

Вопросы практической реализации обмена документами и иной информацией в электронном виде в трансграничном режиме (Технические средства ДТС)

Любая деловая активность для любых видов отношений С, В или G предполагает обмен документами, информацией между участниками бизнес-процесса.

Отдельного внимания требует реализация такого обмена документами – информацией в электронном виде и тем более в трансграничном режиме.

Далее требуется обеспечить требования к **качеству** самого ЭД, т.е. информации подлежащей обмену в соответствии с ГОСТ Р ИСО 15489-1-2007 :

1.1. целостность и авторство – именно на этих требованиях далее и остановимся подробнее

1.2. Достоверность/актуальность - пригодность для последующего использования

1.3... и т.п. в соответствии со Стандартом.

Целостность и авторство информации

Обычно данная задача решается с использованием Электронной Подписи (ЭП) / Электронной Цифровой Подписи (ЭЦП).

Однако при трансграничном обмене требуется ещё и **обеспечение правовых последствий ЭП/ЭЦП для разных правовых систем** участников обмена с учётом:

- технических требований локального законодательства в части использования легитимных криптографических алгоритмов и средств;
- локальных требований к лицензированию видов деятельности, связанных с криптографическими услугами;
- сертификации технических средств;
- экспортных ограничений на технические средства;
- и т.п.

Признание иностранного сертификата и ЭП/ЭЦП

Следует концентрироваться **НЕ на решении задачи признания** зарубежных сертификатов в правовом поле той или иной страны (поскольку нет возможности находясь в одном правовом поле квалифицированно заключить, что сертификат был выдан с полным соблюдением нормативных требований другого правового поля, если специально не изучать этот вопрос), а на **задаче обеспечения доступности услуги** по проверке действительности и сертификата и ЭП/ЭЦП зарубежного автора.

Обычно данная услуга оказывается в рамках доверенных сервисов в соответствии с международными рекомендациями ИТУ-Т серия X.842, объединяемых термином «Доверенная Третья Сторона» (ДТС).

Смысл равноправного информационного обмена сводится к следующим утверждениям:

- ✓ Автор ЭП/ЭЦП вырабатывает ЭП/ЭЦП легитимным способом для своего правового поля, включая и использование криптографических средств, алгоритмов, принятых в качестве национальных стандартов.
- ✓ Проверка ЭП/ЭЦП осуществляется в правовой зоне автора ЭП/ЭЦП (только там может быть определена степень «законности» использования ЭП/ЭЦП). Результат - электронный документ (квитанция), содержащий: время проверки, статус проверки, доказательную базу и ЭП/ЭЦП ДТС.
- ✓ Пользователь «доверяет» только ДТС своей зоны (домена).

Почему РТО занималось изучением всех этих вопросов?

В рамках распределения функций по подготовке к созданию условий для разворачивания ДТС РФ, за РТО была закреплена – техническая поддержка ДТС на инфраструктурном уровне и тестирование с сопредельными ДТС.

Что было оформлено **Письмами МКС №НМ-П13-632(631) от 7.02.2011** в сторону Республик Беларусь и Казахстан.

Строго в рамках обозначенного круга задач в последующие годы РТО и работало, выполняя тестирование с иностранными ДТС и апробацию технологии ДТС на реальных бизнес-процессах.

Несколько слов о принципах классификации состава и функциональности технических средств ДТС

Из опыта практической работы можно рассматривать классификации по:

1. Видам отношений С, В или G. Такая классификация слабо влияет (если точнее, то никак не влияет) на состав и конфигурацию технических средств ДТС.
2. По точке размещения ДТС в информационных потоках данных (In-line, Off-line или On-line (см. X.842)) – незначительное влияние на конфигурацию технических средств ДТС.
3. Наиболее сильное влияние на состав и конфигурацию технических средств ДТС оказывает степень взаимосвязи независимых доменов сторон обмена и разумеется сама специфика трансграничных бизнес-процессов:
 - **Слабая**, на уровне Соглашения сторон ...
 - **Сильная**, помимо законодательных применяются и специальные технические инструменты.

Классификация ДТС по видам распространения/получения квитанций, вытекающая из особенностей обслуживаемых бизнес-процессов для слабосвязанных доменов

Различают:

- Режим **PUSH** (передача).
- Режим **PULL** (запрос).
- Режим **Bridge** (мост).

