Система электронного документооборота (ЭДО)

Используемые термины и сокращения

Термин	Определение
ЭДО	Система электронного документооборота ЕТС
Абонент ЭДО	Организация, зарегистрировавшая свои открытые ключи на Товарной бирже ЕТС и подключенная к системе ЭДО
Электронно-цифровая подпись, ЭЦП	Данные, формируемые в результате криптографического преобразования электронного документа, позволяющие установить подлинность электронного документа
Шифрование	Криптографическое преобразование позволяющее прочесть электронный документ, только тому, для кого он зашифрован
Секретный ключ	Уникальные данные абонента ЭДО, известные только этому абоненту и используемые программным обеспечением для формирования ЭЦП или расшифрования информации.
Открытый ключ	Данные, соответствующие секретному ключу абонента ЭДО и позволяющие проверить подлинность ЭЦП в электронном документе, полученном от этого абонента или зашифровать для него электронное сообщение
Подлинность документа	Свойство электронного документа, характеризующее принадлежность этого документа определенному абоненту ЭДО и неизменность его содержания с момента формирования ЭЦП для этого документа
Сертификат	Электронный документ, подписанный ЭЦП Удостоверяющего центра (РГП КЦМР НБ РК), содержащий открытый ключ абонента ЭДО, а также информацию об электронном адресе этого абонента, сроке действия и других параметрах открытого ключа
Удостоверяющий Центр	Удостоверяющий центр Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" (КЦМР НБ РК), далее "Удостоверяющий центр" (УЦ)
Центр ЭДО	Аппаратно-программный комплекс, расположенный на Товарной бирже ЕТС и выполняющий функции маршрутизации сообщений, распространения сертификатов открытых ключей, хранения списка их состояний, ведения протоколов
Мэйлбокс	Аппаратно-программный комплекс, расположенный в локальной сети абонента ЭДО и предназначенный для передачи сообщений
Приложение ЭДО	Программа или система, использующая ЭДО как транспорт для передачи сообщений при взаимодействии с другими приложениями

Введение

Система ЭДО

ЭДО - это система передачи электронных документов, в которую интегрированы:

- средства криптографической защиты информации;
- система управления открытыми ключами.

Система ЭДО используется для передачи информации между приложениями торгово-расчетной инфраструктуры ЕТС.

Описание документа

Настоящий документ предназначен для потенциальных пользователей системы электронного документооборота ЕТС.

Цель документа – дать общее представление об архитектуре, принципах работы и возможностях использования ЭДО в системах обработки информации.

Общие сведения

Описание системы

С точки зрения конечного пользователя, система ЭДО представляет собой специализированную электронную почту, в которую встроены средства криптографической защиты информации и управления открытыми ключами.

Для защиты передаваемой информации от раскрытия и подлога в системе ЭДО используется сертифицированное программное обеспечение шифрования и электронно-цифровой подписи (ЭЦП).

Отличительной особенностью ЭДО от многих подсистем передачи сообщений, используемых в системах типа "Клиент-Банк" или "Клиент-Депозитарий", является возможность обмена сообщениями по принципу "каждый с каждым". Это обеспечивается системой договорных отношений между участниками, а также используемой системой распространения открытых ключей абонентов и обработки информации о выводе их из действия.

Пользователи ЭДО

Система ЭДО обеспечивает возможность обмена финансовыми документами между всеми участниками и субъектами расчетной инфраструктуры Биржи.

Рис. 1. Пользователи ЭДО.

Преимущества электронных документов

Современный уровень развития телекоммуникационных технологий делает неизбежным использование электронных документов в тех случаях, когда речь идет о сокращении расходов и снижении рисков при обмене юридически значимой информацией.

Использование ЭДО позволяет сократить расходы на:

- подготовку исходящих документов;
- передачу документов;
- ввод, проверку и обработку входящих документов.

Скорость обмена информацией в ЭДО не зависит от того, передаются ли документы внутри одного здания или между различными регионами страны. Сокращение времени на технологические операции в цикле исполнения сделок, связанные с обработкой документов, позволяет ускорить процесс заключения и расчета сделок, снизить издержки.

Электронная подпись, которой защищаются передаваемые документы, позволяет установить авторство электронного документа. Кроме того, никакие исправления не могут быть внесены в подписанный документ без нарушения целостности его ЭЦП.

