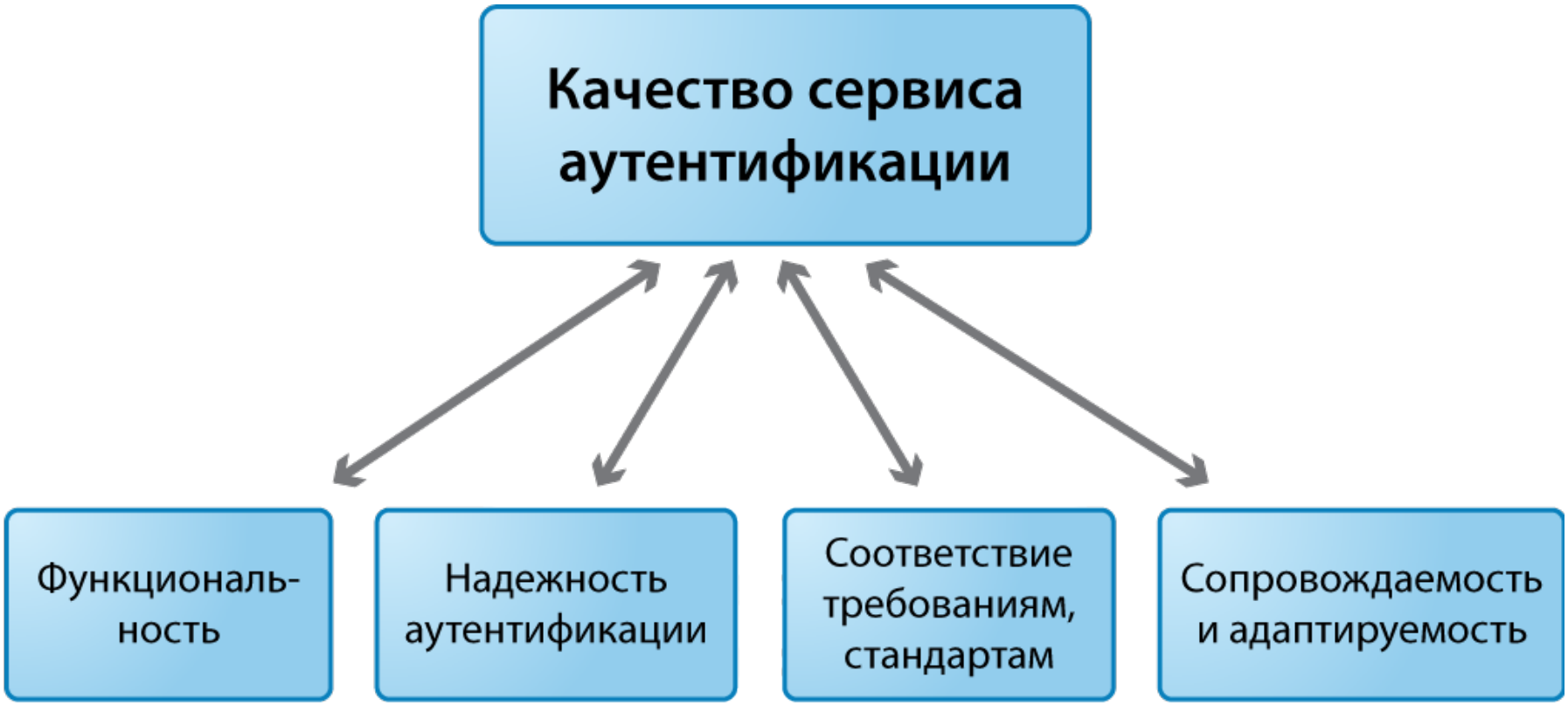
Семинар ТС56 МЭК (Лондон,2006г.)

