Организация «Моста доверия» в Системе регистрации доменов

КОНЦЕПЦИЯ

1. В рамках работ, утвержденных Координационным Центром национального домена интернет (http://www.cctld.ru/), применительно к задачам регистрации доменных имен в зоне первого уровня .RU, перевести технологию транспортировки заявок/ответов между участниками информационного обмена на уровень обращения юридически значимых электронных документов – создание единой зоны обращения электронных документов.

2. Подготовить технические решения ресурсов, на которых могут располагаться инструменты управления характеристиками доменов и сопутствующих услуг с аутентификацией субъектов и объектов доступа по предоставлению цифрового сертификата

ПРОТОТИПЫ

- Ближайшим зарубежным прототипом по реализации является проект «Сертификаты доступа к электронным услугам» (Access Certificates for Electronic Services, ACES, http://hydra.gsa.gov/aces/index.html) [eGov], инициированный в 1996 году Администрацией служб общего назначения США.
- Отечественным прототипом организационно-технического решения проекта является МУЦ, поддерживаемый Центром Компетенции «АНК» (г. Санкт-Петербург, http://www.ank-pki.ru/).

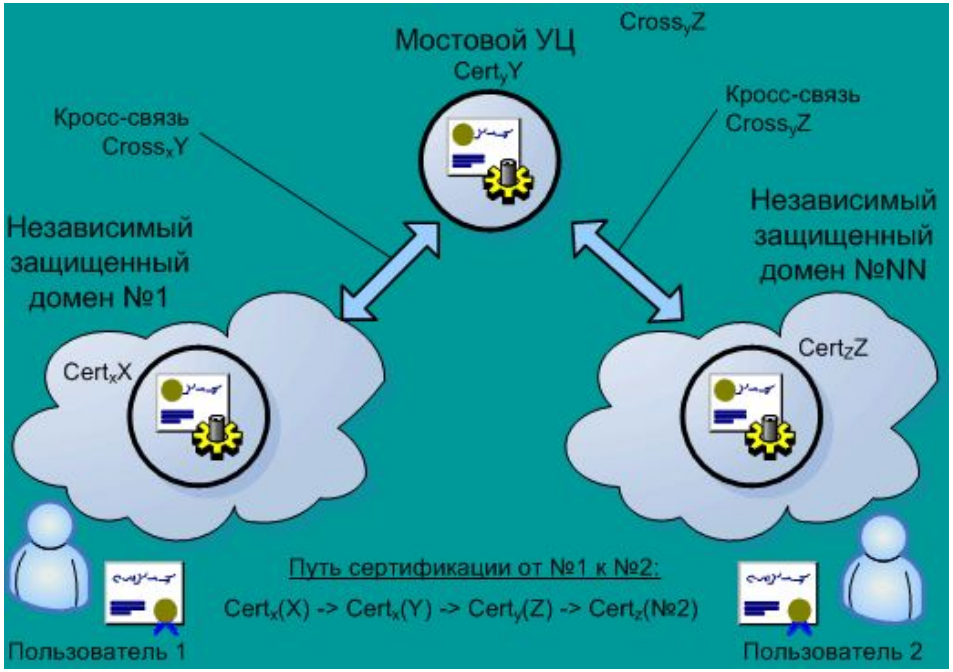
Идеи проектов сводятся к созданию системы, участником которой на основе добровольного присоединения являются самостоятельные УЦ и их пользователи, чьи сертификаты и выработанные ЭЦП признаются всеми участниками системы, т.е. создается единое защищенное пространство обращения электронных юридически значимых документов.

МОСТОВАЯ МОДЕЛЬ

Особенности:

- Точки доверия остаются внутри независимых доменов.
- При компрометации одного из издателей Регистратора, мостовой издатель разрывает связь доверия, тем самым обеспечивается максимальное управление и живучесть всего объединенного домена.
- При компрометации издателя МУЦ, узлы объединенного домена разрывают в одностороннем порядке связь с МУЦ, изолируя свое защищенное пространство до окончания процедур внеплановой смены ключей издателя МУЦ и обновления всех кросс связей для всех узлов.