Простота проверки ЭЦП и невозможность ее подделки позволят избежать риска подлога документов. Быстрота распространения открытых ключей новых абонентов и скорость отзыва ключей после окончания их использования существенно снижают риск несанкционированного использования криптографических ключей. Надежность алгоритмов шифрования и электронной подписи проверена их многолетним использованием в различных банковских системах, в том числе в Национальном Банке РК.

Юридическая сила ЭЦП

Согласно законодательству РК, документы в электронной форме, точно так же как и бумажные документы, считаются совершенными в простой письменной форме.

Для формирования ЭЦП и шифрования сообщений ЭДО использует программное обеспечение криптографической защиты информации Tumar CSP сертифицированный в Республике Казахстан на соответствие требованиям безопасности, установленными "СТ РК 1073 – 2007".

Право использования средств защиты информации предоставляется пользователям системы ЭДО, подписавшим с ЕТС договор на информационно-техническое обслуживание. Пользователями ЭДО могут быть и государственные организации, и коммерческие предприятия, связанные с ними договорными обязательствами.

Необходимость подключения к ЭДО

Начало эксплуатации системы ЭДО является важным этапом в развитии ЕТС как торгово-расчетной системы, так как создана база для внедрения новых технологий:

- Центр электронных договоров;
- Расчеты по схеме "поставка против платежа";
- Торговля с предварительным депонированием.

Использование системы ЭДО позволяет отказаться от использования бумажных документов при совершении сделок купли-продажи товаров, включая оформление сделок и проведение расчетов по заключенным сделкам.

Подключение к ЭДО предоставляет возможность участникам рынка использовать одну систему для обмена документами со всеми организациями, осуществляющими торговлю на Бирже ЕТС и расчеты с Клиринговым центром ЕТС.

Техническое описание

Основные понятия криптографии

Для защиты информации при передаче по телекоммуникационным каналам ЭДО использует алгоритмы криптографических преобразований, реализованные в сертифицированном программном продукте Tumar CSP.

Действие криптографических преобразований основано на использовании криптографических ключей – наборов данных, формируемых уникальным образом на базе случайной последовательности чисел. Существует два основных типа алгоритмов шифрования – симметричный и асимметричный. При использовании симметричного алгоритма шифрования отправитель и получатель должны использовать один и тот же криптографический ключ для шифрования и расшифрования, и существует проблема передачи этого ключа между двумя абонентами. Асимметричный алгоритм использует два ключа – один для шифрования, а другой для расшифрования. Один из этих ключей каждый пользователь должен хранить в тайне (этот ключ называется секретным), а другой ключ сообщает всем, с кем он собирается обмениваться сообщениями (открытый ключ). Если для шифрования с помощью асимметричного алгоритма используется открытый ключ, то для расшифрования – соответствующий секретный ключ и наоборот. Открытый и секретный ключи связаны между собой специальным математическим соотношением, которое позволяет проверить принадлежность открытого ключа соответствующему секретному ключу, но не позволяет вычислить значение секретного ключа по значению открытого. Преимущество асимметричного алгоритма в том, что он позволяет передавать открытые ключи по каналам связи, но, с другой стороны, ввиду сложности алгоритма скорость работы программ на его основе значительно ниже, чем программ на основе симметричного алгоритма.

Для шифрования в программном продукте СКЗИ Tumar CSP используется схема симметричного алгоритма шифрования с открытым распределением ключей, что позволяет сочетать скорость работы симметричного алгоритма и удобство распределения ключей. Для зашифрования электронного документа отправитель использует производный ключ, который получается с помощью математического преобразования секретного ключа отправителя и открытого ключа получателя. Для расшифрования сообщения получатель использует тот же производный ключ, который получает с помощью своего секретного ключа и открытого ключа отправителя. Для каждой пары отправителя и получателя производный ключ будет уникальным.

Принцип работы ЭЦП основан на асимметричном алгоритме шифрования. ЭЦП – это последовательность данных, формируемых из отправляемого электронного сообщения с

помощью специального алгоритма шифрования с использованием секретного ключа отправителя и передаваемая вместе с этим сообщением. Проверить ЭЦП может любой абонент, имеющий открытый ключ пользователя, подписавшего документ. Открытый ключ ЭЦП выполняет роль своего рода аналога "карточки с образцом подписи".