Важное замечание:

В общем виде для проверки ЭЦП требуется предоставить в ДТС сам ЭД. Для ряда бизнес-процессов такая доставка ЭД в стороннюю подсистему может быть сопряжена с риском компрометации самого контента ЭД, особенно для документов с ограничивающими грифами и может быть просто превентивно запрещена на уровне национального НПА. На практике данную проблему решают через использование **отсоединённых подписей**, что выдвигает для ДТС требование по возможности проверки как присоединённых, так и отсоединённых подписей.

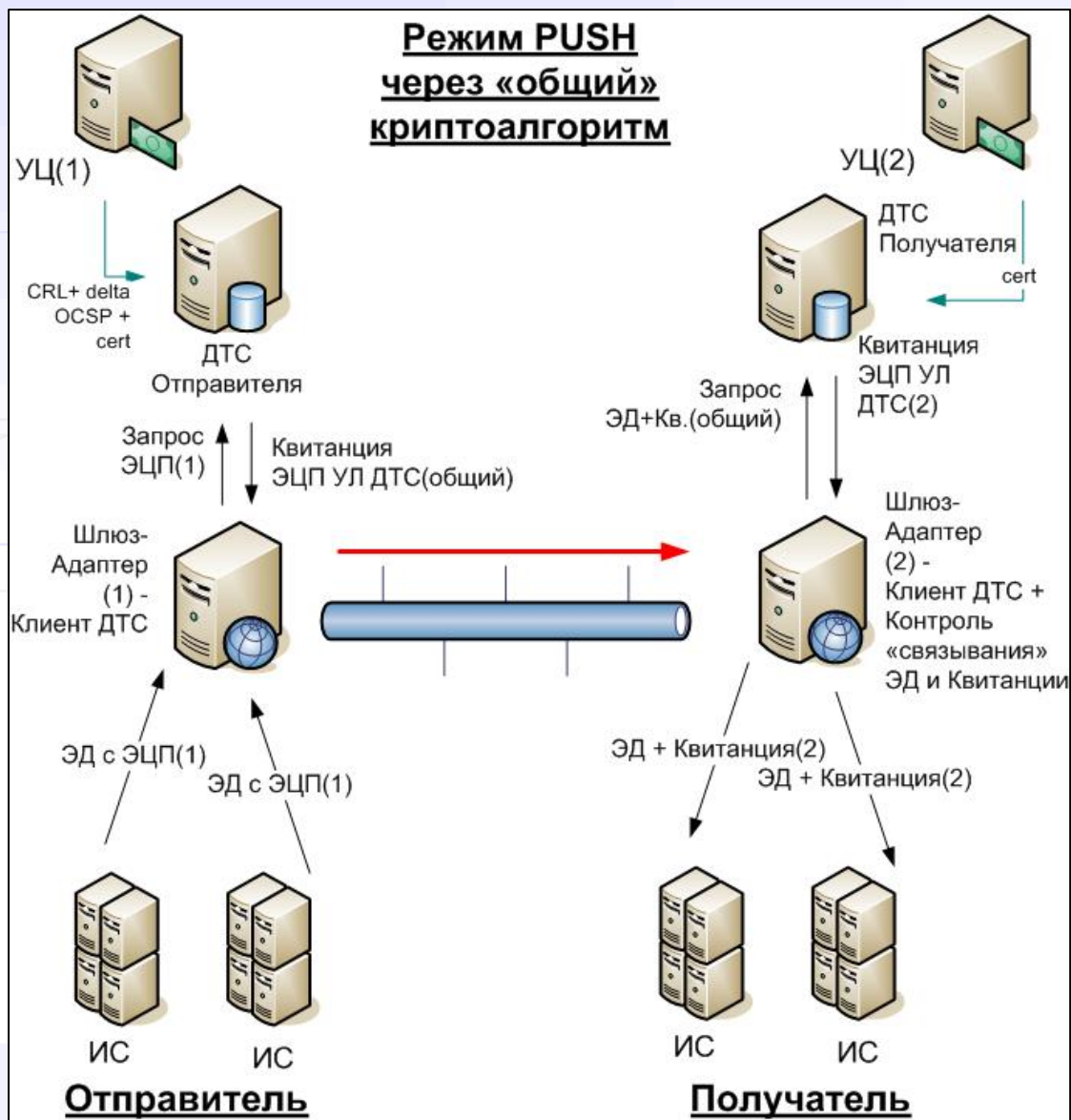
Особенности выбора криптоалгоритмов при трансграничном обмене в слабосвязанных доменах

С учетом изначально неопределённого числа взаимодействующих доменов, для организации доверия квитанциям по проверке ЭЦП может строиться:

1. через "общий алгоритм" (со стойкостью не ниже стойкости алгоритмов сторон).
2. по принципу "двух телефонов".