Наилучшим образом подходит для PKI систем объединяющих неопределенно большое число самостоятельно регулируемых (независимых) защищенных доменов.



СПОСОБЫ ОПОВЕЩЕНИЯ УЧАСТНИКОВ СИСТЕМЫ О РАЗРЫВЕ СВЯЗЕЙ ДОВЕРИЯ

В МУЦ для оповещения участников системы о разрыве связей доверия используется стандартный PKI механизм – Списки Отозванных Сертификатов (СОС), основные СОС размещаются регулярно, а обновления к ним (дельта CRL) – по мере необходимости, на публично доступном сетевом справочнике МУЦ.

Для заверения СОС используется механизм «косвенных» СОС (indirect CRL), предусмотренный стандартом X.509. В качестве автора СОС выступает специальное уполномоченное лицо, отличное от уполномоченного лица издателя МУЦ.

Такое решение позволяет снизить риск компрометации ключей уполномоченного лица МУЦ даже без применения каких-либо специальных технических средств, т.к. отсутствует необходимость в постоянном нахождении закрытых ключей УЛ МУЦ в системе.

ОБЕСПЕЧЕНИЕ СОВМЕСТИМОСТИ

Для обеспечения криптографической совместимости с продуктами, которые уже используются у потенциальных участников, применены параметры алгоритмов, таблицы замены и правила использования, определенные текущим состоянием интернет драфтов для ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94.

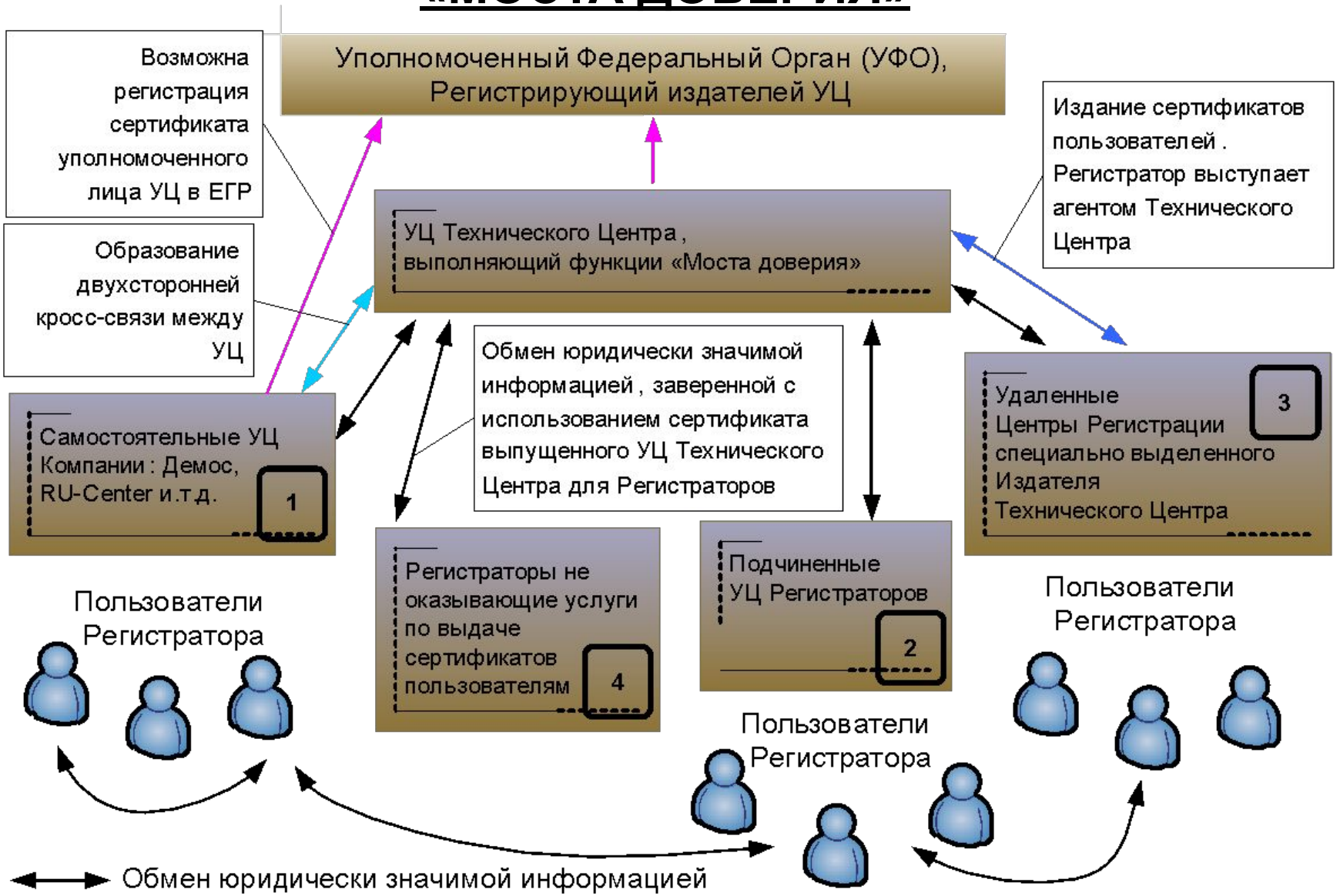
В рамках Проекта для отечественных криптографических алгоритмов уже проведены или находятся в работе:

- С ООО «Лисси» выработаны единые требования к формату транспортного контейнера (PKCS#12).
- С ЗАО «Сигнал-КОМ» проведено взаимное тестирование решений для обеспечения совместимости форматов и представления данных.
- С компанией «Демос-Телеком» - организация двухсторонних тестовых кросс-связей для технических решений МУЦ и RSA Keon (с использованием КриптоПро CSP).
- Тестирование корректности использования специальных расширений, присутствующих в сертификатах мостовых издателей и кросс-связей по методикам National Institute of Standards and Technology (NIST).

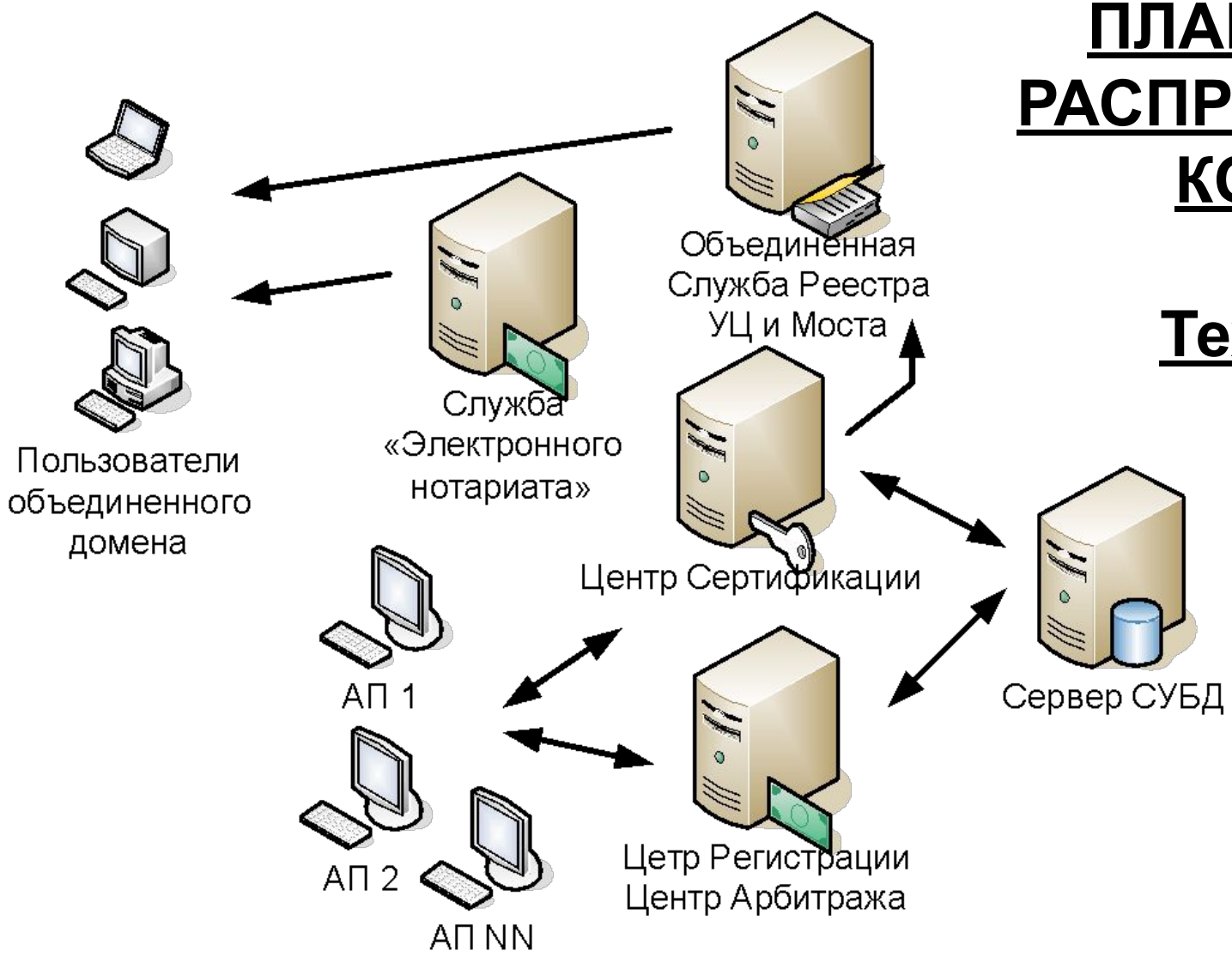
ОСНОВНЫЕ КОМПОНЕНТЫ МУЦ

- Орган управления политиками Моста доверия:
  - Осуществляет надзор за работой МУЦ.
  - Принимает решение о возможности рассмотрения заявок на кросс-сертификацию с МУЦ.
  - Подвергает экспертизе политику сертификатов заявителя на кросс-сертификацию.
- Удостоверяющий центр, образующий МУЦ:
  - Осуществляет типовой набор функций определенных для УЦ. Проводит техэкспертизу средств Участников на предмет совместимости с МУЦ.
  - Обеспечивает механизмы кросс - сертификации во внешние домены доверия.
- Реестр МУЦ:
  - Публикация и поддержание актуальности изданных сертификатов.

ПРЕДПОЛАГАЕМАЯ ОРГАНИЗАЦИЯ «МОСТА ДОВЕРИЯ»