Качество → соответствие стандартам → гарантии качества → страхование

Доступность услуг и облачных сервисов



Аутентификация – доверенный сервис

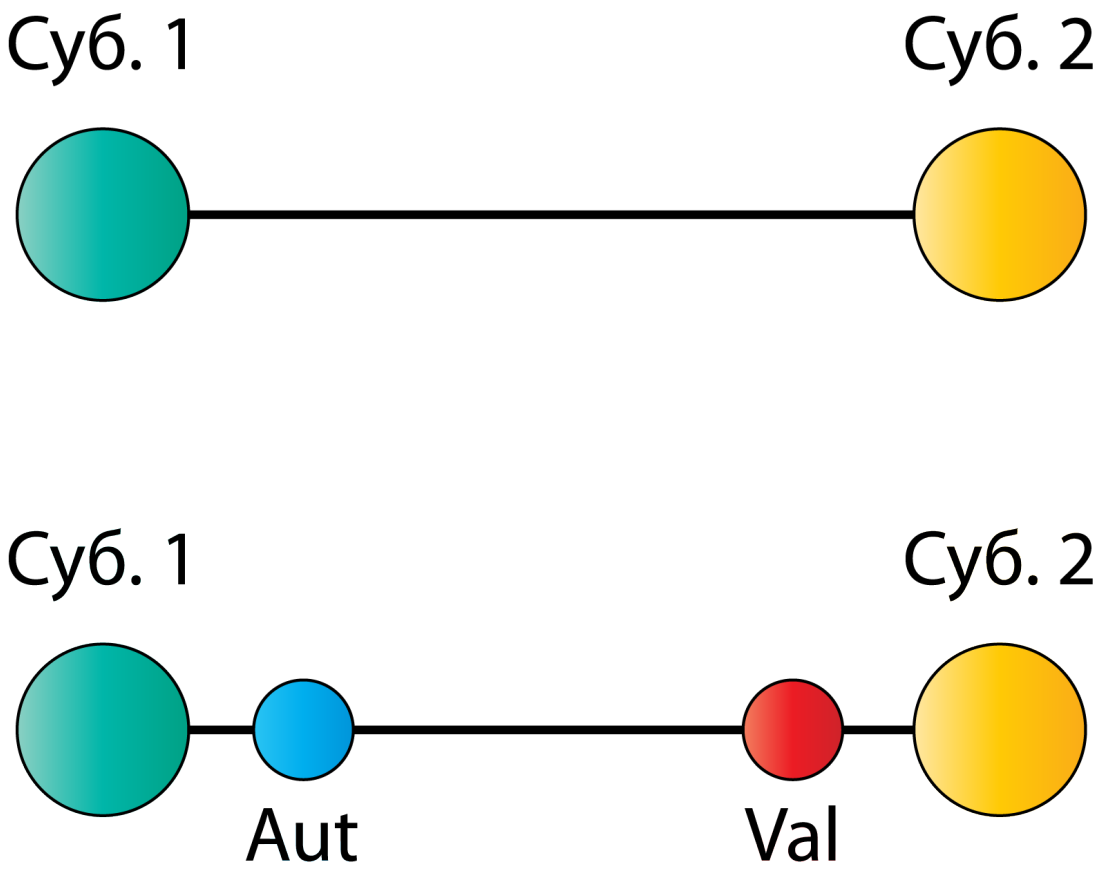


