НЦЭУ

PKI-FORUM
РОССИЯ

Доверенная третья сторона: где мы находимся и перспективы развития в Республике Беларусь

НЦЭУ

PKI-FORUM РОССИЯ

Межгосударственный обмен электронными документами

Служба **ДОВЕРЕННОЙ ТРЕТЬЕЙ СТОРОНЫ (ДТС)** предназначена для межгосударственного обмена электронными документами и автоматизации процессов, связанных с подтверждением подлинности электронной цифровой подписи, идентичности и целостности электронного документа и как следствие – признание его юридической силы и достоверности, защиты данных и обеспечения архивного хранения электронных документов.

Техническая концепция «Доверенной третьей стороны», воплощающая эти идеи, изложена в международных рекомендациях X.842, определяющих требования к перечню доверенных сервисов как к комплексу организационно-технических мероприятий

НЦЭУ

PKI-FORUM РОССИЯ

Концепция ДТС и возможности

Концепция ДТС не требует изменения в законодательстве стран-участников, так как центры ДТС в каждой стране проходят проверку на соответствие только национальным стандартам.
Существующий в стране центр ДТС будет проверять действительность сертификата и электронной цифровой подписи под документом другого государства, а также выдавать квалифицированную справку (квитанцию) о результатах такой проверки.

Применение сервиса ДТС позволяет:

- повысить удобство обмена электронными документами, подписанными ЭЦП различных государств;
- повысить уровень надежности и защищенности трансграничного межгосударственного информационного взаимодействия;
- разрешать спорные вопросы, возникающие между участниками межгосударственных информационных процессов.

НЦЭУ

PKI-FORUM РОССИЯ

Новые полномочия Государственного предприятия «НЦЭУ»

НЦЭУ осуществляет функции национального оператора доверенной третьей стороны по признанию подлинности электронных документов при межгосударственном электронном взаимодействии

Указ Президента РБ от 8 ноября 2011 № 515
(с изменениями, внесенными Указом Президента РБ от 15.03.2016 № 98)

НЦЭУ

PKI-FORUM РОССИЯ

В НЦЭУ 30 декабря 2016 г. для коммерческого использования введена в постоянную эксплуатацию автоматизированная информационная система доверенной третьей стороны Республики Беларусь (ДТС-Беларусь).

На сегодняшний день успешно проведено тестирование и осуществляется взаимодействие ДТС-Беларусь с ДТС Республики Казахстан (РГП «Государственная техническая служба» Комитета национальной безопасности Республики Казахстан).

В рамках пилотного проекта ТПД РБ-РФ успешно проведено тестирование по взаимодействию с ДТС ООО «УЦ ГИС» на базе ПАК «СДТС Litiria DVCS».

НЦЭУ

PKI-FORUM РОССИЯ

В рамках развития интегрированной информационной системы (далее – интегрированная система) Евразийский экономический союз (далее – ЕАЭС) создается служба ДТС Евразийской экономической комиссии (далее – ЕЭК), а также сервис ДТС национального сегмента РБ интегрированной системы ЕАЭС.