ПЛАНИРУЕМОЕ РАСПРЕДЕЛЕНИЕ КОМПОНЕНТ МУЦ + УЦ Технического Центра

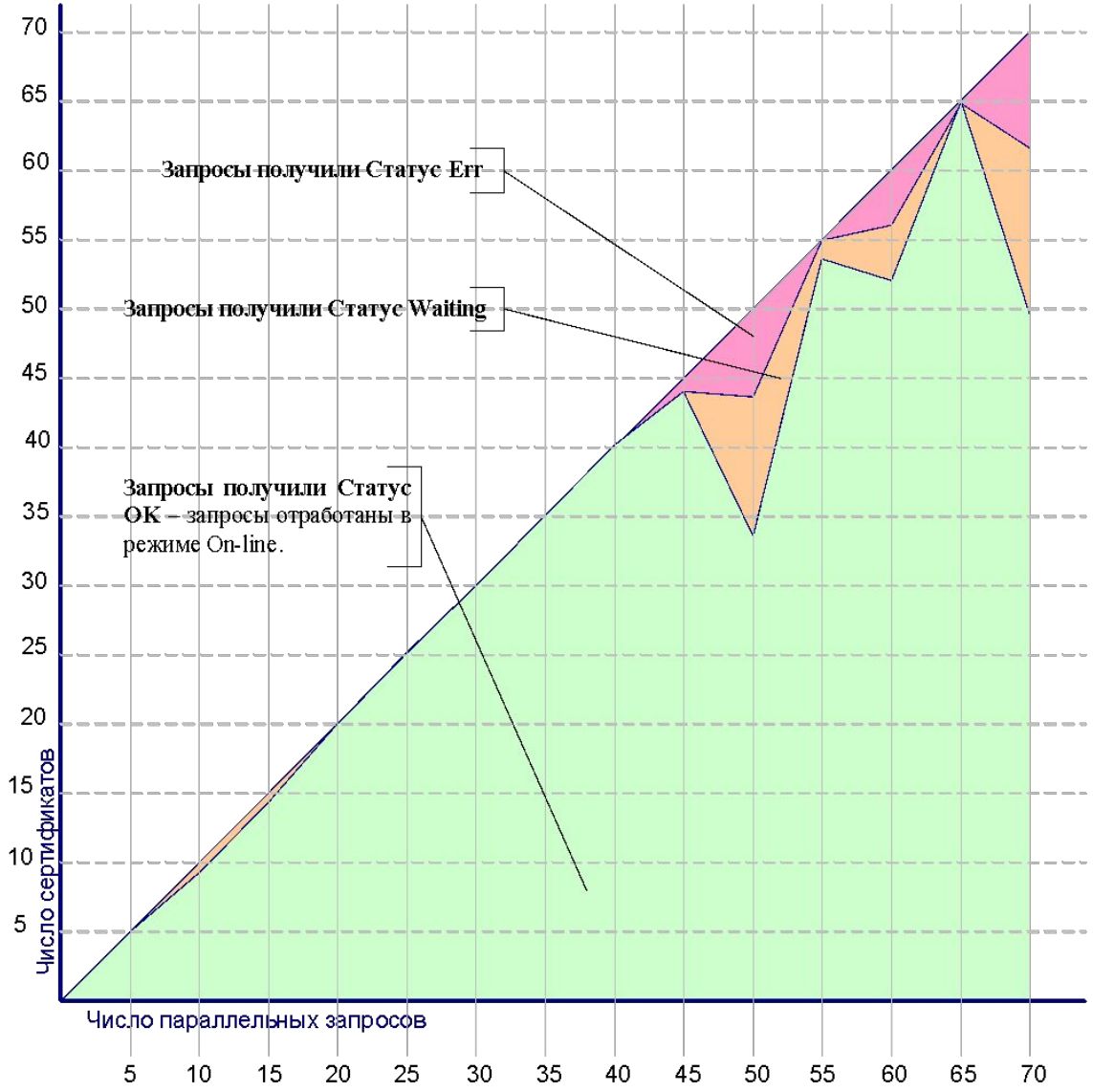


- отчуждаемое хранилище с ключами УЛ УЦ Технического Центра

- отчуждаемое хранилище с ключами УЛ Моста Технического Центра

ТЕСТИРОВАНИЕ КОМПЛЕКСА УЦ ТЕХНИЧЕСКОГО ЦЕНТРА

- **OK** – запросы отработаны в режиме On-line.
- **Waiting** – запросы приняты к обработке УЦ и размещены в очереди.
- **Err** – запросы не приняты к обработке УЦ (TLS, СУБД)



ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ РЕАЛИЗАЦИИ ПРОЕКТА

- Распространение передовых технологий и отечественной криптографии.
- Применение единообразного – типового решения вне зависимости от конкретного Регистратора или их числа.
- Повышение защищенности циркулирующих электронных документов, а также технологии предоставления сопутствующих услуг.
- Упрощению технологии сбора доказательной базы при конфликтных ситуациях в ходе регистрации, передаче прав и т.п. на домены в зоне RU.
- Создание наработок для последующих стадий проекта.

ИСПОЛЬЗУЕМЫЕ РЕШЕНИЯ:

ООО «Топ Кросс», г. Москва.

E-mail: info@top-cross.ru

WWW: http://www.top-cross.ru/

Компоненты Удостоверяющего Центра сертификатов ключей подписи, компоненты службы «Электронного нотариата», клиентское программное обеспечение.

ООО «КриптоЭкс», г. Москва

E-mail: info@cryptoex.ru

WWW: http://www.cryptoex.ru/

Криптографическая защита. Сертифицированная ФАПСИ Программная библиотека защиты информации (ПБЗИ) «Крипто-Си».

Генеральный директор
ООО «Топ Кросс»
Муругов Сергей Михайлович

Вопросы ?...