

Вторая международная конференция
«Стандартизация, сертификация, обеспечение
эффективности, качества и безопасности информационных
технологий»

ИТ-стандарт 2011

11 – 12 октября, МИРЭА
г. Москва, пр. Вернадского, д. 78

Инфраструктура открытых ключей (PKI) как технологическая среда трансграничного пространства доверия на основе сети Интернет



Общество с ограниченной ответственностью
«ГАЗИНФОРМСЕРВИС»

Кирюшкин Сергей
Анатольевич,
ООО «Газинформсервис»



МИНКОМСВЯЗЬ
РОССИИ

Домрачев Алексей Александрович,
Министерство связи и массовых
коммуникаций РФ

Документ как “штука”



Документ как “облако”



Характеристики документа

ГОСТ Р ИСО 15489-1-2007: в подразделе 7.2 определяет следующие характеристики важнейшего элемента информационного общества – документа:

«...»

7.2.2 Аутентичность

... Чтобы обеспечить аутентичность документов, организации должны внедрить и документально зафиксировать политику и процедуры контроля над созданием, получением, передачей, сохранением и отбором документов и тем самым гарантировать, что создатели документов уполномочены на это и идентифицированы, а документы защищены от несанкционированного дополнения, удаления, изменения, использования и сокрытия (засекречивания);

7.2.3 Достоверность

Достоверным является документ, содержание которого можно считать полным и точным представлением подтверждаемых операций, деятельности или фактов и которому можно доверять в последующих операциях или в последующей деятельности...

7.2.4 Целостность

Целостность документа определяется его полнотой и неизменностью. Необходимо чтобы документ был защищен от несанкционированного изменения...

7.2. Характеристики документа

- Аутентичность
- Целостность
- Достоверность

Как они обеспечиваются в традиционном документообороте?

Подпись,
Печать,
Правила

Как их обеспечить в электронном документообороте?