Развитие требований

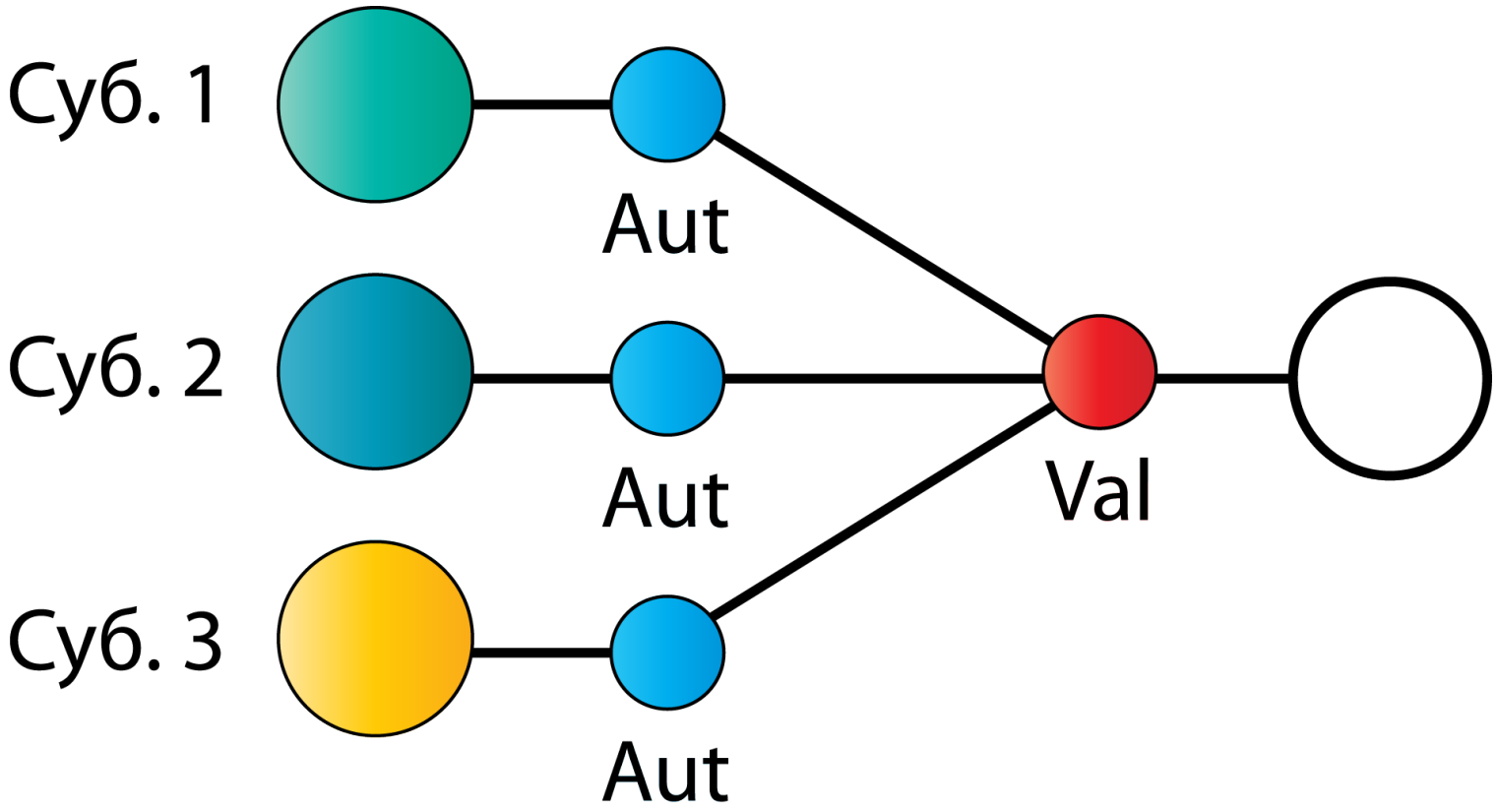
Нормативная база по аутентификации

- 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.