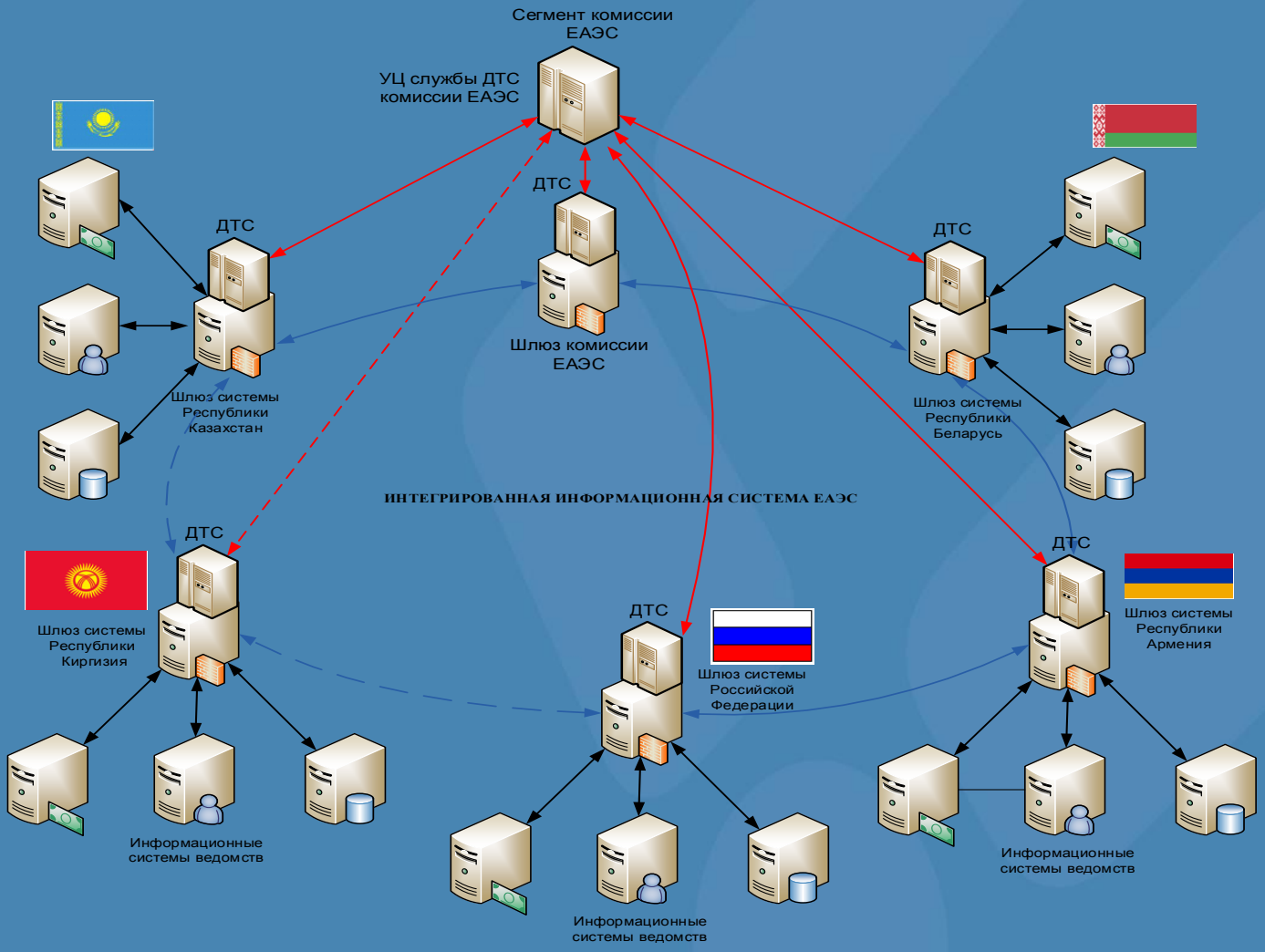
Сервис ДТС РБ создается на базе типового ПО ДТС, переданного ЕЭК.

Сервис ДТС национального сегмента Республики Беларусь интегрированной системы ЕАЭС предназначен для организации взаимодействия с другими уполномоченными операторами ДТС интегрированной системы ЕАЭС и их уполномоченных лиц.

НЦЭУ

PKI-FORUM РОССИЯ

Схема электронного документооборота в интегрированной информационной системе ЕАЭС



НЦЭУ

PKI-FORUM РОССИЯ

1 этап (до 2018 года) – должно обеспечиваться развитие трансграничного пространства доверия для осуществления полноценного межгосударственного электронного взаимодействия.

До конца года планируется утвердить:

- Требования к созданию, развитию и функционированию трансграничного пространства доверия;

- **Положение об УЦ службы ДТС интегрированной информационной системы союза;**
- **Порядок функционирования службы ДТС интегрированной информационной системы союза**
- **Регламент УЦ службы ДТС интегрированной информационной системы союза;**