Разные бизнес процессы могут потребовать поддержку различных режимов из чего следует, что ДТС должна уметь одновременно работать с несколькими различными СКЗИ и этот перечень не должен быть фиксированным и может только расширяться.

Схема взаимодействия при PUSH



Режим PUSH (X.842 п. 4.2.3 Off-line TTP Services).

Данный режим взаимодействия функционально аналогичных ДТС различных доменов такой, при котором квитанция о проверке ЭЦП отправителя предварительно и заранее (до начала самой передачи электронного документа) подготавливается в ДТС отправителя и пересылается принимающей стороне вместе с самим электронным сообщением.

Схема взаимодействия при PUSH

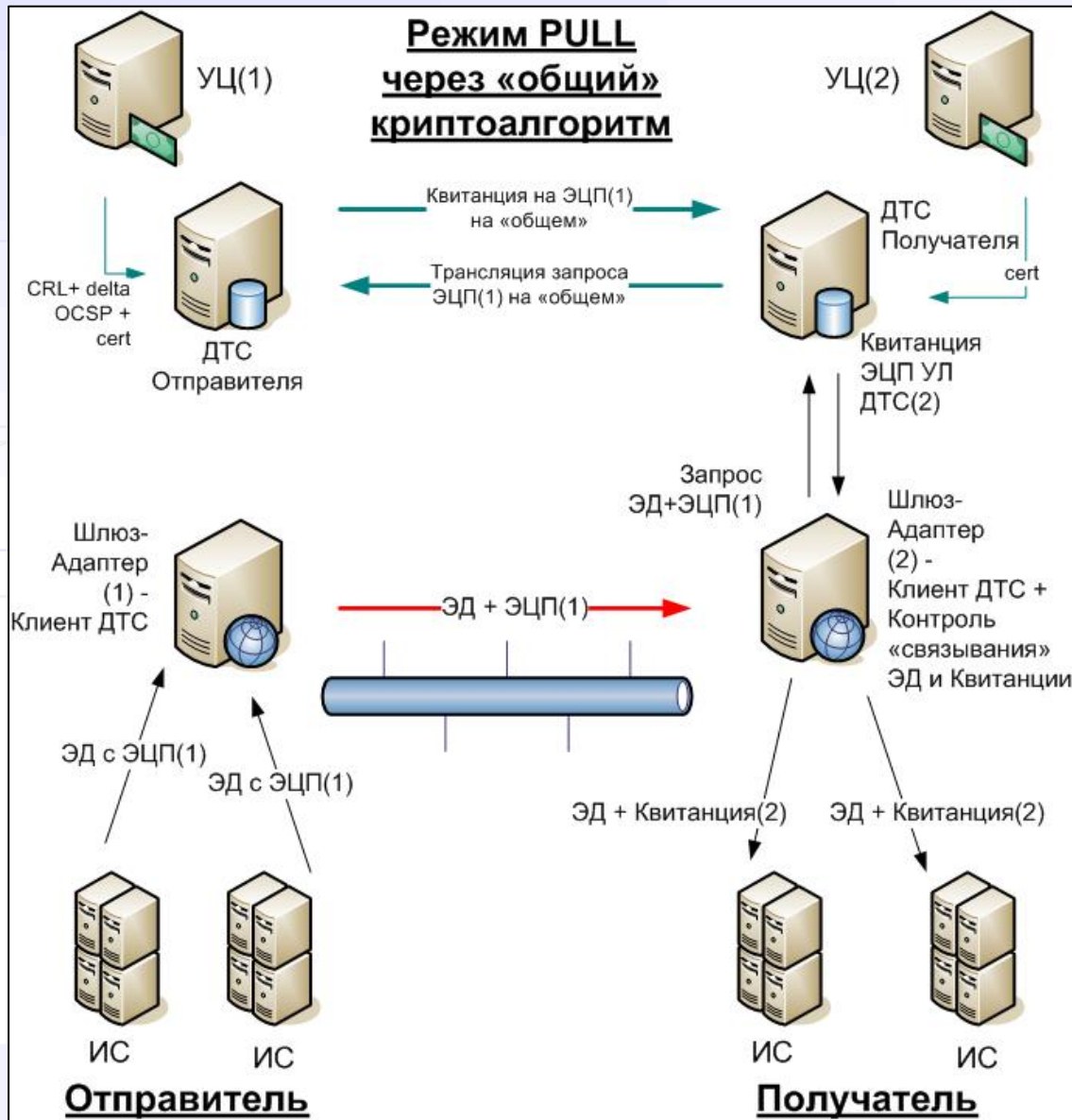
На принимающей стороне ДТС только проверяет действительность полученной квитанции без прямого обращения к ДТС отправителя.

