

Методология формирования и функционирования в сети Интернет трансграничного пространства доверия. Опыт разработки и внедрения службы валидации (проверки подлинности, VA) как сервиса доверенной третьей стороны

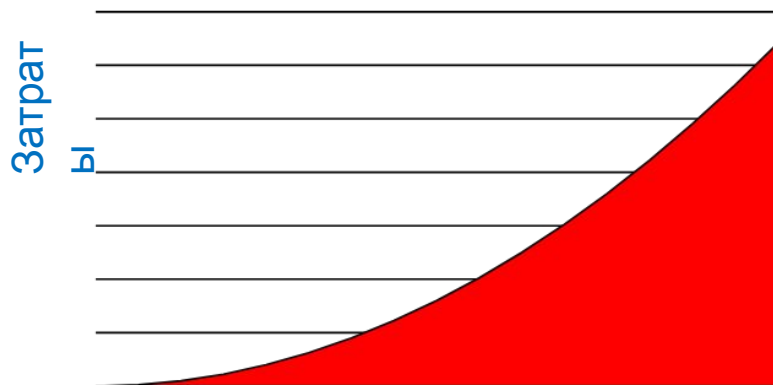
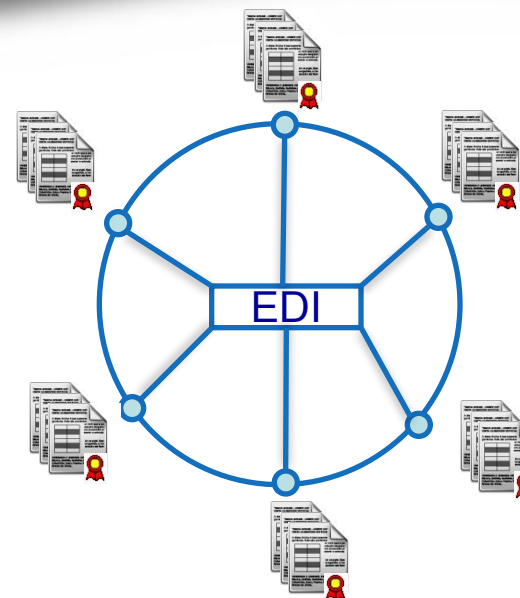
*д.т.н., профессор Кустов В.Н., генеральный директор
ООО «Удостоверяющий центр Газинформсервис»
к.т.н. Кирюшкин С.А., советник генерального директора
ООО «Газинформсервис»*

Рассматриваемые вопросы

1. Служба валидации (проверки подлинности, Validation Authority, VA) как эффективная модель многодоменного доверия инфраструктуры открытых ключей
2. Опыт разработки и внедрения службы валидации в прикладные системы: вопросы эффективности эксплуатации сервиса и пользовательской эргономики
3. Опыт применения службы валидации (проверки подлинности) в ШОС



1.1. Актуальность вопроса создания инфраструктуры ИТ-доверия для ШОС



Количество документов



Количество документов

PKI как базовая инфраструктура

ДТС

Инфраструктура открытых ключей



1.2. Почему иные модели доверия не подходят для реализации ТИВ?

- 1. Проблемы с различиями в стандартах используемых криптографических средств (КС).**
- 2. Проблемы с ввозом-вывозом КС.**
- 3. Проблемы с обслуживанием КС.**

1.3. Достоинства модели, основанной на сервисе валидации

- 1. Возможность использования несовместимых КС.**
- 2. Возможность получения юридически-значимого результата процедуры установления доверия.**
- 3. Возможность получения юридически-значимого результата процедуры проверки подписи.**

1.3. Достоинства модели, основанной на сервисе валидации

Классификация популярных моделей доверия

Таблица 1.

<i>Характеристика</i>	<i>Возможность использования несовместимых криптографий</i>	<i>Возможность получения юридически-значимого результата процедуры установления доверия к сертификату</i>	<i>Возможность получения юридически-значимого результата процедуры проверки подписи в режиме онлайн (без обращения в УЦ)</i>
<i>Модель Доверия</i>			
Иерархическая	Нет	Да (OCSP-ответ)	Нет
Браузерная	Нет	Да (OCSP-ответ)	Нет
Сетевая	Нет	Да (OCSP-ответ)	Нет
Мостовая	Нет	Да (OCSP-ответ)	Нет
На основе валидации	Да	Да (vpkc-ответ)	Да (VSD-ответ)

1.3. Достоинства модели, основанной на сервисе валидации

Классификация популярных моделей доверия

Таблица 2.

<i>Характеристика</i>	<i>Возможность использования несовместимых криптографий</i>	<i>Возможность получения юридически-значимого результата процедуры установления доверия к сертификату</i>	<i>Возможность получения юридически-значимого результата процедуры проверки подписи в режиме онлайн (без обращения в УЦ)</i>
Модель Доверия			
Иерархическая	Нет	Нет	Нет
Браузерная	Нет	Нет	Нет
Сетевая	Нет	Нет	Нет
Мостовая	Нет	Нет	Нет
На основе валидации	Да	Да (vpkc-ответ)	Да (VSD-ответ)

2.1. Чем определяются требования, и где они сформулированы?