НЦЭУ

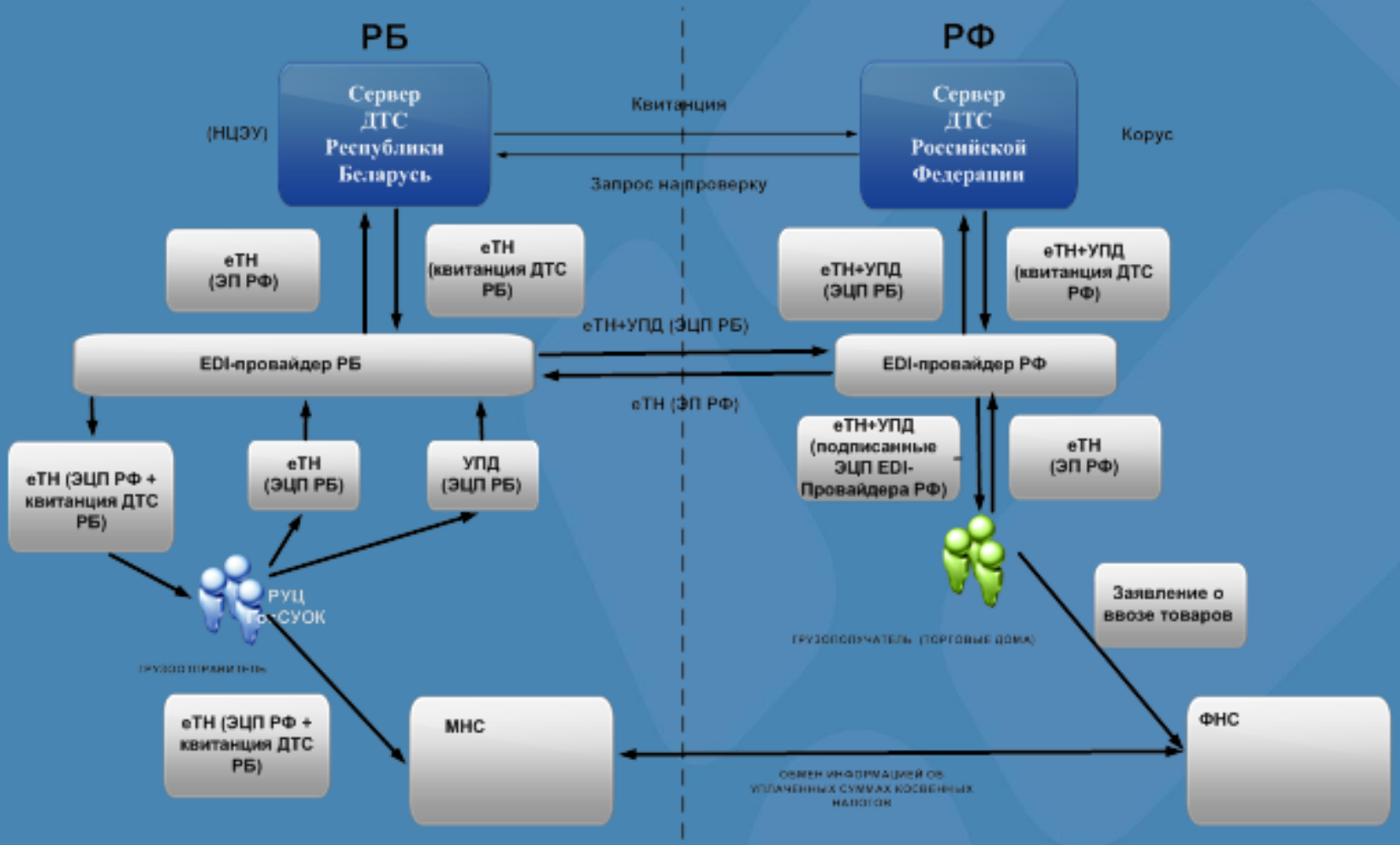
PKI-FORUM РОССИЯ

2 этап (до 2020 года) –должна быть обеспечена возможность электронного взаимодействия физических и юридических лиц между собой, а также с органами государственной власти государств-членов при нахождении физических и юридических лиц на территориях своих государств.

Разработан проект Плана мероприятий по реализации второго этапа, которым предусмотрено:

- **разработка порядка функционирования службы ДТС для взаимодействия B2B, B2G, C2C, C2B, C2G;**
- **разработка требований к операторам ДТС (включая порядок проверки таких операторов и их аккредитация).**

Пример информационного обмена электронными документами с использованием сервисов ДТС при перемещении товара



Стандартизация в РБ в области PKI и сервисов ДТС

В Республике Беларусь разработаны проекты Государственных стандартов:

СТБ 34.101.78 – 2018 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»;

СТБ 34.101.79 – 2018 «Информационные технологии и безопасность. Криптографические токены»;

СТБ 34.101.80 - 2018 «Информационные технологии и безопасность. Расширенные электронные цифровые подписи»;

СТБ 34.101.81 – 2018 «Информационные технологии и безопасность. Протоколы службы заверения данных»;

СТБ 34.101.82 – 2018 «Информационные технологии и безопасность. Протокол постановки штампа времени»;

СТБ 34.101.50 – 2018 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий».