Преимущество — минимальные требования к ДТС при Off-Line (асинхронном) взаимодействии, но это пожалуй и единственное из преимуществ.

Недостатки:

- ✓ Для модификации режима Off-line в асинхронный режим (In-line (X.842 п. 4.2.1 In-line TTP Services)) потребуются дополнительные модули поддержки очередей и т. п.
- ✓ Невозможность (большая сложность) использования режима PUSH в On-Line системах (электронные торговые площадки, торговые хабы, порталы электронных услуг, системы электронного документооборота с иностранными участниками обмена и т.п.) без значительной переделки последних.
- ✓ Крайняя неэффективность при работе с электронными сообщениями, имеющими несколько ЭЦП. Для режима PUSH число подтверждающих действительность квитанций равно квадрату числа сторон (авторов подписи), в то время как при режиме PULL число квитанций равно числу сторон.

Схема взаимодействия при PULL



Режим PULL (X.842 п. 4.2.2 On-line TTP Services). Данный режим взаимодействия функционально аналогичных ДТС различных доменов такой, при которой принимающая сторона самостоятельно и автоматически связывается с ДТС отправляющей стороны для проведения проверки ЭЦП на стороне отправителя.

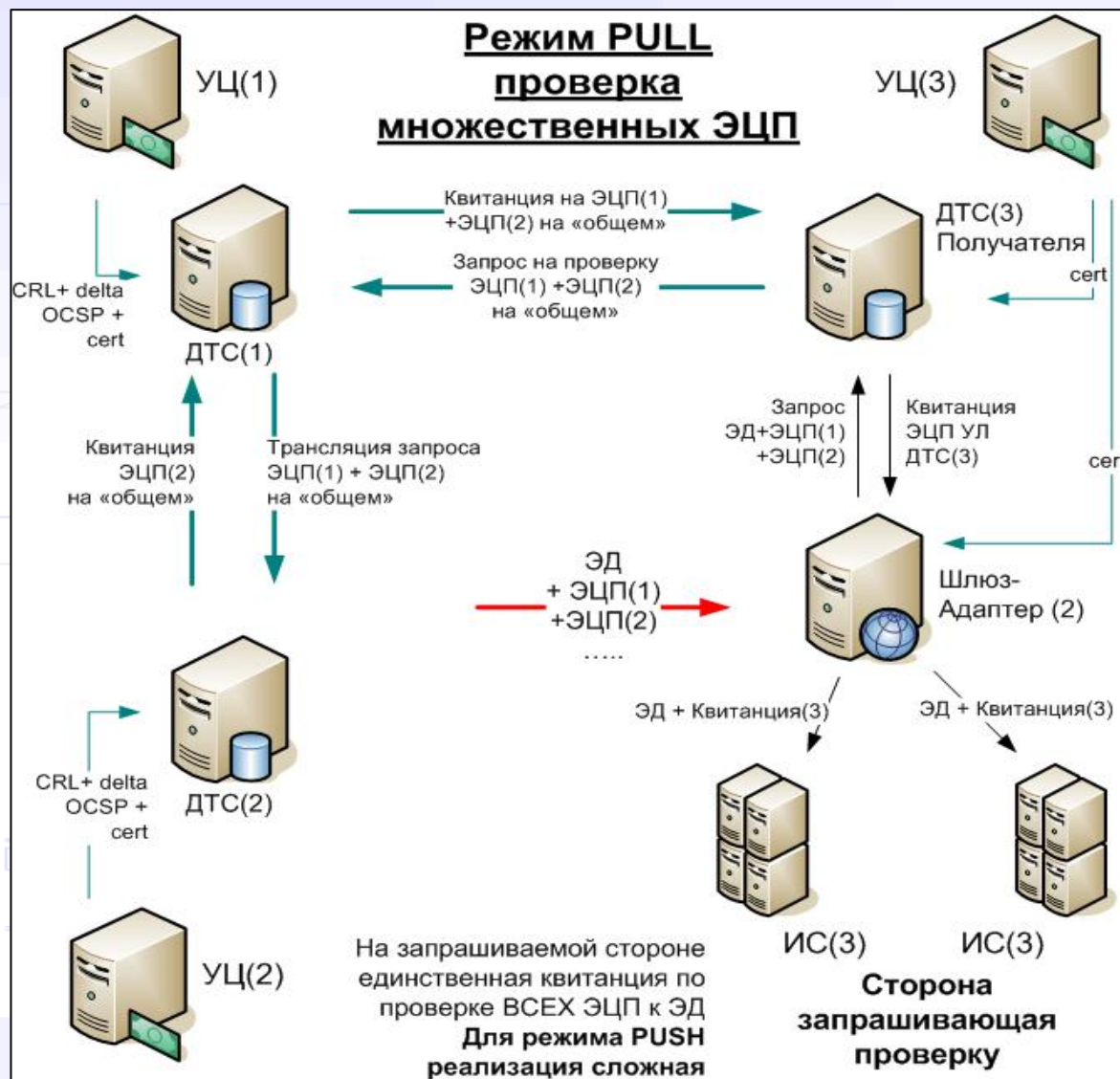
Схема взаимодействия при PULL

Очевидным преимуществом данного режима является возможность его использования для трансграничных On-line бизнес-процессов, такие как:

- ✓ электронные торговые площадки
- ✓ торговые хабы
- ✓ порталы электронных услуг
- ✓ системы электронного документооборота с иностранными участниками обмена
- ✓ и т.п..

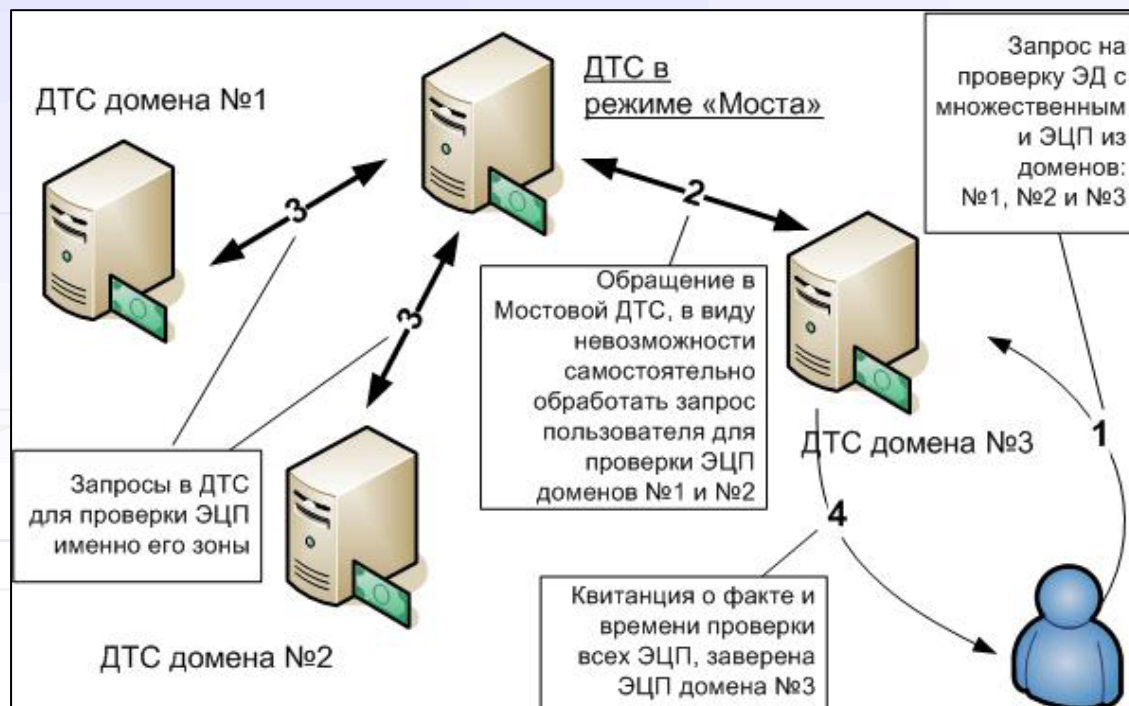
Следует также учитывать, что режим PULL предъявляет более высокие требования к коэффициенту готовности самой ДТС и окружающей телекоммуникационной инфраструктуры и такие требования должны быть соизмеримы (не ниже) с требованиями к самой On-line ИС.