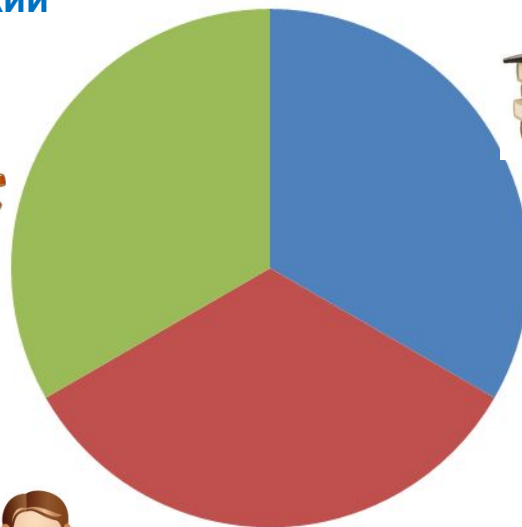
ЭЦП,
правила

Уровни решения задачи интероперабельности IT

Технологический



Юридический

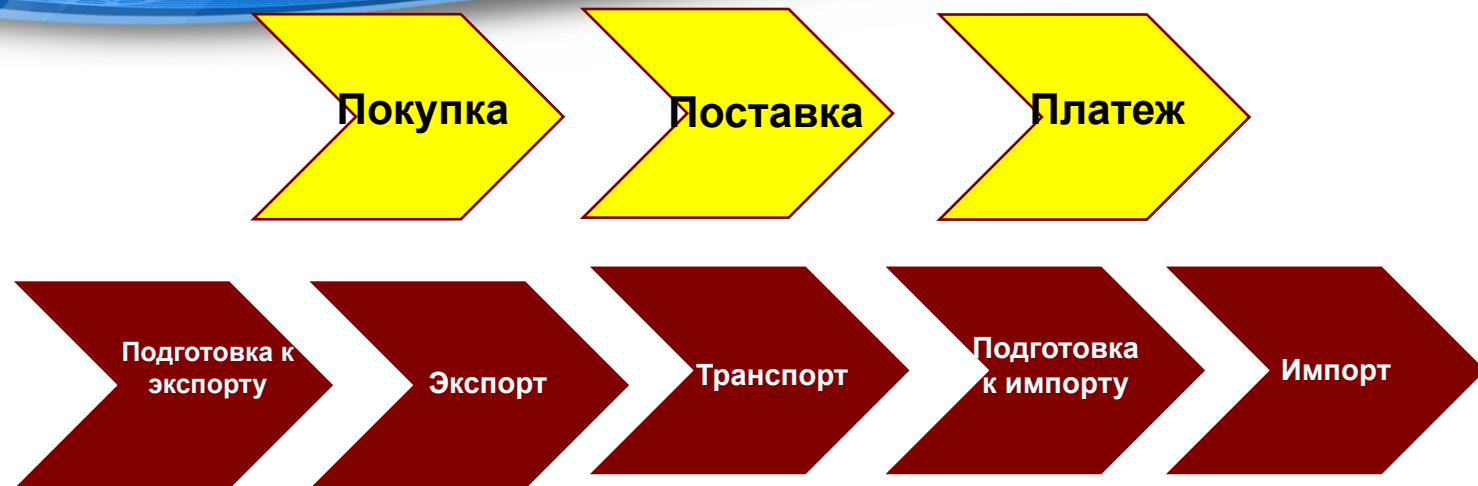


Организационный

Компоненты модели



Документы в логистической цепочке международной торговли в соответствии со стандартом UN/CEFACT



включает:

Информационно-маркетинговые процедуры:

- Реклама
- Анализ рынка
- Формирование спроса

Процедуры заключения договоров:

- Конкурсы
- Аукционы
- Согласование и заключение договоров

Контрольные операции на пунктах пропуска:

- Получение лицензии на импорт/экспорт
- Предоставление таможенных и грузовых деклараций

Банковские и страховые операции:

- Предоставление кредитного рейтинга
- Обеспечение страховки
- Предоставление кредита
- Оплата