1. Определена политика безопасности.
2. Корректное использование технических и организационных мер.
3. Корректное выполнение всех операций.
4. Определены интерфейсы и процедуры взаимодействия с пользователями.
5. Определены правила и нормативы для безопасного уровня доверия.
6. Качество процедур, операций и технологий соответствует требованиям.
7. ДТС исполняет свои договорные обязательства они понятны и применимы.
8. Обеспечен контроль соответствия законодательству и регламентам.
9. Известные угрозы и меры безопасности четко идентифицированы.
10. Оценивание угроз и рисков проведено.
11. Организационно-штатные требования и требования к персоналу соблюдаются.
12. Уровень доверия к ДТС контролируется.
13. Деятельность ДТС контролируется уполномоченным органом

2. 2. Как требования к операторам ДТС коррелируют с требованиями к УЦ?

X.842 - ТТР

X.843 - CSP

Закон об ЭЦП

X.509 - PKI

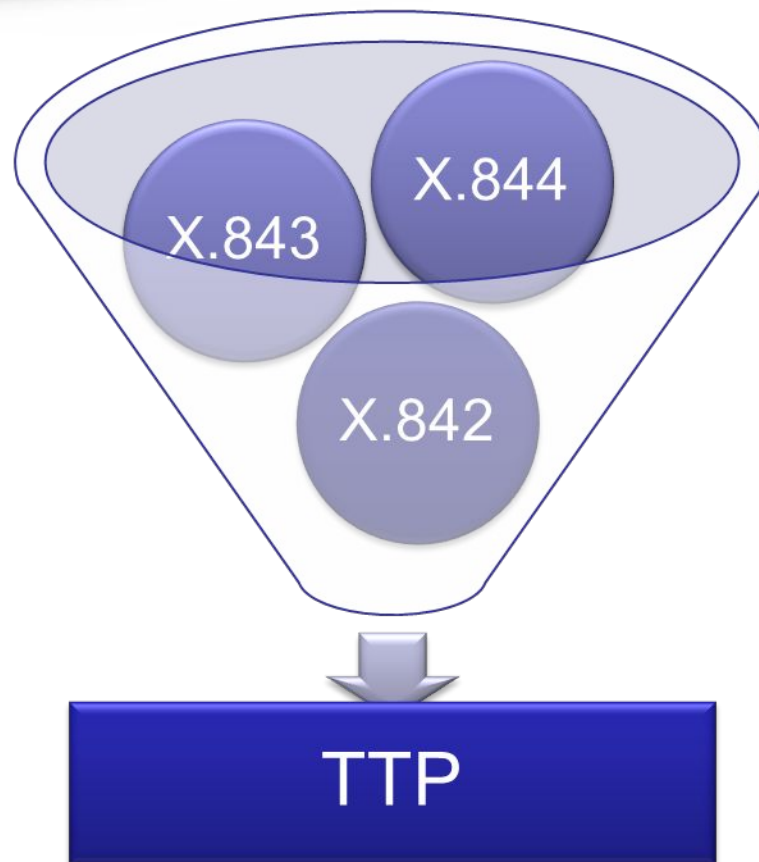
**WebTrust Program
for Certification Authorities**

2.2. Как требования к операторам ДТС коррелируют с требованиями к УЦ?



Инициатива Web 3.0

2. 2. Как требования к операторам ДТС коррелируют с требованиями к УЦ?



2.3. Опыт согласования с заказчиком эргономических характеристик сервиса валидации

- 1. Прозрачность и обоснованность правовой модели.**
- 2. Прозрачность пользовательского режима сервиса валидации.**
- 3. Получение услуги сервиса валидации там, где удобно пользователю.**
- 4. При необходимости, услуги получения иностранного КС должна обеспечивать ДТС.**