Схема взаимодействия при проверке множественных подписей



ДТС может выполнять проверки множественных подписей, в том числе и из различных правовых зон, путём обращения к другим функционально аналогичным ДТС, выполняющим проверку действительности ЭП/ЭЦП для своей правовой зоны. В этом случае надо уметь предотвращать закливание запросов между ДТС, но такие решения существуют в практике.

Схема взаимодействия в режиме «Моста»



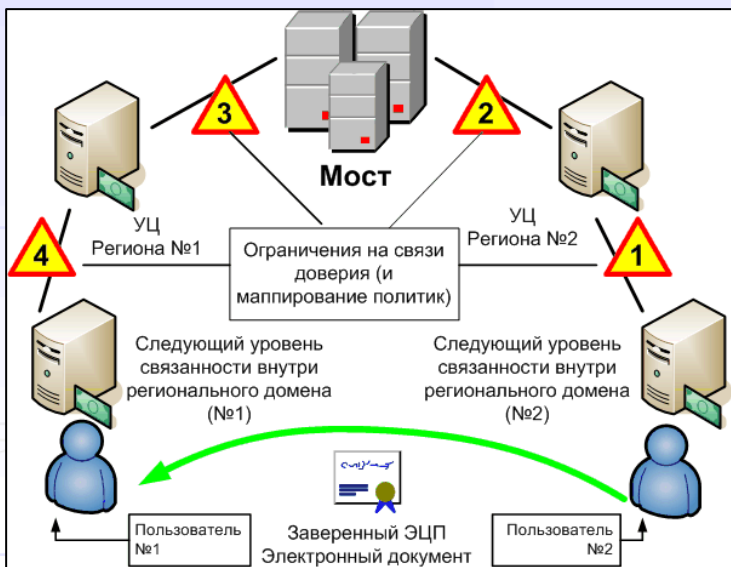
Режим Bridge - режим взаимодействия функционально аналогичных ДТС различных доменов при котором одна из ДТС выступает в роли посредника между ДТС отправителя и получателя.

К очевидным преимуществам такого режима можно отнести относительную организационно-техническую простоту всей объединённой системы взаимодействия начиная с некоего числа участвующих доменов.

Сильносвязанные домены

Преимущества:

- ✓ Обкатанная десятилетиями технология, примеры, Федеральный мостж США и Канады.
- ✓ Полная независимость доменов.
- ✓ Возможность поэтапного подключения.
- ✓ Высокая управляемость и степень живучести; проблемы в одном из доменов не разрушают всё конструкцию.
- ✓ Нет нужды в промежуточных квитанциях, во взаимодействии ДТС-ДТС, меньше накладных расходов.
- ✓ ДТС являются 100% типовыми.