**Инфраструктура информационного доверия
и информационной безопасности**

PKI как базовая инфраструктура

ДТС

Инфраструктура открытых ключей

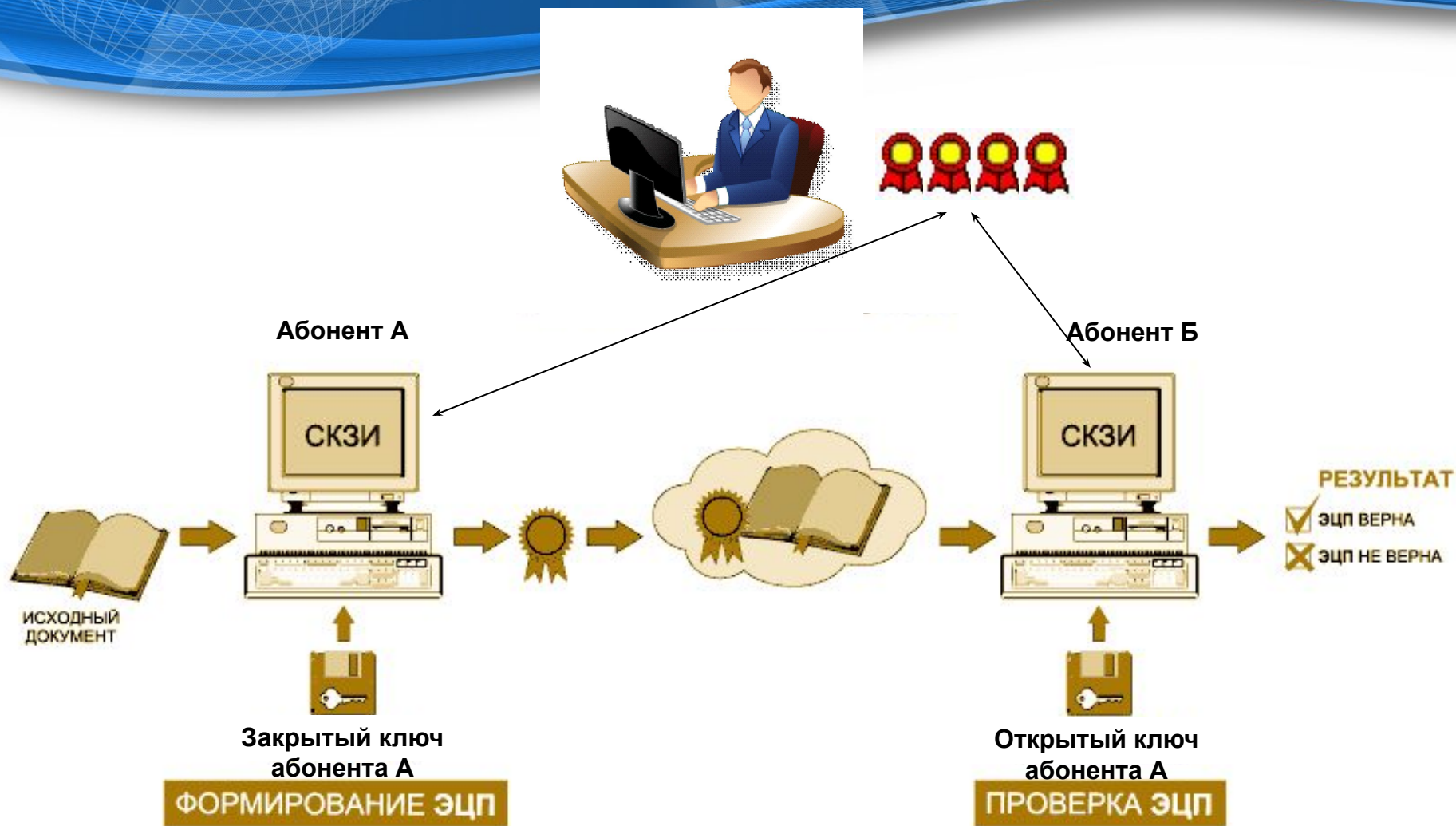


Web 2.0

**Инфраструктура
информационного доверия и
безопасности**

Web 3.0

УЦ как специализированная доверенная третья сторона (ДТС, ТТР)

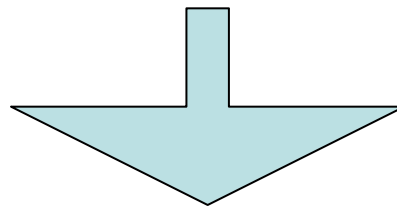


Сервисы доверенной третьей стороны

X.842 Сервисы доверенной третьей стороны

↳ **X.509** Инфраструктура сертификатов открытых ключей и атрибутивных сертификатов