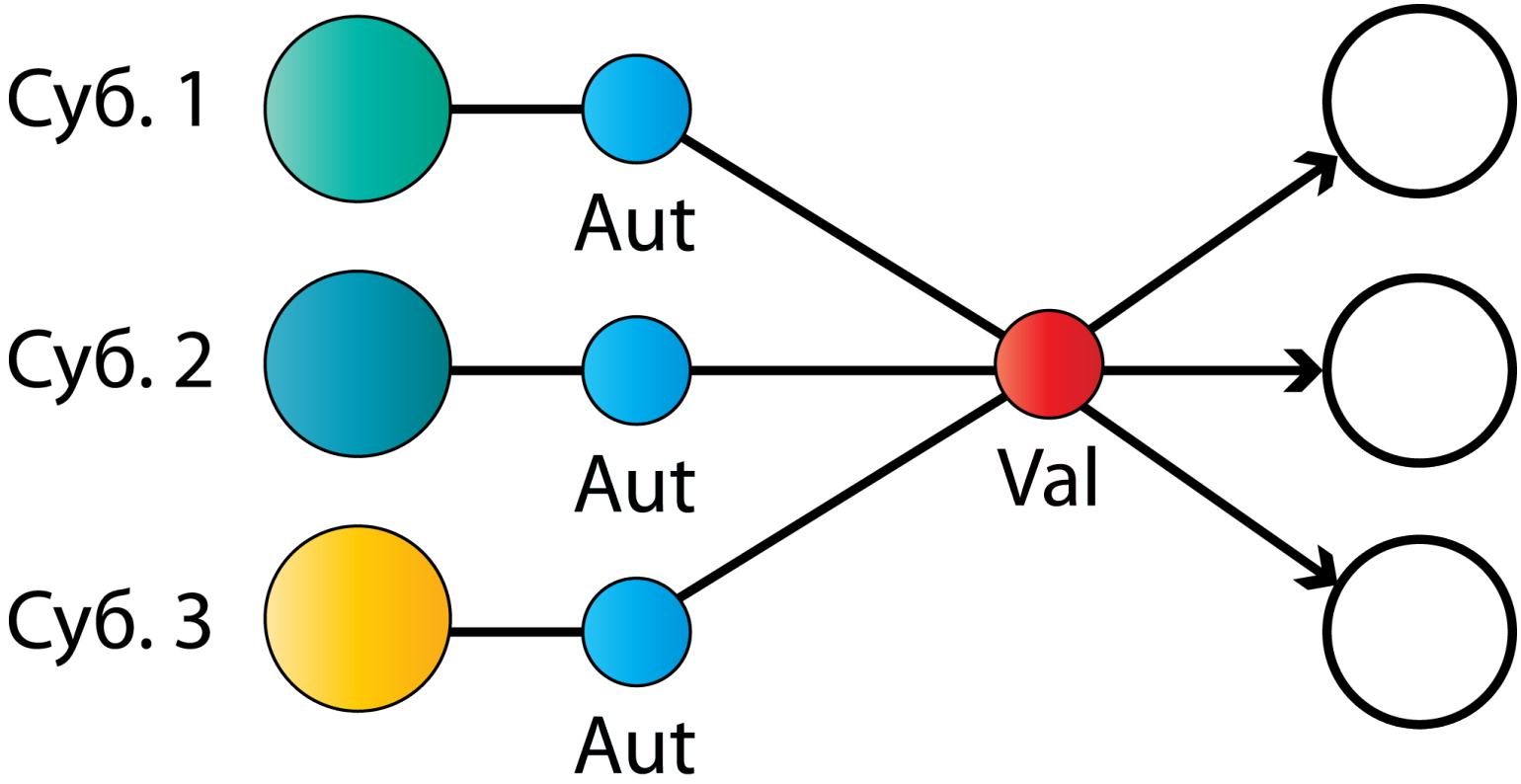
Отношения доверия



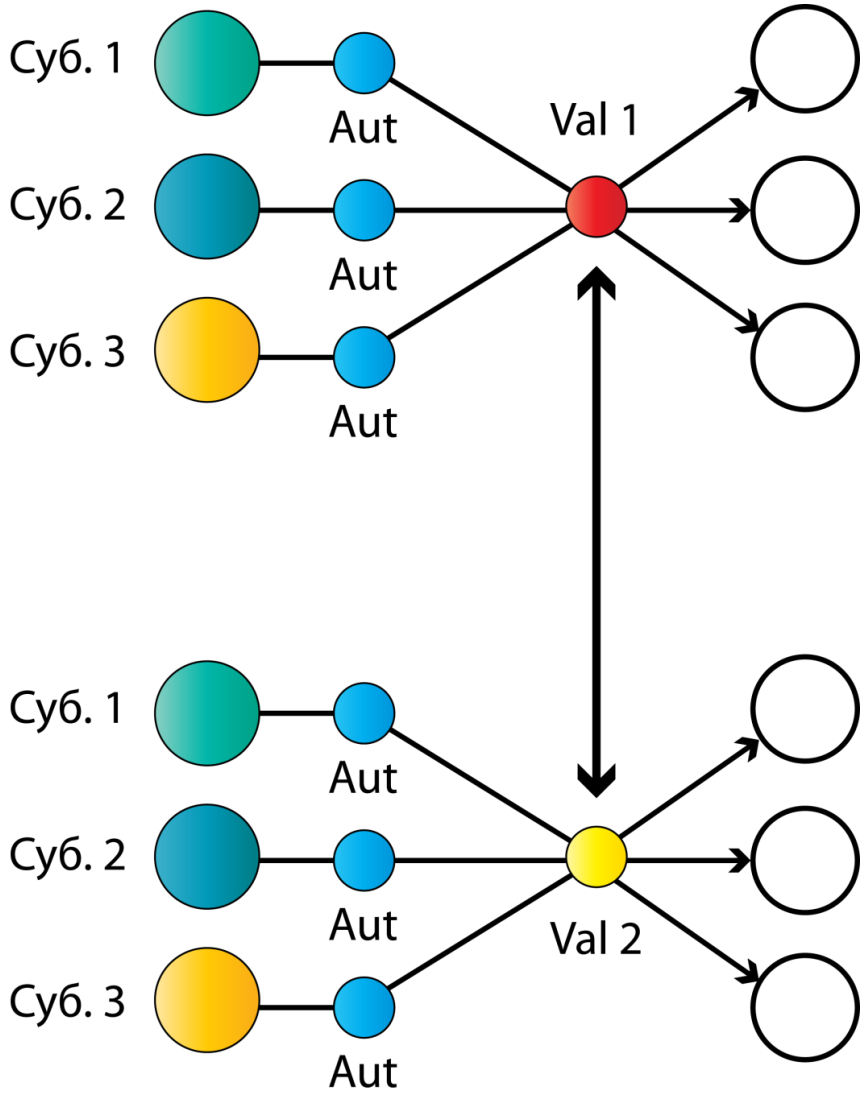