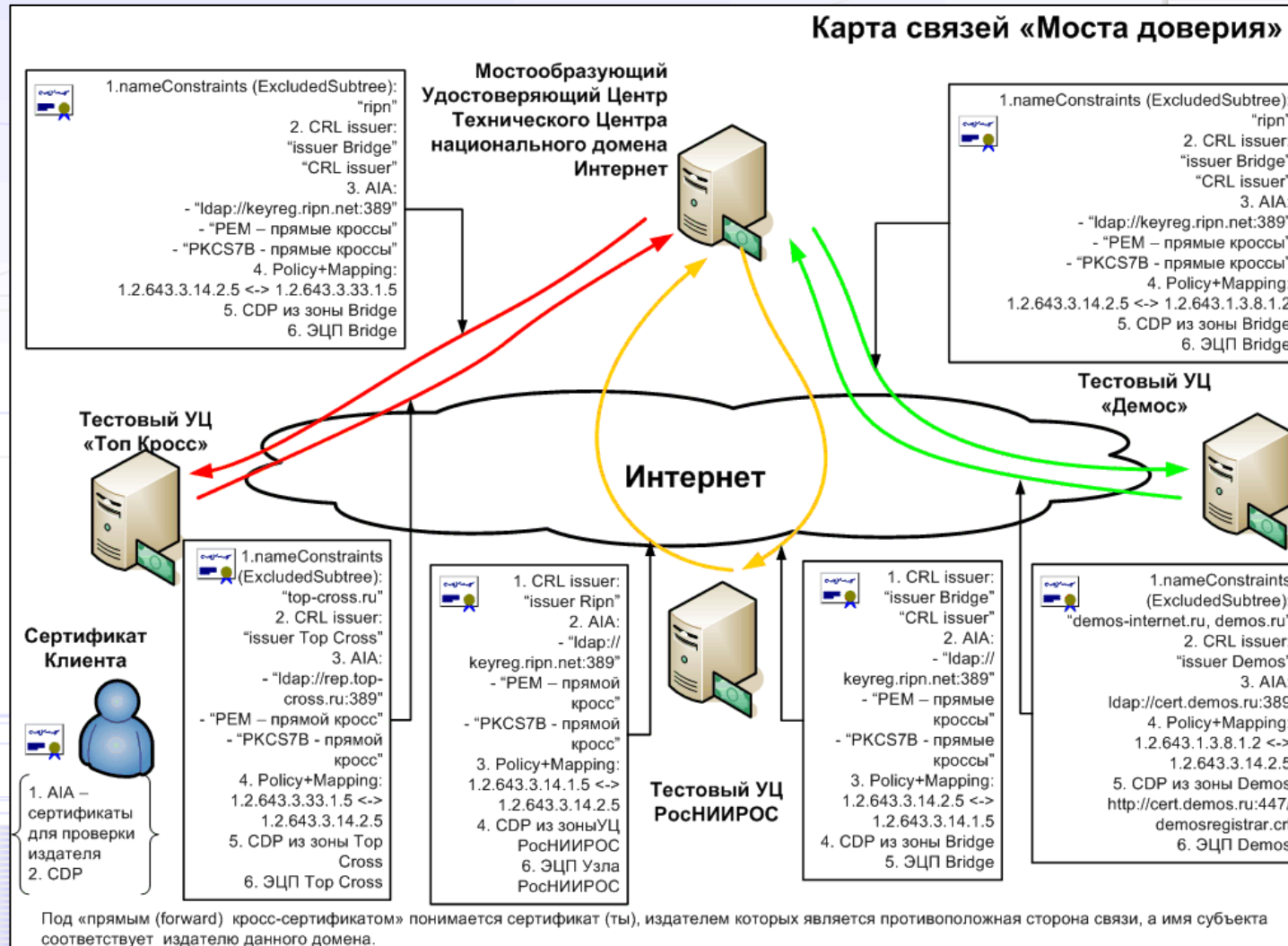


Недостатки:

- ✓ Необходимость экспорта-импорта криптографии для размещения в ДТС (это общий недостаток трансграничных систем, вспоминаем, принципы «общего алгоритма» или «двух телефонов» также требуют работы с иностранным СКЗИ).
- ✓ При построении цепочки сертификации требуется полное соответствие международной методики, такой как, разработанной в National Institute of Standards and Technology (NIST): PKITS - “Public Key Interoperability Test Suite (PKITS) Certification Path Validation” (однако, соответствие стандартом с натяжкой можно отнести к недостаткам). Такие решения и сейчас есть на рынке.

