Н.Н. ЕГИПКО
Советник отдела Центра таможенной статистики
Секретариата Комиссии Таможенного союза

«НЕКОТОРЫЕ АСПЕКТЫ ПОСТРОЕНИЯ ПОДСИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБЕСПЕЧЕНИЯ ЮРИДИЧЕСКОЙ ЗНАЧИМОСТИ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ ИИСВВТ ПРИ ПРИМЕНЕНИИ МЕХАНИЗМОВ «ЕДИНОГО ОКНА»

Рекомендации международной организация СЕФАКТ ООН по созданию механизма и выработке правовой основы системы «единого окна», известные как № 33 и № 35, содержат юридические и технические аспекты, касающиеся использования электронной подписи, как одного из важных элементов обеспечения безопасности бизнеса.

В контексте данных рекомендаций «единое окно» определяется как механизм, благодаря которому стандартизованную информацию и документы в электронном виде можно представлять только один раз.

На рисунке 1 представлен вариант модели механизма, с учетом развития инфокоммуникационных технологий государств-членов Таможенного союза.

Рис. 1. Модель для механизма «Единого окна»

Мировая практика показала, что единственный способ обеспечить достоверность и неотказуемость при обмене электронными документами – это использование электронной цифровой подписи, выработанной на квалифицированных или усиленных сертификатах..

Необходимо подчеркнуть, что ЭЦП является не только средством идентификации и аутентификации, но и необходимым реквизитом при организации юридически значимого электронного документооборота. Сообщение или файл, у которого отсутствуют необходимые реквизиты, не может считаться электронным документом.

Рис. 2. Схема юридически значимого обмена документами

Одной из наиболее важных задач при проектировании ИИСВВТ (Рис. 3), является создание технического решения, которое бы обеспечило юридическую значимость информационного обмена, как между национальными сегментами, так и с Центральным узлом системы. Актуальность данной задачи обусловлена тем, что в странах Таможенного союза широко используется технология PKI – «Инфраструктура открытых ключей», на основе международных рекомендаций X.509, но при этом применяются национальные криптографические алгоритмы формирования и проверки ЭЦП.

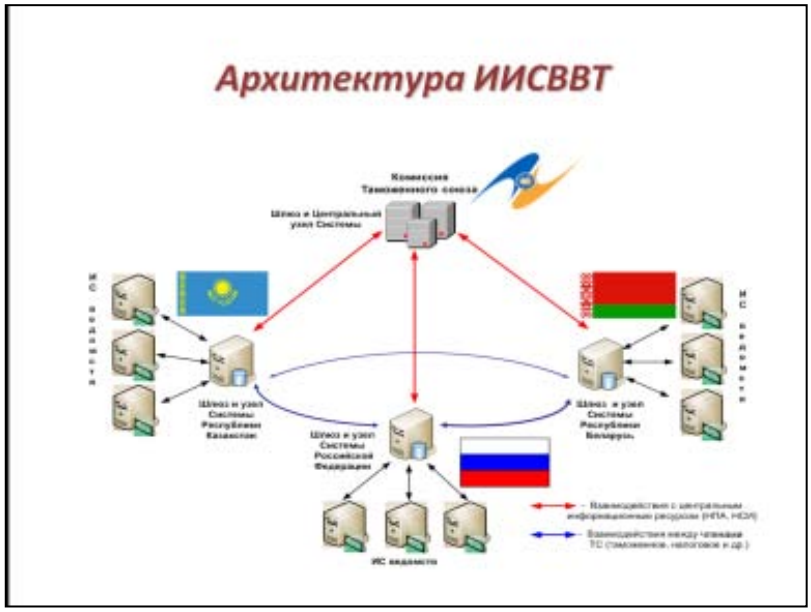

Рис. 3. Архитектура ИИСВВТ**.**

В составе Центрального узла, (рис.4.) можно выделить три типа информационных систем по критерию обработки в них юридически значимой информации. На слайде они представлены в порядке повышения требований информационной безопасности.

Наиболее критичными являются учетные системы, в них обязательно применение средств ЭЦП, так как потери, искажения или модификация данных недопустимы.