Система доверия



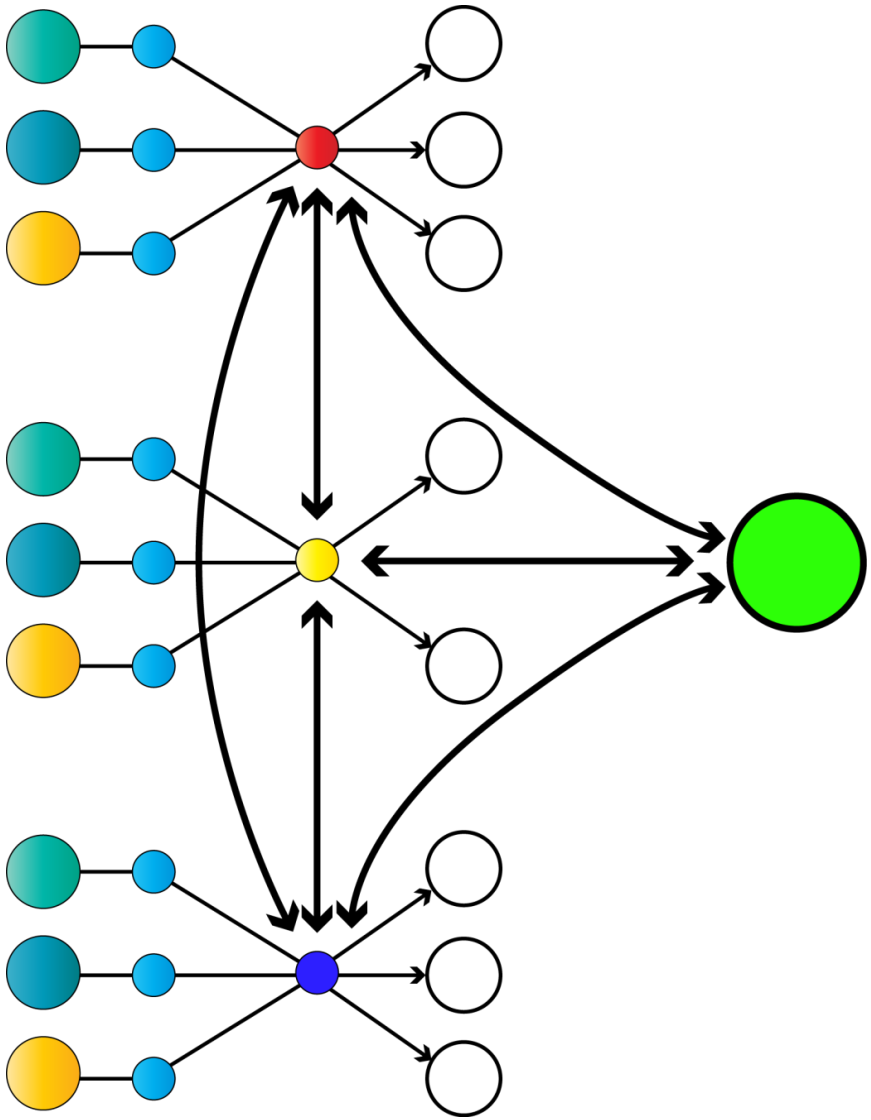
Домен доверия



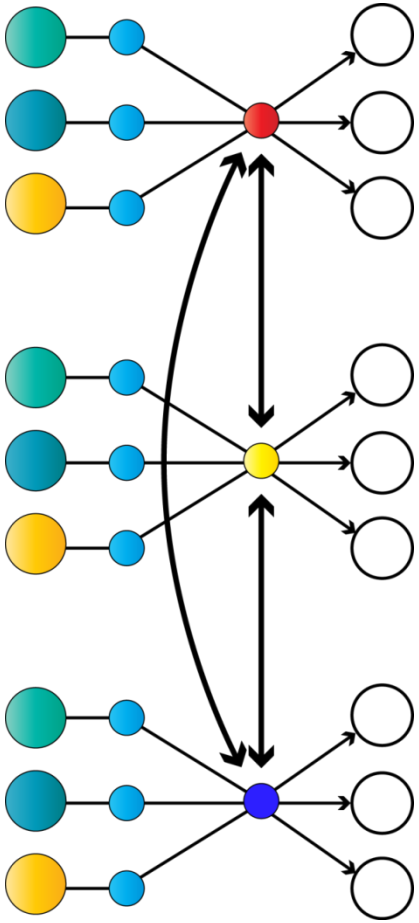