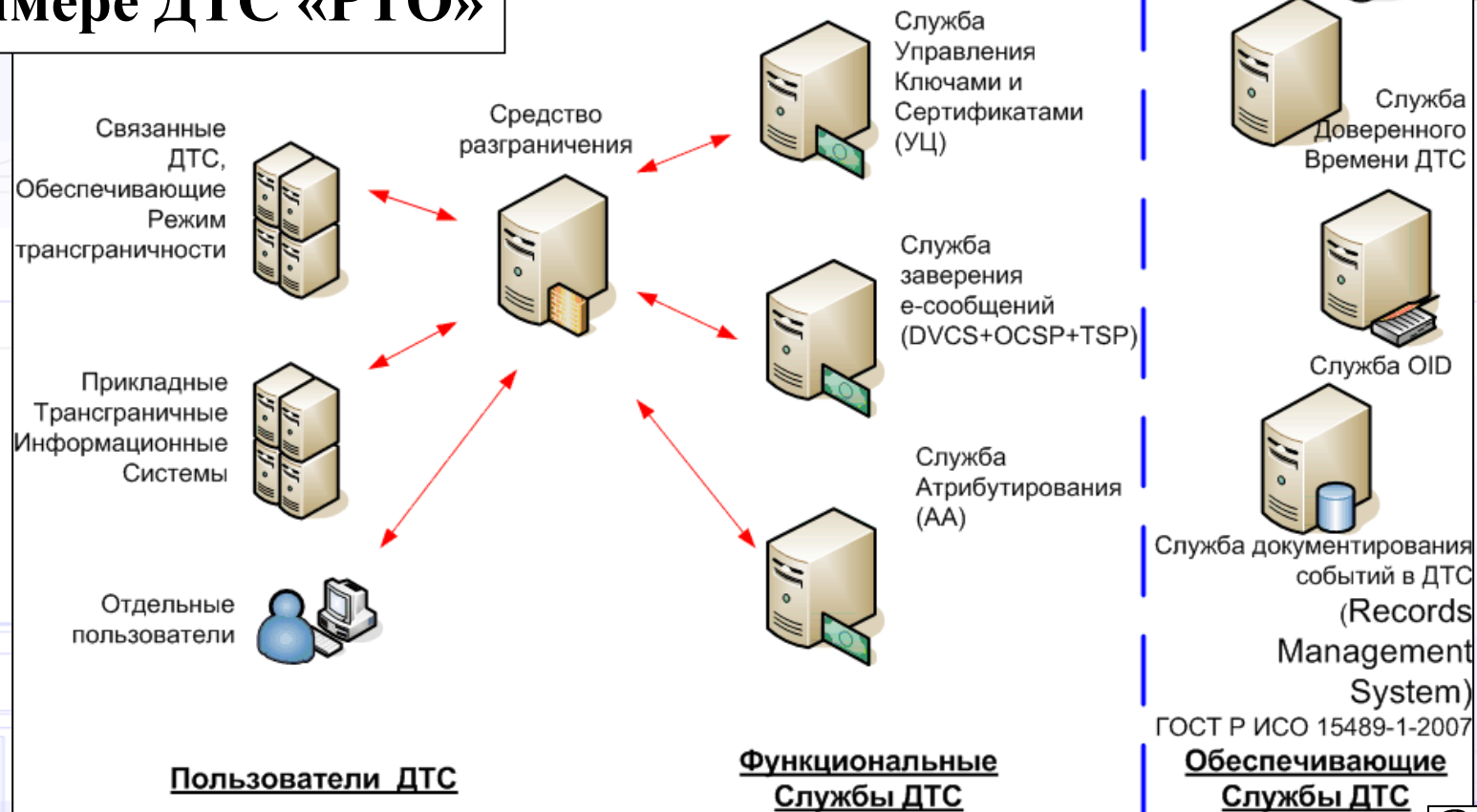
Мостовое объединение взаимодействующих доменов

Нет ничего сложного, подобное объединение было апробировано ещё в 2005 году!!!



Обобщённая Структурная Схема ДТС на примере ДТС «РТО»

Использование группы сигналов (среди которых маркеры эталонного времени) ГЛОНАСС рекомендовано Указом Президента от 17 мая 2007 г. N 638 "Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации".



*Русское
Техническое
Общество*

ООО «Русское Техническое Общество»:

- Лицензиат ФСБ РФ
- Технические решения Служб ДТС
- Услуги ДТС

<http://www.rto-ttp.ru/>

© 2015 ООО «РТО»
Муругов Сергей Михайлович
msm@rto-ttp.ru

Вопросы ?...