Устойчивость криптографических алгоритмов к "взлому" (подбору секретного ключа) определяется математическими свойствами используемых функций. Длина ключа такова, что для его поиска методом перебора потребуются сотни лет на ЭВМ существующей мощности.

Архитектура ЭДО

Структурно система состоит из Центра ЭДО, расположенного на бирже ЕРТС и почтовых серверов - Мэйлбоксов, установленных в локальных сетях абонентов ЭДО.

В функции Центра ЭДО входит хранение сертификатов открытых ключей, проверки действительности сертификатов всех проходящих через него сообщений и заверения их с помощью ЭЦП (подробнее об управлении ключами см. п. 3.3.), а также поддержание системного времени.

Мэйлбокс выполняет функции передачи сообщения Мэйлбоксам других абонентов, взаимодействует с Центром ЭДО и приложениями конечных пользователей. Сообщения от одного Мэйлбокса к другому передаются напрямую без промежуточного хранения в Центре ЭДО (подробнее - см. п.0.).

Приложения подключаются к ЭДО через Мэйлбокс. К одному Мэйлбоксу может быть подключено любое количество приложений.

Взаимодействие приложения и почтового сервера происходит по протоколу, реализованному в программном интерфейсе (API), который представляет из себя динамически загружаемую библиотеку Windows (dll). Если вызовы dll не могут быть встроены в приложение, то можно воспользоваться интерфейсом обмена сообщениями через файловую систему с помощью файлового шлюза.