НЦЭУ

PKI-FORUM РОССИЯ

СТБ 34.101.78 – 2018 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»

Задачи, решаемые в стандарте:

- конкретизировать перечень сторон ИОК;
- разработать форматы данных обмена между сторонами ИОК;
- разработать прикладные интерфейсы взаимодействия сторон ИОК, а также сторон ИОК с прикладными системами документооборота и архивного хранения;
- разработать формат ключевого контейнера программных криптографических токенов;
- разработать высокоуровневый программный интерфейс взаимодействия криптографического ПО средств ЭЦП (клиентских программ) с аппаратными криптографическими токенами.

НЦЭУ

PKI-FORUM РОССИЯ

СТБ 34.101.79 – 2018 «Информационные технологии и безопасность. Криптографические токены»

Целью разработки стандарта является насыщение, детализация и унификация взаимодействия сторон ИОК.

Задачи, решаемые в стандарте:

- конкретизировать перечень сторон ИОК;
- разработать форматы данных обмена между сторонами ИОК;
- разработать прикладные интерфейсы взаимодействия сторон ИОК, а также сторон ИОК с прикладными системами документооборота и архивного хранения;
- разработать формат ключевого контейнера программных криптографических токенов;
- разработать высокоуровневый программный интерфейс взаимодействия криптографического ПО средств ЭЦП (клиентских программ) с аппаратными криптографическими токенами.

НЦЭУ

PKI-FORUM РОССИЯ

СТБ 34.101.78 – 2018 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»

Целью разработки стандарта является определение криптографической подсистемы криптографических токенов аутентификации и ЭЦП.

Задачи, решаемые при разработке стандарта:

- определить перечень идентификационных данных владельца токена;
- определить перечень криптографических объектов, размещаемых на токене;
- определить криптографические алгоритмы и протоколы, реализуемые токеном;
- определить схему взаимодействия токена с сервером аутентификации;
- определить командный интерфейс взаимодействия криптографического программного обеспечения средств ЭЦП (клиентских программ) с криптографическим токеном;
- определить логику работы прикладных программ eId и eSign.

НЦЭУ

PKI-FORUM РОССИЯ

СТБ 34.101.80 - 2018 «Информационные технологии и безопасность. Расширенные электронные цифровые подписи»

Стандарт устанавливает форматы расширенной электронной цифровой подписи, которая дополнительно к базовой, включает (и при необходимости контролирует) атрибуты подписанного документа и подписавшей его стороны.

Стандарт планируется применять при создании и обработке электронных документов форматов АСН.1, XML и PDF.

Определены три формата: CAdES, XAdES и PAdES.

НЦЭУ

PKI-FORUM РОССИЯ

СТБ 34.101.81 – 2018 «Информационные технологии и безопасность. Протоколы службы заверения данных»

Стандарт определяет протоколы службе заверения данных (СЗД), с помощью которых можно удостоверить факты владения данными, существования данных, действительности ЭД и СОК. Стандарт основан на RFS 3029.

Стандарт так же определит форматы запросов к СЗД и соответствующего ответа, правила создания и обработки запроса и ответа.

Стандарт основан на RFS 3029, 2001.

НЦЭУ

PKI-FORUM РОССИЯ

СТБ 34.101.82 – 2018 «Информационные технологии и безопасность. Протокол постановки штампа времени»

Стандарт устанавливает протокол постановки штампа времени, который подтверждает факт существования данных к определенному моменту времени. Стандарт определяет форматы сообщений, которыми обмениваются стороны протокола, и действия сторон.

Базируется на RFS 3161, 2001.

НЦЭУ

PKI-FORUM РОССИЯ

СТБ 34.101.50 – 2018 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий»

Стандарт устанавливает правила регистрации объектов информационных технологий. Идентификаторы определяются в соответствии с соглашениями абстрактно-синтаксической нотации версии 1 (АСН.1) по ГОСТ 34.973. В стандарте определена структура дерева идентификаторов, определены методы назначения идентификаторов.

НЦЭУ

PKI-FORUM
РОССИЯ

Спасибо за внимание!

Контактные данные:
МОСКАЛЕВ Дмитрий Владимирович,
Республиканский удостоверяющий центр
Государственного предприятия «НЦЭУ»
Телефон: +375 29 665-11-59
Skype: dmmoskalev
E-mail: mdv@nces.by