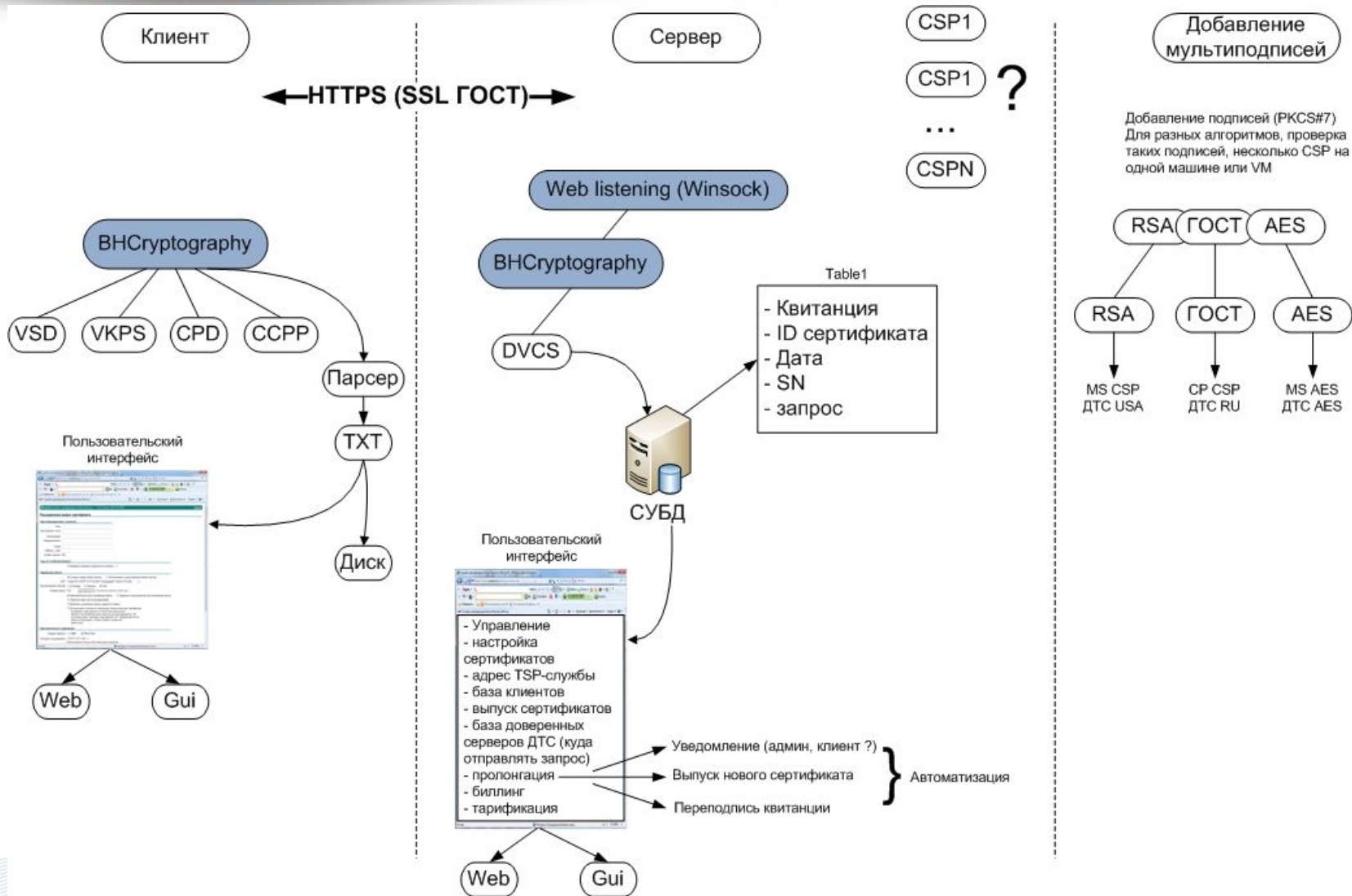
2. 4. Востребованность сервиса валидации для задач трансграничной электронной торговли

- 1. Государственные закупки в РФ.**
- 2. Проект Европейской комиссии PERPOL.**
- 3. Государство - самый крупный заказчик в системе
электронной торговли.**
- 4. Опыт взаимодействия УЦ ООО
«Газинформсервис» с компанией Unizetto
Technologies.**