Передача сообщений

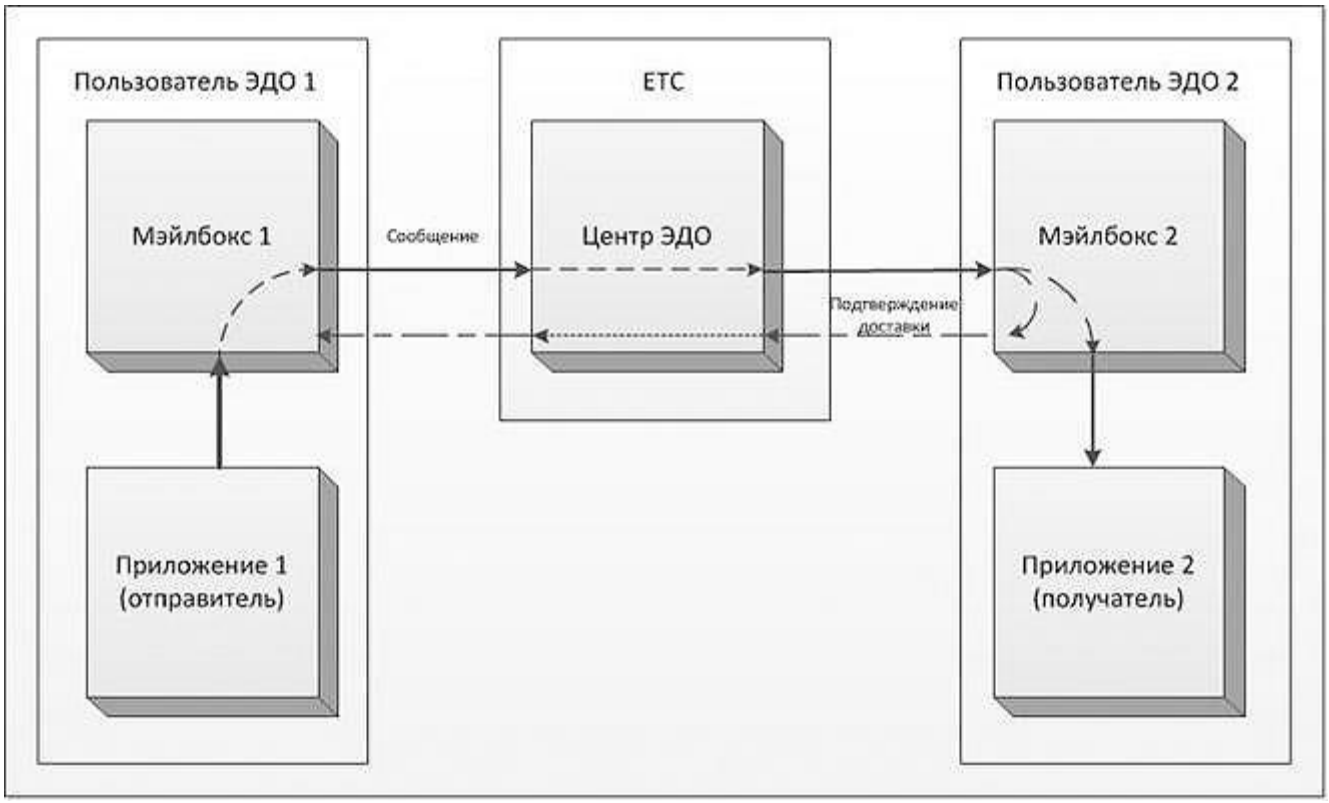

Рис. 2. Схема передачи сообщений.

На приведенной диаграмме изображен процесс передачи документа от одного приложения к другому через систему ЭДО. При приеме сообщения, Мэйлбокс получателя автоматически формирует и передает через Центр ЭДО отправителю подтверждение о доставке документа. Подтверждение доставки содержит ЭЦП Мэйлбокса получателя и заверяется Центром ЭДО и при необходимости позволяет отправителю доказать, что сообщение было доставлено. До тех пор, пока Мэйлбокс отправителя не получит это уведомление, сообщение не считается доставленным, и через некоторый интервал времени попытка отправления повторяется. Таким образом реализуется гарантированная доставка, т. е. отправитель не считает сообщение отправленным до тех пор, пока не получит уведомление о доставке.

Управление ключами

Ключи первичной инициализации для начала работы абонента с Удостоверяющим центром, в том числе для их замены на криптографические ключи электронной цифровой подписи, может быть сформирована менеджером биржи ЕТС или самостоятельно абонентом.

Распространение информации об открытых ключах подписи и шифрования абонентов реализовано с помощью механизма сертификатов. На этапе подключения к ЭДО организации заменяет ключи первичной инициализации в УЦ на криптографические ключи ЭЦП и оповещает об этом Биржу, если абонент самостоятельно создает ключи он предоставляет в ЕТС информацию об открытом ключе, на основании которого ЕТС формирует электронный сертификат этого ключа и помещает его в базу данных Центра ЭДО.

Программное обеспечение Мэйлбокса или приложения посылает запрос на сертификат в Центр ЭДО каждый раз, когда необходимо получить информацию об открытом ключе какого-либо абонента. Для минимизации количества обращений к Центру ЭДО полученные сертификаты хранятся в локальной базе данных Мэйлбокса и приложения.

Если организации необходимо вывести свой ключ из обращения, то она направляет в ЕТС бумажный документ на отзыв открытого ключа или отзывает его через Web портал УЦ https://ca.kisc.kz/.

Все сообщения, проходящие через Центр ЭДО, проверяются на то, что сертификаты всех открытых ключей, использованных в данном сообщении, действительны, после чего сообщение заверяется ЭЦП Центра ЭДО с указанием времени прохождения сообщения. Подпись Центра ЭДО под сообщением означает, что все сертификаты, указанные в заголовке сообщения были действительны на момент прохождения этого сообщения через Центр ЭДО.

Преимущества

По сравнению с другими системами защищенной передачи электронных сообщений ЭДО обладает уникальным набором технических характеристик:

- высокая степень защищенности;
- невозможность использования выведенных из действия ключей после того, как факт вывода ключа из действия зарегистрирован в системе;
- наличие развитой системы управления открытыми ключами, позволяющей взаимодействие между пользователями системы по принципу "каждый с каждым";
- передача сообщений без промежуточного хранения в центре;
- "технологичность" в эксплуатации и обслуживании;
- открытый API для интеграции приложений с системой ЭДО.

Технические требования

Сеть электронного документооборота ЕТС строится с использованием тех же каналов связи, которые используются для подключения Рабочих станций ЕТС. Все, что нужно участнику ЕТС для подключения к ЭДО, - это персональный компьютер с Windows NT/2000 и подключенный к сегменту сети, имеющему выход в ЕТС, например, к тому же сегменту, где установлены Рабочие станции ЕТС. Возможно подключение через каналы интернет.