Пространство доверия AAA



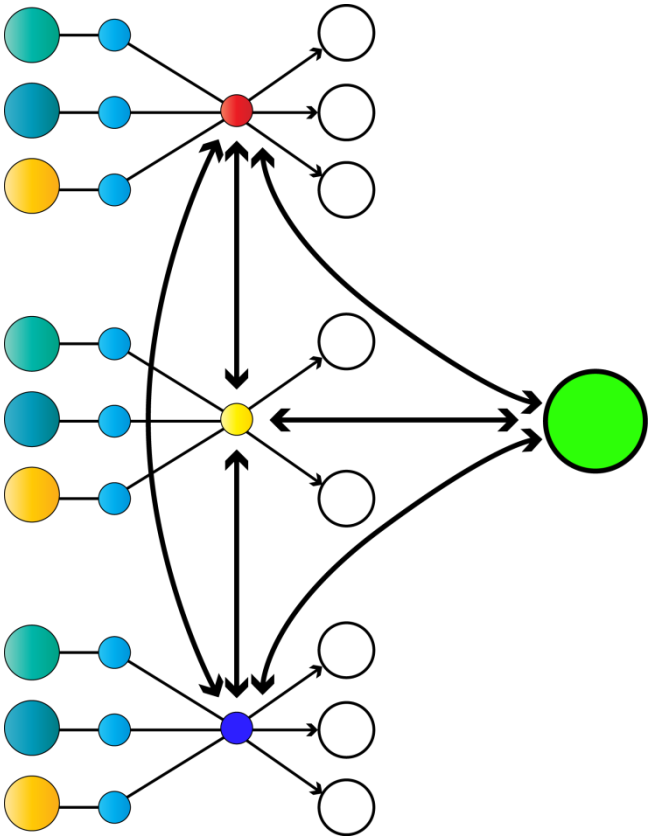
Мостовая схема



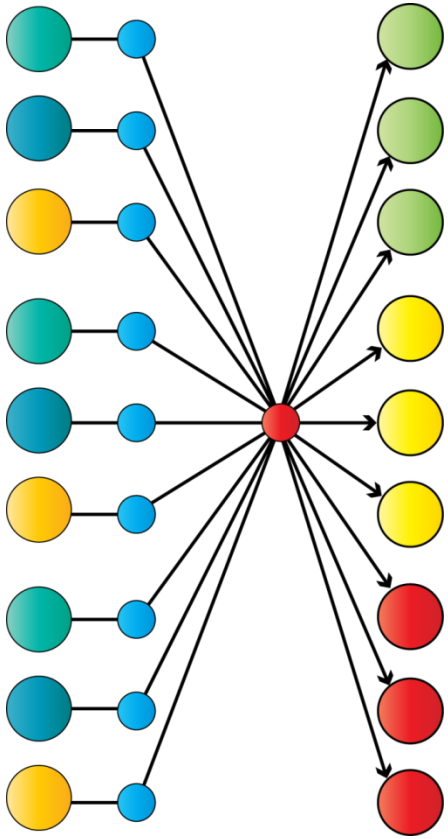
Модели формирования ЕПД ААА



распределенная (сетевая)