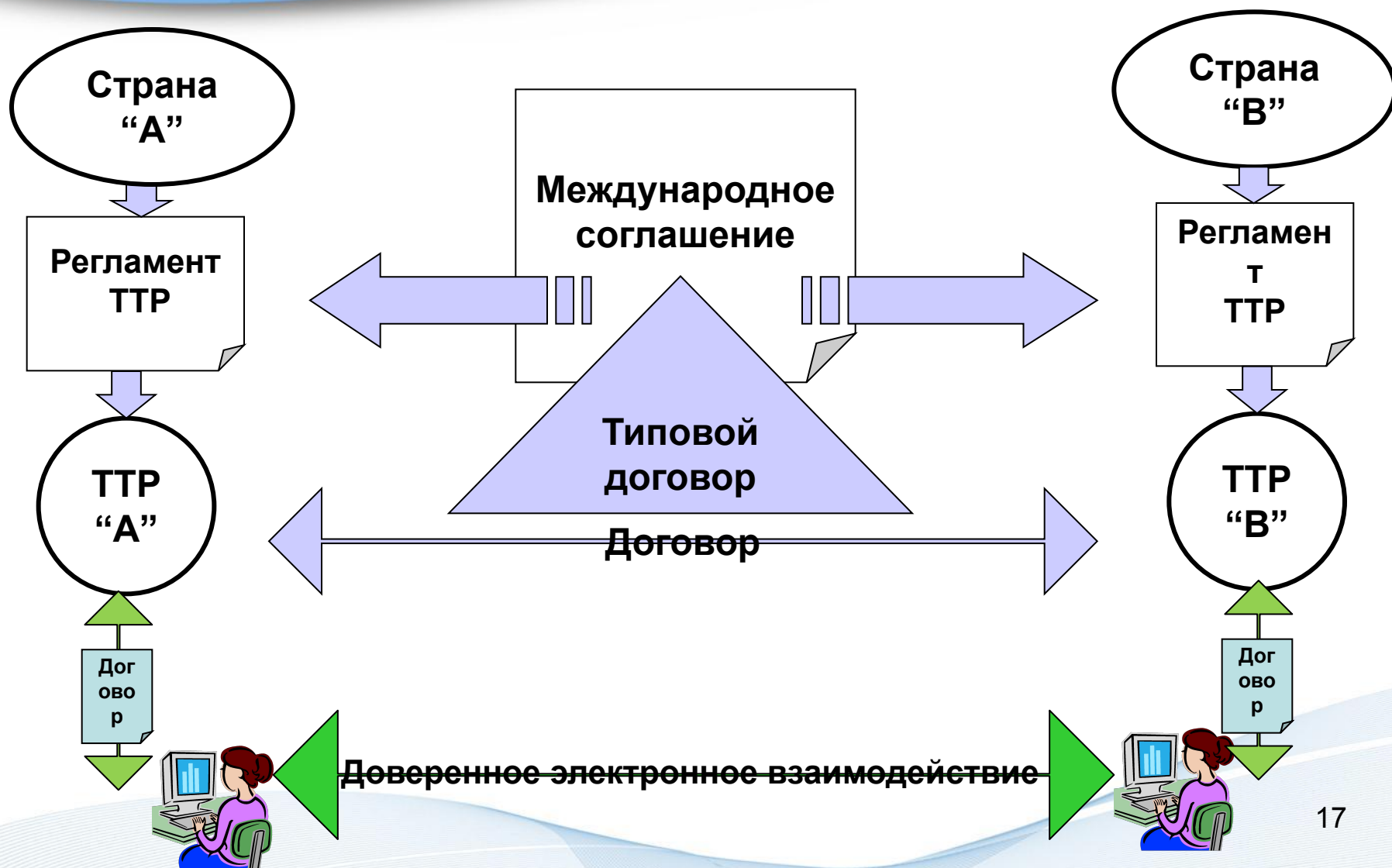
2.5. Что мы можем предложить?

- сервис трансляции защищенной информации в канале, позволяющий обеспечить конфиденциальный документооборот с использованием различных криптографических алгоритмов;
- сервис подтверждения подлинности на основе международных рекомендаций RFC 3029, позволяющий обеспечить аутентичность и целостность электронных документов, созданных и подписанных в электронном в соответствии с правилами иностранного государства.

2.5. Что мы можем предложить?

