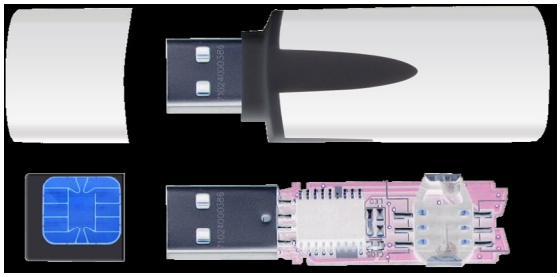
USB-токен «iBank 2 Key».

Хранения секретных ключей ЭЦП в файлах к использованию аппаратного криптопровайдера в виде USB-токена «iBank 2 Key».



USB-токен объединяет в компактном пластиковом корпусе PC/SC-совместимый USB-картридер и SIM-карту на базе микроконтроллера ST19NR66 производства компании STMicroelectronics.

В микроконтроллере SIM-карты при производстве масочным методом «прошита» карточная операционная система российского разработчика «Терна СИС». В составе карточной операционной системы содержится средство криптографической защиты информации «Криптомодуль-С», сертифицированное ФСБ РФ. Сертификат № СФ/114-1436 от 09.03.2010г.

Главное достоинство USB-токена «iBank 2 Key» – **формирование ЭЦП клиента под документом по российскому криптографическому алгоритму согласно ГОСТ Р34.10-2001 непосредственно внутри SIM-карты токена.**

На вход USB-токена передается электронный документ, а на выходе токена – ЭЦП под документом. При этом секретный ключ ЭЦП генерируется самим токеном при инициализации, хранится в защищенной памяти токена и никогда, никем и ни при каких условиях не может быть считан из токена.

Кроме функций генерации ключей ЭЦП, формирования и проверки ЭЦП в USB-токене «iBank 2 Key» реализованы функции шифрования по ГОСТ 28147-89, вычисления хеш-функции по ГОСТ Р34.11-94, аппаратной генерации случайных чисел. Доступ ко всем криптографическим функциям USB-токена предоставляется только после ввода корректного PIN-кода токена.

В системе электронного банкинга «iBank 2» встроена поддержка USB-токенов «iBank 2 Key». Работа USB-токена обеспечена для настольных платформ Microsoft Windows 2000/XP/2003/Vista, Linux и MacOS.

В одном USB-токене могут храниться до **64-х** секретных ключей ЭЦП, поддерживается хранение и работа секретных ключей ЭЦП разных ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank 2».

Описание на изделие “**ActivIdentity OTP-токен”** модель “**Mini Token”, версия АТ**.

1 Общая информация об изделии.

OTP-токен – аббревиатура для «One-Time Password токен»- токен для генерации одноразовых паролей. OTP токен (далее просто токен) используется для аутентификации пользователей в программных приложениях.

Производитель:	ActivIdentity, Inc. **(США)**
Адрес:	6623 Dumbarton Circle Fremont, CA 94555 United States
Телефон:	+1 (510) 574 0100
Веб:	http://www.actividentity.com
Электронная почта:	info@actividentity.com

2 Комплектация (состав) изделия

Общие технические сведения об изделии	
Размер (ДхШхВ), мм	45x38x11
Масса, г	25
Время жизни встроенной батареи, лет	6
Размер ЖК-экрана, символов	8
Водонепроницаемость, м	1
Требования к эксплуатации	
Рабочая температура	0° - +50°C
Температура хранения	-10° -+50°C

Изделие моделей “**Mini Token”**поставляется в отдельной упаковке, не требует никаких действий по подготовке к работе со стороны пользователя и полностью готовок эксплуатации.

3. Органы индикации, управления и программирования

Внешний вид изделия модели “Mini Token” представлен на Рисунке 1. 8-символьный LCD-дисплей

Рисунок 1. Внешний вид OTP-токена

Функциональная кнопка

Кольцо для ключей (брелка)

Уникальный идентификатор ОТР токена

Рисунок 2. Обратная сторона ОТР-токена

На лицевой стороне устройства расположены функциональная кнопка и LCD-дисплей. При удерживании 2-х секунд функциональной кнопки изделие включается и отображает на LCD-дисплее одноразовый пароль. Длина пароля –8 цифр. Через 20 секунд после нажатия кнопки токен автоматически выключается.