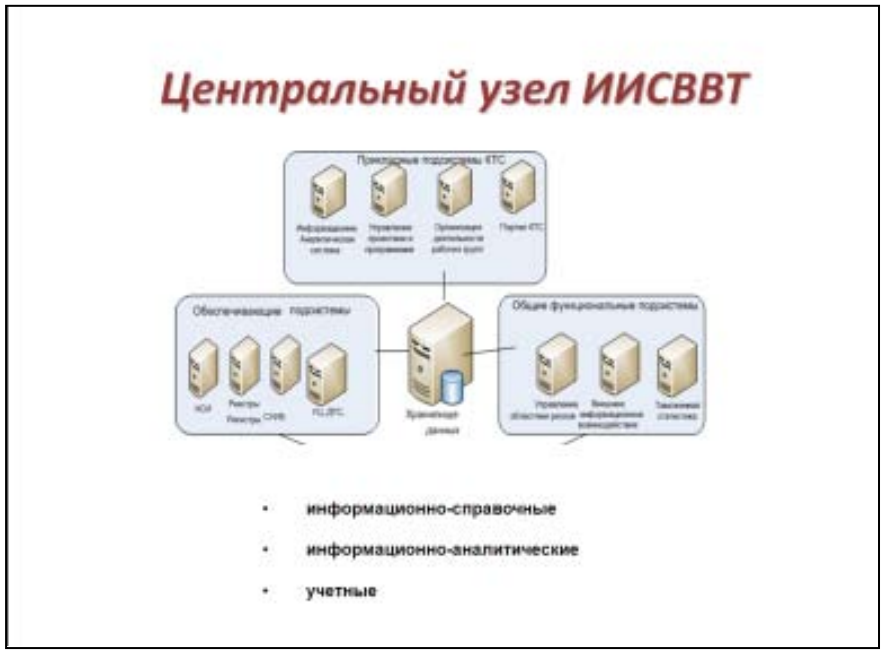

Рис. 4. . Архитектура ЦУ КТС.

Использование ЭЦП связано с двумя действиями: формирование и проверка (Рис. 5). Для формирования ЭЦП необходимо иметь криптографическое средство и ключ подписи.

Проверка или валидация ЭЦП состоит из двух операций:

- Первая, чисто математическая – проверка на соответствие ЭЦП тексту полученного документа и открытому ключу подписи;
- Вторая – необходимо убедиться в действительности сертификата ключа автора на момент формирования подписи.

Данная задача решается просто в случаях – если владелец СКП и проверяющая сторона находятся на обслуживании одного и того же Удостоверяющего Центра или принадлежат одному домену доверия. Если же

эти условия не соблюдаются, то возникают серьезные организационно-технические сложности.

Рис. 5. Схема формирования и валидации ЭЦП.

Существует несколько путей решения задачи легитимности ЭЦП. Первый путь - обеспечить всех участников в рамках Таможенного союза единой технологией ЭЦП. Однако данное решение не применимо, так как оно входит в противоречие с ранее принятыми соглашениями Сторон:

- Система не должна подменять национальные системы государств-членов;
- Система не должна требовать от государств-членов внесения изменений в средства обеспечения информационной безопасности информационных систем государственных органов, регулирующих внешнюю и взаимную торговлю;
- архитектура Системы должна предусматривать возможность информационного взаимодействия с внешними информационными системами.

Второй путь – признание на территории Таможенного союза сертификатов всех УЦ Сторон и обеспечение проверки любой ЭЦП в правовом поле каждого из государств. В настоящее время в государствах-членах Таможенного союза развернуто много Удостоверяющих центров на основе технологии PKI, однако создать единую систему проверки не представляется возможным в связи с применением национальных криптографических алгоритмов. Криптографические средства относятся к технологиям двойного применения и вопрос согласования с национальными уполномоченными органами, т.е. спецслужбами, очень сложная и длительная процедура.

Третье направление – это обеспечение доступности услуг по проверке действительности ЭЦП зарубежного автора на территории и в правовом поле его государства. Международные рекомендации X.842, объединенные термином «Доверенная Третья Сторона» определяют порядок реализации услуг "Электронного нотариуса". «Электронный нотариус» обеспечивает проверку ЭЦП и сертификата с выработкой квитанций, содержащих результаты проверки и «штамп» времени.

В составе Центрального узла ИИСВВТ (Рис. 6) должны быть развернуты сервисы ДТС: Удостоверяющий центр и "Электронный нотариат" (DVCS-сервис). ДТС Центрального узла взаимодействует с ДТС из состава национального сегмента государства-члена Таможенного союза.

В соответствии с технологией ДТС, в состав прикладных и общих функциональных подсистем ЦУ, обеспечивающих предоставление юридически значимых сервисов, должны входить средства криптографии и интеграционный программный модуль. Средства криптографии обеспечивают выработку и проверку ЭЦП в соответствии с правилами и требованиями Таможенного союза. Интеграционный модуль обеспечивает формирование dvcs-запроса к ДТС в случаях, когда электронный документ подписан внешней подписью, т.е. по национальным стандартам одной из Сторон.