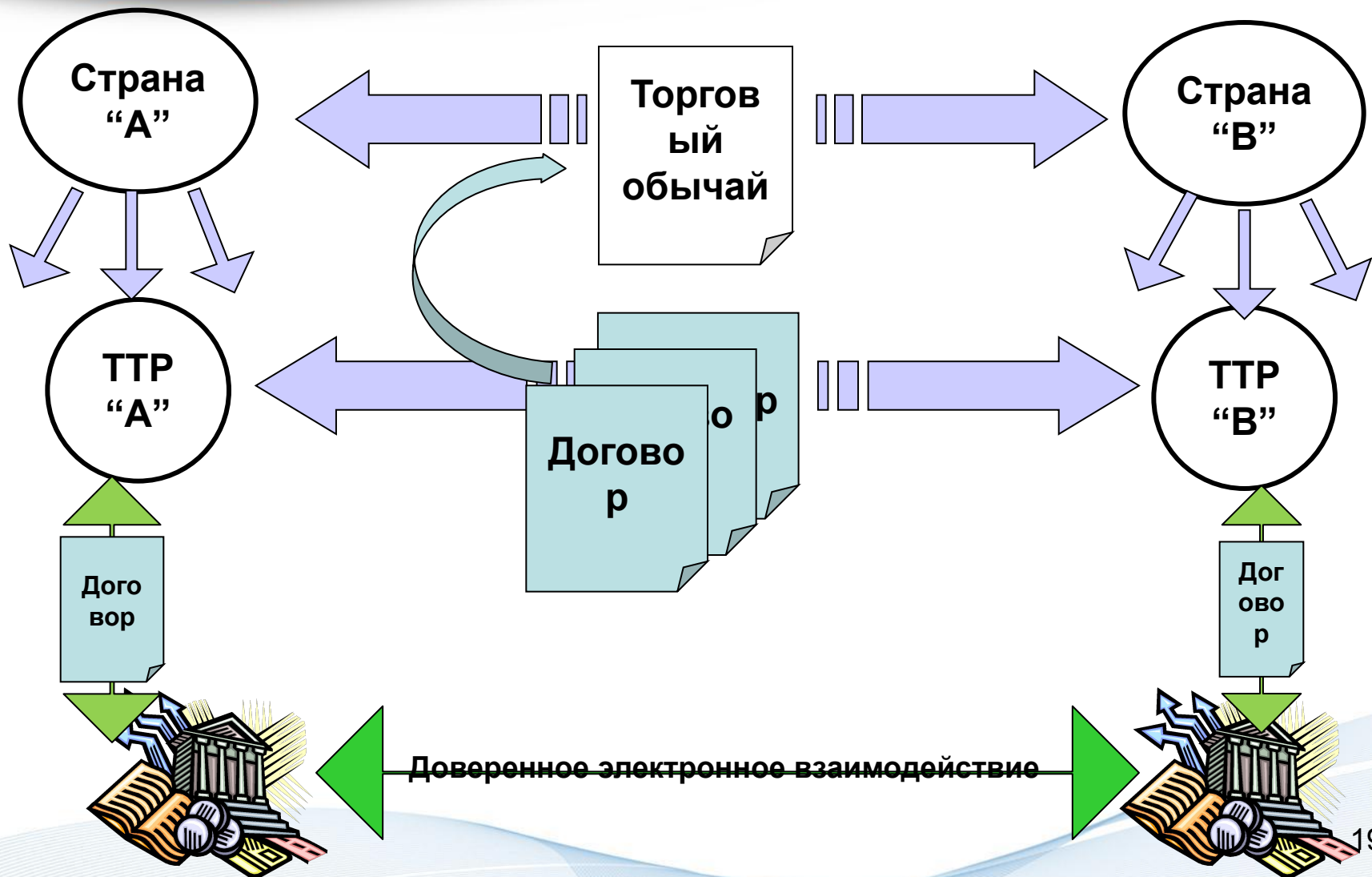


3.1. О проекте ЭЦП-ШОС

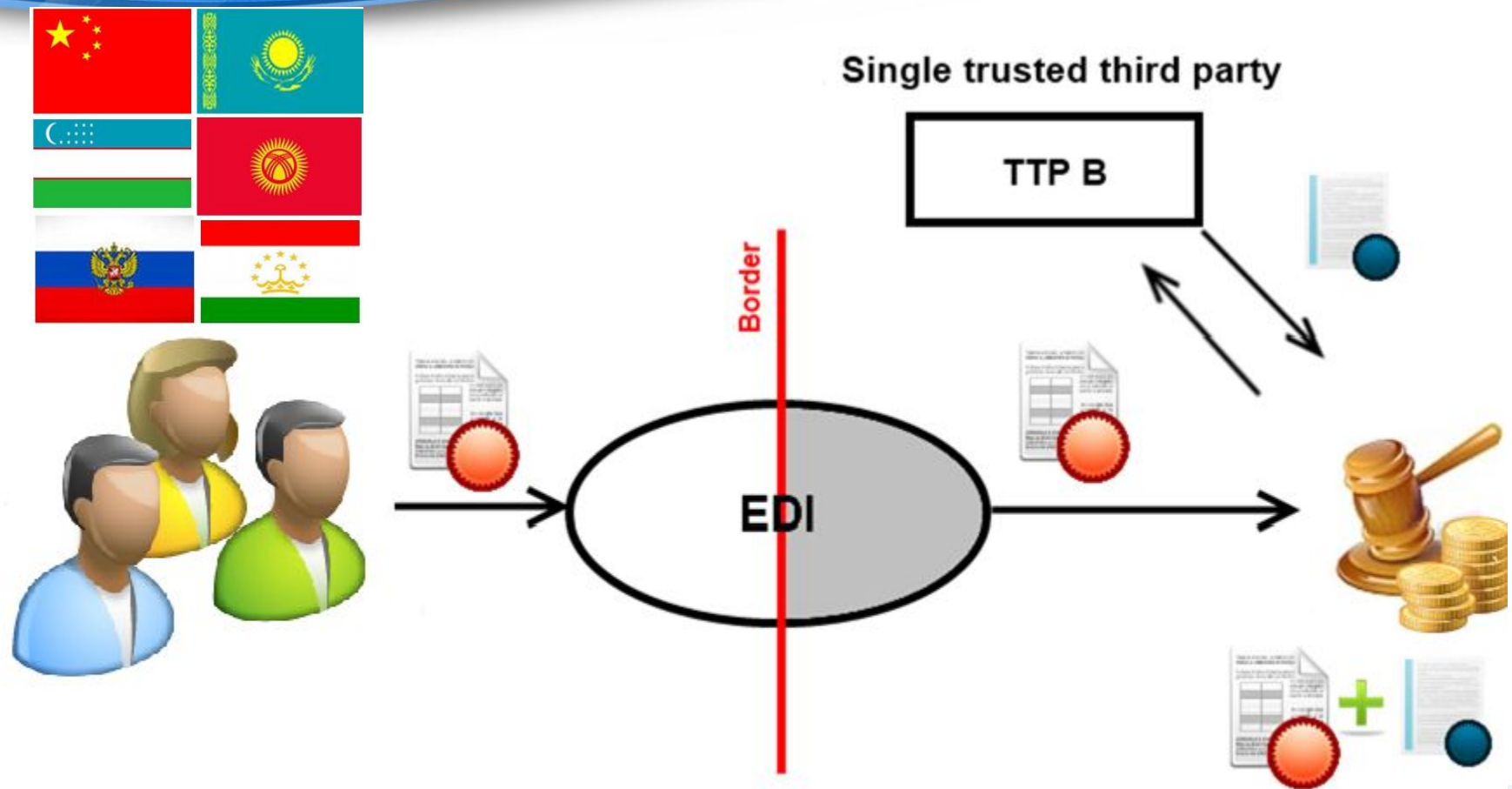


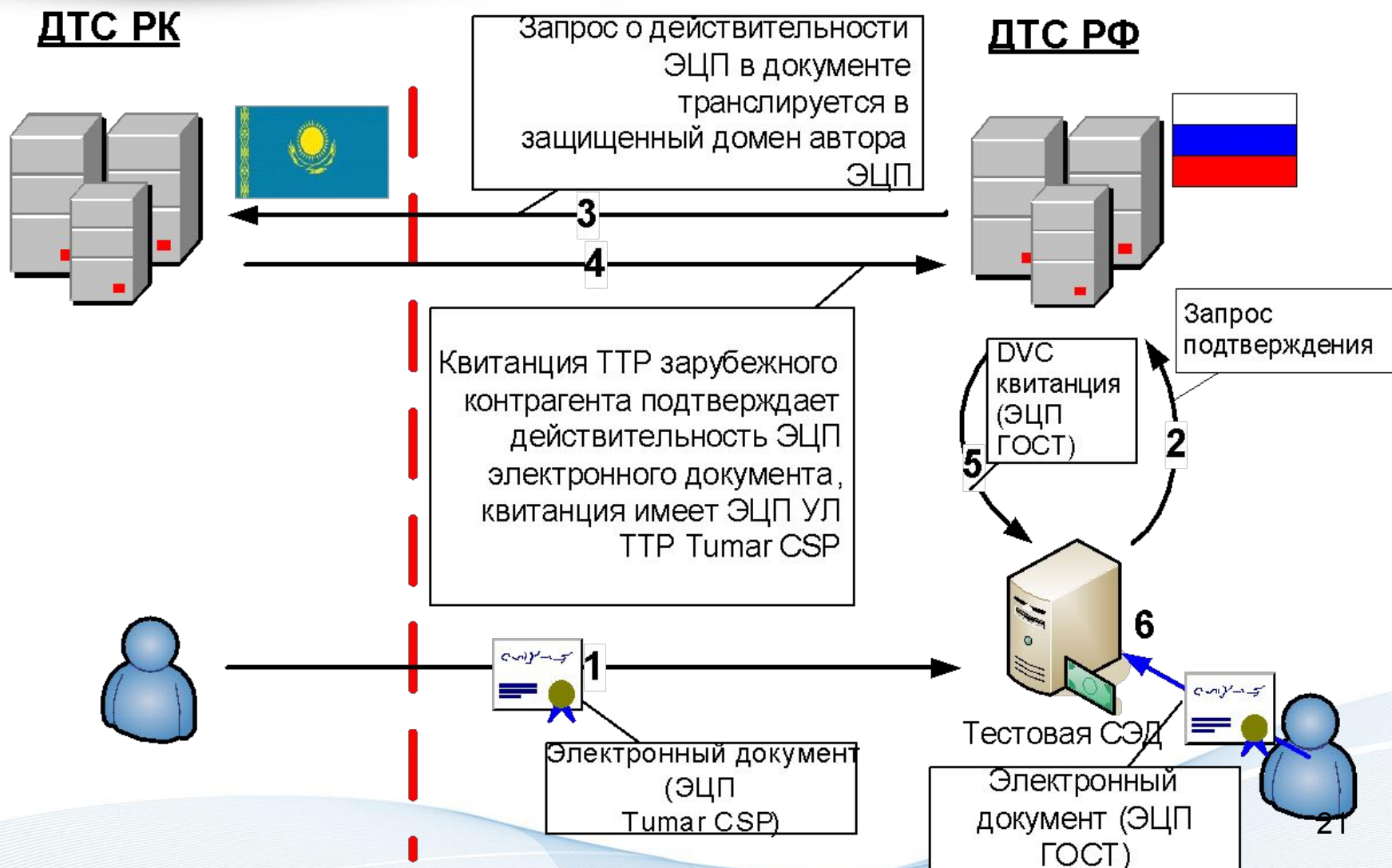
- **Электронная торговля**
- **Государственные закупки**
- **Системы дистанционного образования**
- **Телемедицинские проекты**
- **Процедуры таможенного контроля на границе**