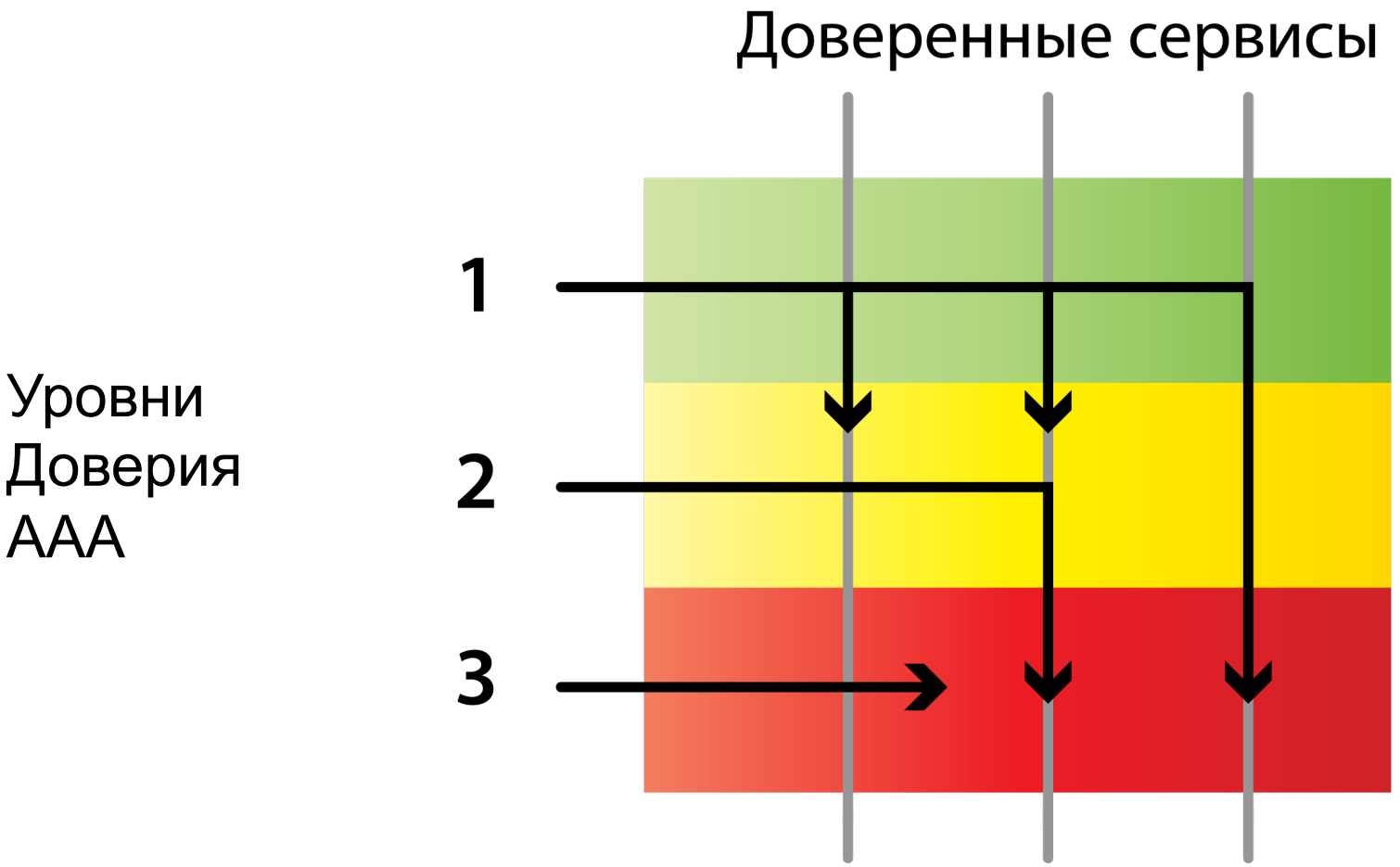


мостовая



централизованная

Уровни доверия ААА – часть ЕПД



Надежность аутентификации

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

Предварительные оценки

	процессы	Показатель надежности
1.	**Регистрация**	
1.1.	субъект ***предъявляет*** свои идентификаторы (удостоверения или электронные удостоверения -ЭУ)	нет данных
1.2.	Центр регистрации (ЦР) ***проверяет*** предъявленные субъектом идентификаторы	0,97 - 0,99
1.3.	ЦР ***создает*** учетную запись субъекта	0,97 - 0,999
1.4.	ЦР ***регистрирует/создает*** секрет (аутентификатор) и ***издает*** ЭУ	0,96 - 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	нет данных
2.	**Подтверждение подлинности**	
2.1.	Субъект ***хранит*** секрет и соответствующее ему ЭУ	0,537 - 0,999
2.2.	Субъект ***предъявляет*** секрет и ЭУ доверяющей стороне (ДС)	0,95 - 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

Краткий анализ потенциальных возможностей построения ЕПД

- Требования к усиленной квалифицированной подписи
  - Плюсы: наведен порядок с квалифицированной подписью
  - Минусы: нет требований к доверенным сервисам
- Аккредитация УЦ
  - Плюсы: начат процесс формирования ЕПД
  - Минусы: имеются только финансовые и организационные требования к УЦ, нет требований к регистрации, нет требований к доверенным сервисам, однако появилось понятие доверенного времени.
- Построение ЕСИА
  - Плюсы: один проектировщик и эксплуатант (хороший шанс создания ЕПД «от аутентификации»)
  - Минусы: нет регламентов и требований к доверенным сервисам
- Юридически-значимый ЭДО? Трансграничность?

Вместо заключения

- Европа: уже несколько лет существует понятие **Trusted CA** – доверенный УЦ. Достаточно одной доверенной функции. Например, корректность проверки СКП. Все аккредитованные УЦ – Trusted

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

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

Предложение в меморандум PKI-2012

- Объединить усилия федеральных органов государственной власти и заинтересованных коммерческих структур в целях выработки унифицированных политик, стандартов, регламентов и общих методик безопасного и эффективного информационного обмена, основанных на принципах формирования ЕПД.

- Разработать и предложить для широкого применения эталонные специализированные модули идентификации и установления идентичности для систем управления доступом при осуществлении онлайн взаимодействия через применение общих политик и подходов в действиях по пересечению организационных границ (доменов доверия) в едином информационном пространстве.

Аладдин РД

Сервис аутентификации в ЕПД должен быть доверенным!

Спасибо за внимание!

a.sabanov@aladdin-rd.ru