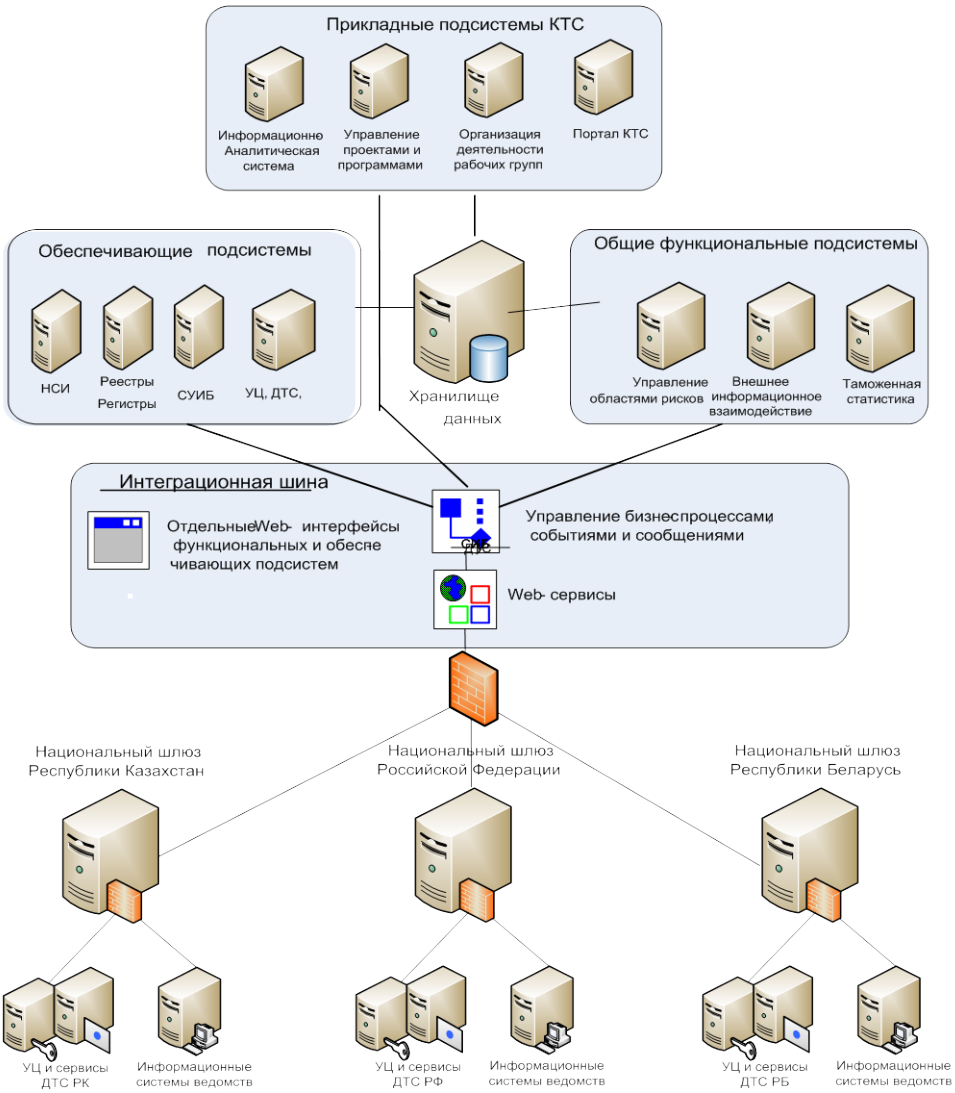

Рис.6. Основные компоненты ИИСВВТ.

Удостоверяющий Центр является ключевым элементом подсистемы информационной безопасности. Он обеспечивает выпуск и управление сертификатами ключей подписи для прикладных систем, «Электронного нотариата», а также, для 3-х ДТС из состава национальных сегментов. Схема распределения и управления сертификатами и ключами представлена на рисунке 7.