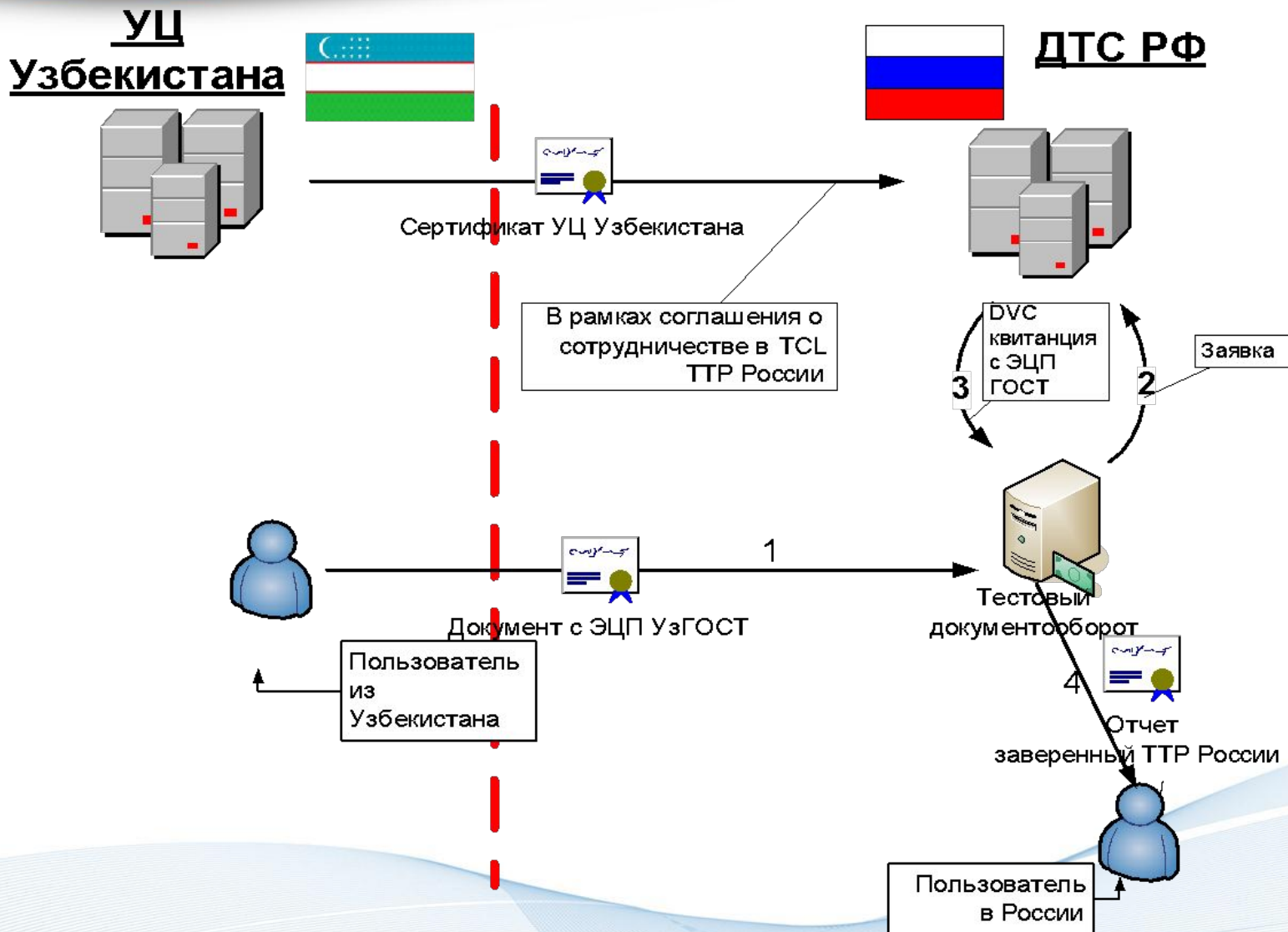
3.1. О проекте ЭЦП-ШОС

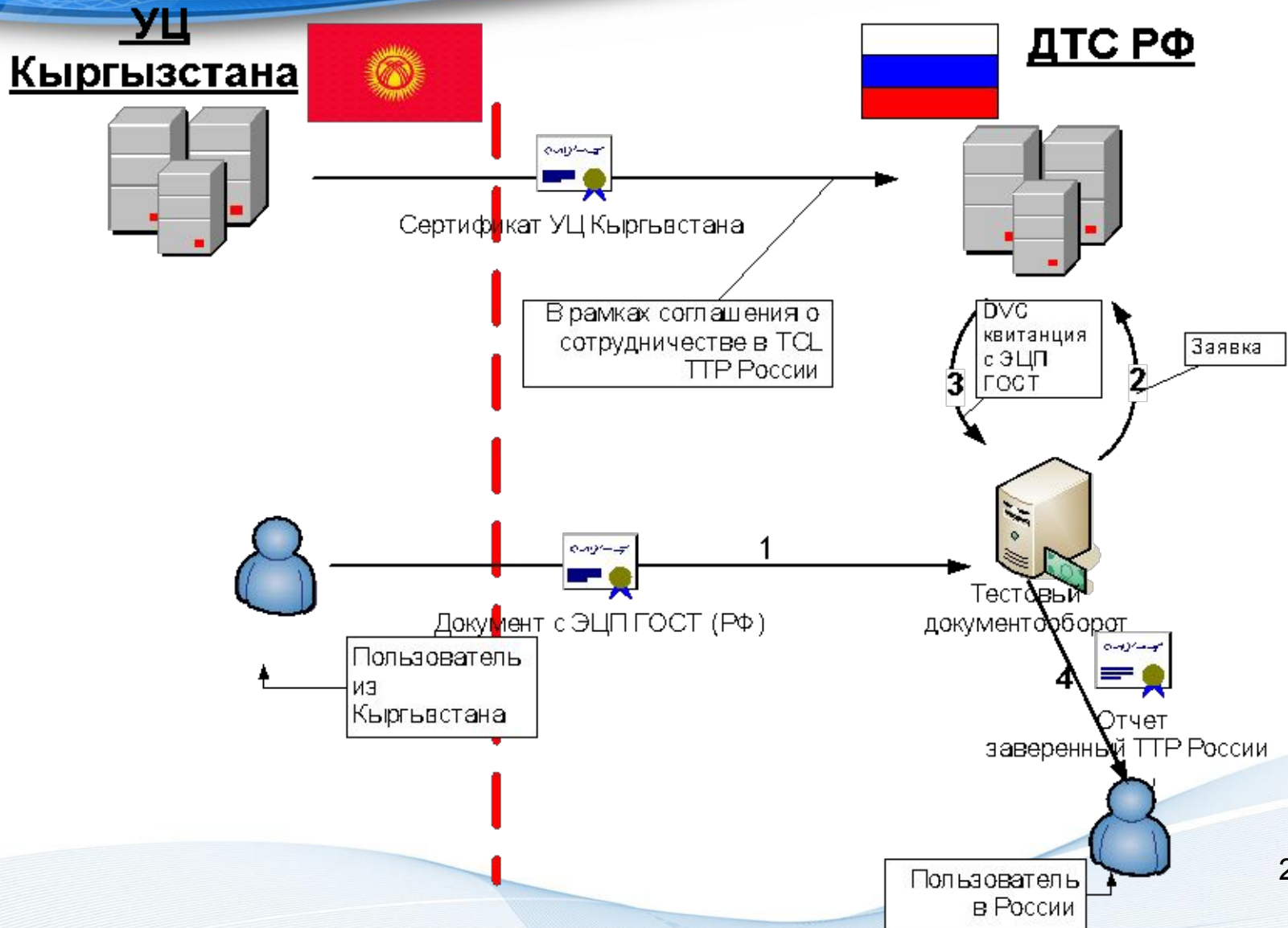


3.2. Об опыте двустороннего взаимодействия со странами-членами ШОС



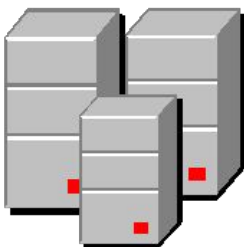






Предложение по испытаниям на основе электронной торговой площадки ШОС

ДТС СТРАНЫ ШОС

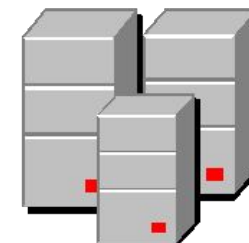


Запрос о действительности ЭЦП в ofercie транслируется в защищенный домен автора ЭЦП

3

4

ДТС СТРАНЫ ШОС



*TTP – *Trusted Third Party* (Третья Доверенная Сторона), рекомендации ITU X.842, X.843

Квитанция TTP зарубежного контрагента подтверждает действительность ЭЦП электронной oferty, квитанция имеет ЭЦП УЛ TTP Tumar CSP

Запрос подтверждения

DVC
квитанция
(ЭЦП
ГОСТ)

Принятие иностранной oferty к рассмотрению



1
Электронная oferta (Tumar CSP)



ЭТП ШОС

6
Электронная oferta (ЭЦП ГОСТ)



Спасибо за внимание!

Вопросы?

д.т.н., профессор Кустов В.Н., генеральный директор ООО «Удостоверяющий центр Газинформсервис»

к.т.н. Кирюшкин С.А., советник генерального директора ООО «Газинформсервис»