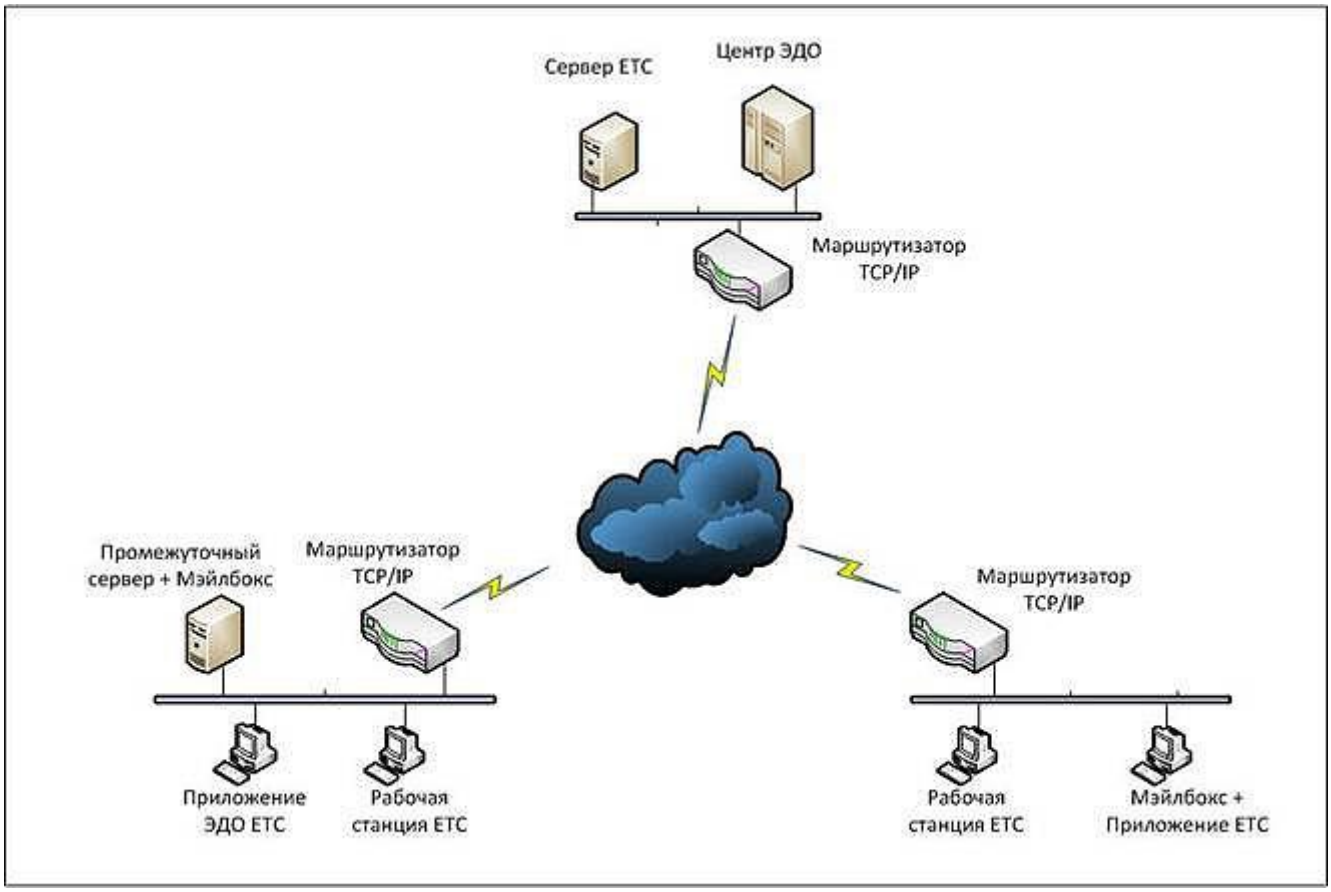

Рис. 3. Схема подключения.

Почтовый сервер может быть установлен на одном ПК с Рабочей станцией или Промежуточным сервером ЕТС. Приложение ЭДО, взаимодействующее с Мэйлбоксом, может так же работать с ним на одном ПК.

В Условиях оказания услуг информационно-технического обеспечения ЕТС оговорены требования по информационной безопасности, которые должен выполнять Участник ЭДО. Выполнение этих требований является ответственностью Участника. Требования определяют необходимость выполнения организационных и технических мер по защите секретных ключей и программного обеспечения от несанкционированного использования.