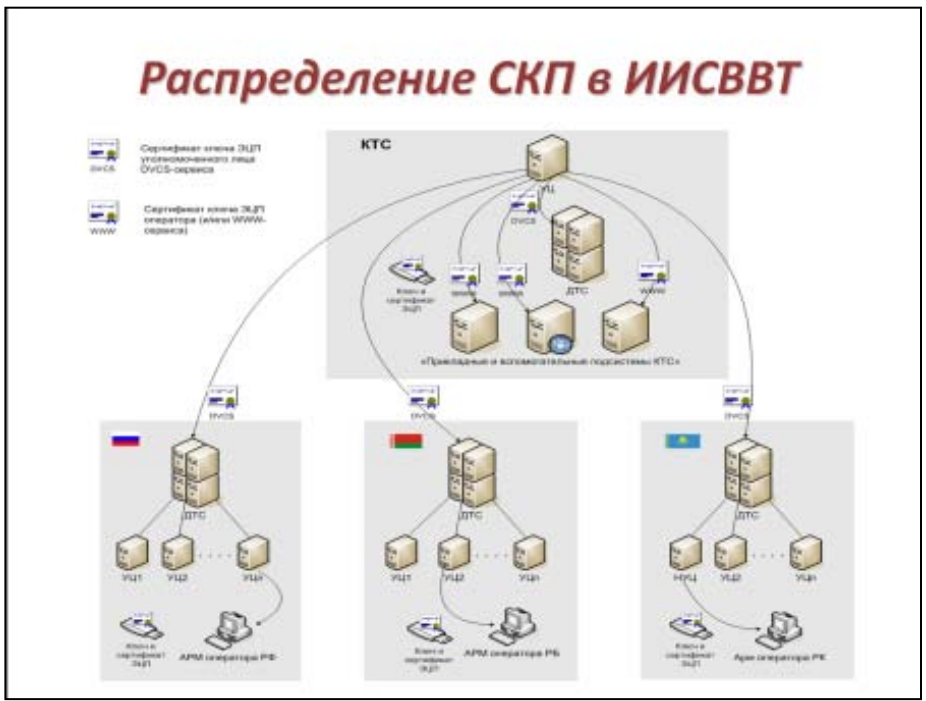

Рис.7. Схема распределения СКП и ключей в ИИСВВТ

При проверке ЭЦП, ДТС Центрального узла выполняет управление запросами и квитанциями при обмене с ДТС национальных сегментов. ДТС национального уровня взаимодействует с Удостоверяющими Центрами в национальном домене доверия. (Рис.8.)

Рис. 8. Схема распределения запросов при валидации ЭЦП электронного документа.

При проверке ЭЦП, ДТС обеспечивает выполнение следующих функций:

- Проверка действительности ЭЦП;
- Проверка действительности сертификата открытого ключа на конкретный момент времени.

Результатом работы Электронного нотариуса является квитанция с результатами проверки ЭЦП, содержащая «штамп» времени и заверенная

подписью ДТС. ДТС в составе национальных сегментов выполняют аналогичные операции и функции.

Процедура проверки ЭЦП и действительности сертификата на определенный момент времени имеет большое количество особенностей. Это предмет детального рассмотрения и согласования на последующих этапах создания ИИСВВТ.

Также следует отметить, что для ряда систем необходимо рассмотреть вопрос применения усовершенствованной подписи (Рис. 9), основанной на европейском стандарте CMS Advanced Electronic Signatures (CAdES) (ETSI TS 101 733, RFC 5126). Данная подпись позволит решить основные трудности, связанные с доказыванием статуса сертификата на момент подписания, и обеспечить участников электронного обмена всей необходимой доказательной базой.

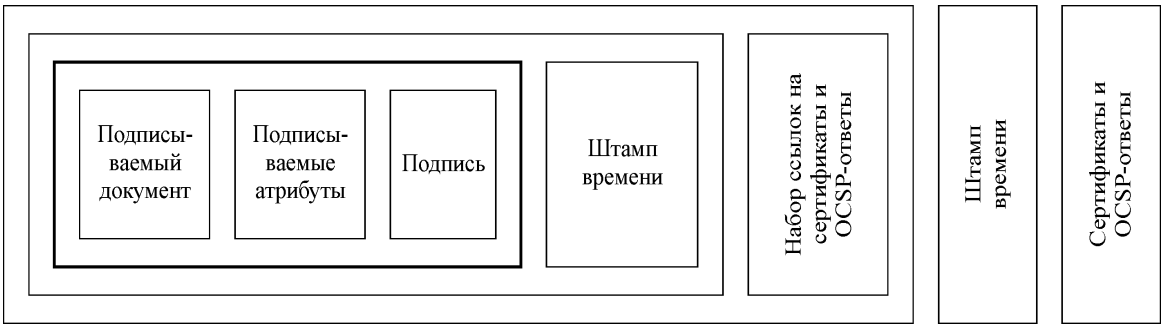

Рис. 9. Формат усовершенствованной электронной цифровой подписи

Заключение.

Представленный подход позволит обеспечить юридическую значимость электронных документов и сообщений в ИИСВВТ при трансграничном обмене в рамках механизма «Единого окна».

Реализация предложенной технологии, основанной на сервисах PKI и "Доверенной третьей стороны", полностью согласуется с принятыми Соглашениями в рамках Таможенного союза и положениями нового закона России об ЭЦП.

Как отметил Ответственный Секретарь Сергей Юрьевич Глазьев, Комиссия Таможенного союза в настоящее время имеет полномочия более чем по 150 государственным функциям, в связи с чем, электронный документооборот переходит в новое качество, и сегодня Секретариату КТС требуется осуществлять оперативный юридически значимый электронный информационный обмен.