↳ **ФЗ-1,** Применение РКІ только в интересах
ФЗ-63 обеспечения механизмов ЭЦП



Наиболее распространенные сервисы - для задач ЭЦП



X.842

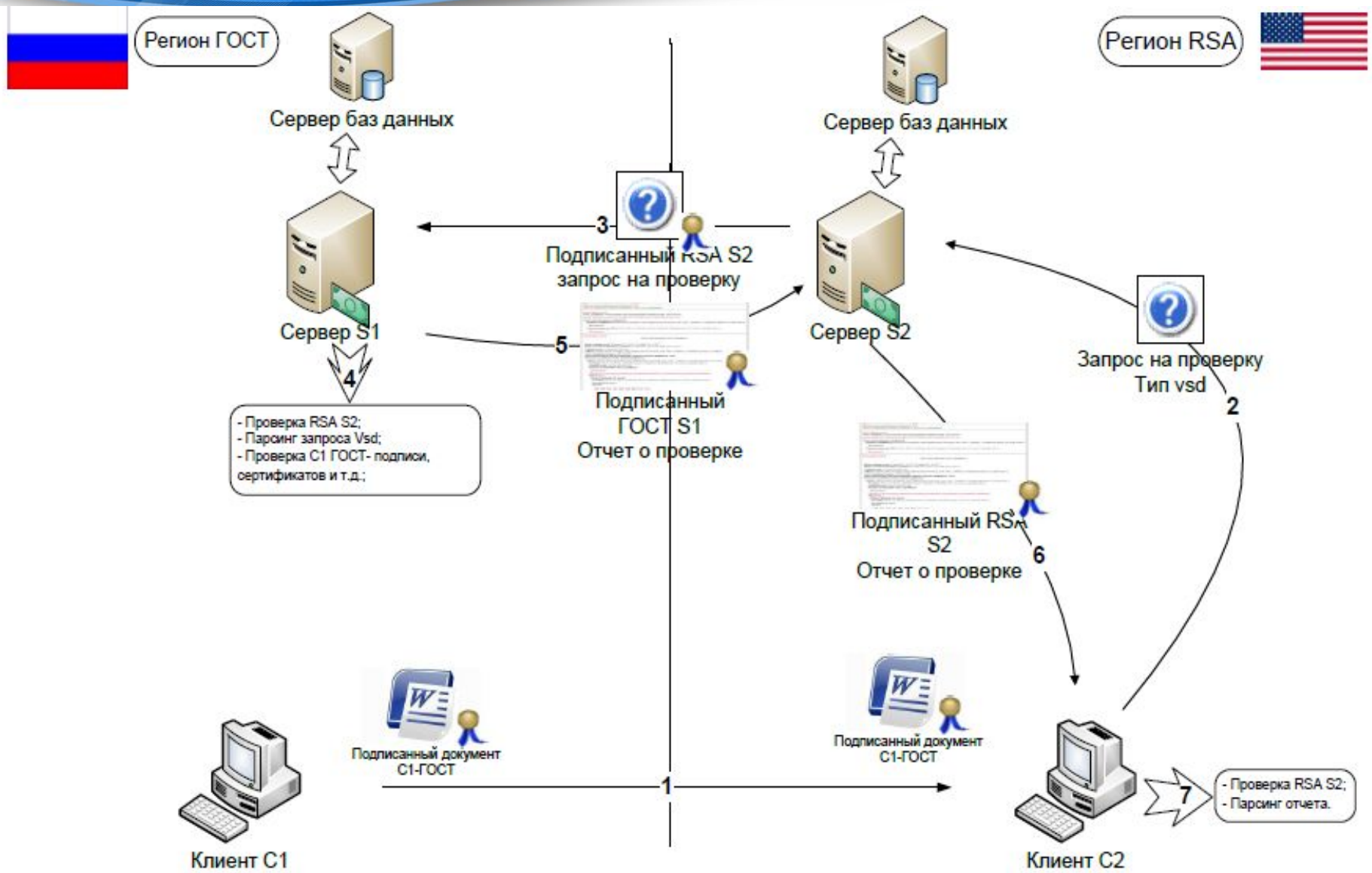
7.3	Key Management Services	16
7.3.1	Key Generation Service	16
7.3.2	Key Registration Service	16
7.3.3	Key Certification Service	16
7.3.4	Key Distribution Service	17
7.3.5	Key Installation Service	17
7.3.6	Key Storage Service	17
7.3.7	Key Derivation Service	17
7.3.8	Key Archiving Service	17

ITU-T Rec. X.842 (10/2000) (E)

iii

		<i>Page</i>
	7.3.9 Key Revocation Service	17
	7.3.10 Key Destruction Service	17
7.4	Certificate Management Services	18
	7.4.1 Public Key Certificate Service	18
	7.4.2 Privilege Attribute Service	18
	7.4.3 On-line Authentication Service Based on Certificates	19
	7.4.4 Revocation of Certificates Service	19

Трансграничная интероперабельность PKI на основе сервисов ДТС (DVCS, VA)



Сервисы документирования на базе ДТС

- Сервис подписи



- Сервис времени



- Сервис местоположения



- Нотариальный сервис



- Сервис апостилирования



- Сервис обеспечения платежей



- Мониторинг правовых статусов субъектов

- Сервис доверенного хранения данных



- Сервис печати с сохранением характеристик электронных документов



- Сервис регистрации и учета

Вывод

- РКИ – эффективная технологическая среда для реализации трансграничного пространства доверия как составной части единого информационного пространства таможенного союза

Вторая международная конференция
«Стандартизация, сертификация, обеспечение
эффективности, качества и безопасности информационных
технологий»

ИТ-стандарт 2011

11 – 12 октября, МИРЭА
г. Москва, пр. Вернадского, д. 78

Спасибо за внимание!



Общество с ограниченной ответственностью
«ГАЗИНФОРМСЕРВИС»

**Кирюшкин Сергей
Анатольевич,**
ООО «Газинформсервис»



МИНКОМСВЯЗЬ
РОССИИ

Домрачев Алексей Александрович,
Министерство связи и массовых
коммуникаций РФ