С обратной стороны располагаются контакты для программирования токена, закрытые наклейкой, а также нанесена информация, идентифицирующая изделие — идентификатор изделия, номер партии, дата изготовления ОТР-токена. В токен встроены часы реального времени.

4. Описание устройства и руководство по использованию

ОТР-Токен «Mini Token»- это компактное и удобное устройство для аутентификации пользователя. Устройство является чрезвычайно простым в работе: при нажатии на функциональную кнопку токен активируется и на LCD-дисплее отображается одноразовый пароль, который можно вводить в используемое приложение. Для генерации одноразовых паролей используются следующие алгоритмы:

алгоритм с синхронизацией по событию и использованием DES/3DES для вычисления одноразового пароля

собственный патентованный алгоритм ActivIdentity с синхронизацией повремени и событию

ОТР-токен программируется производителем непосредственно на заводе-изготовителе. При стандартной инициализации в каждый ОТР-токен программируется уникальный идентификатор и секретный ключ ОТР-токена. Также уникальный идентификатор ОТР-токена наносится непосредственно на сам ОТР-токен на обратной стороне в виде алфавитно-цифровой последовательности и штрих-кода.

Продавец или дистрибьютор может самостоятельно провести или изменить стандартную инициализацию ОТР-токена с помощью внешнего программатора, подключаемого к технологическому разъёму на обратной стороне токена. Предварительно необходимо удалить заглушку разъёма.

SMS Банкинг

Услуга предназначена для оперативного информирования Вас о состоянии Ваших счетов, подключенных к системе «iBank 2», путем направления sms-сообщений и/или уведомлений по электронной почте.

Предоставленные возможности мониторинга являются дополнительным инструментом обеспечения Вашей финансовой безопасности. Услуга позволяет Вам незамедлительно получать информацию о движении средств по счетам, получать сведения о случаях доступа к системе «iBank 2»

Клиент может самостоятельно настраивать и получать следующие типы сообщений:

Об отвержении исходящего документа.

Банк отправляет клиенту сообщение с указанием типа, номера, даты, суммы и причины отвержения документа.

О входящем банковском письме.

Банк отправляет сообщение с указанием темы письма.

О движении средств по счету.

Банк отправляет сообщение с указанием основных реквизитов операции – номера счета, суммы, даты и номера документа, реквизитов плательщика/получателя, назначения платежа.

О входе в систему «iBank2».

В начале каждого сеанса работы в Internet-Банкинге, а также при каждой синхронизации PC-Банкинга Банк направляет клиенту сообщение с наименованием сервиса, идентификатором ключа ЭЦП и параметрами подключившегося пользователя.

Текущие остатки по расписанию

Клиент может настроить и получать по расписанию (например, каждый день в 9 часов утра) сообщение о текущих остатках на своих счетах.

Выписка по расписанию

Клиент может настроить и получать по расписанию выписку об операциях по каждому своему счету.

Перечень событий и условий, производимых со счетом, о которых Вы желаете получить информацию, а также номера телефонов и адреса электронной почты, на которые Банку следует направлять данную информацию, указываются Вами самостоятельно в системе «iBank2». Зарегистрировать в системе Вы можете любое количество мобильных телефонов.

Система характеризуется высокой надежностью и безопасностью. В серверных модулях SMS-Банкинга используются сертифицированные ФСБ РФ криптобиблиотеки, осуществляется шифрование и обеспечение целостности передаваемых данных.

Инструкция по настройке SMS уведомлений в IBank2

1. Возможности Клиента по тонкой настройке уведомлений

Система IBank 2 позволяет рассылать уведомления о событиях в системе на мобильный телефон в формате SMS с помощью канала обслуживания SMS - Банкинг. Настройка рассылки уведомлений осуществляется с помощью категории *Мониторинг* дерева документов АРМ РС-Банкинг для корпоративных клиентов.

1.1. Настройка каналов доставки сообщений

Для настройки каналов доставки сообщений выберите пункт Каналы доставки категории Мониторинг дерева документов (см. рис. 1.1.).

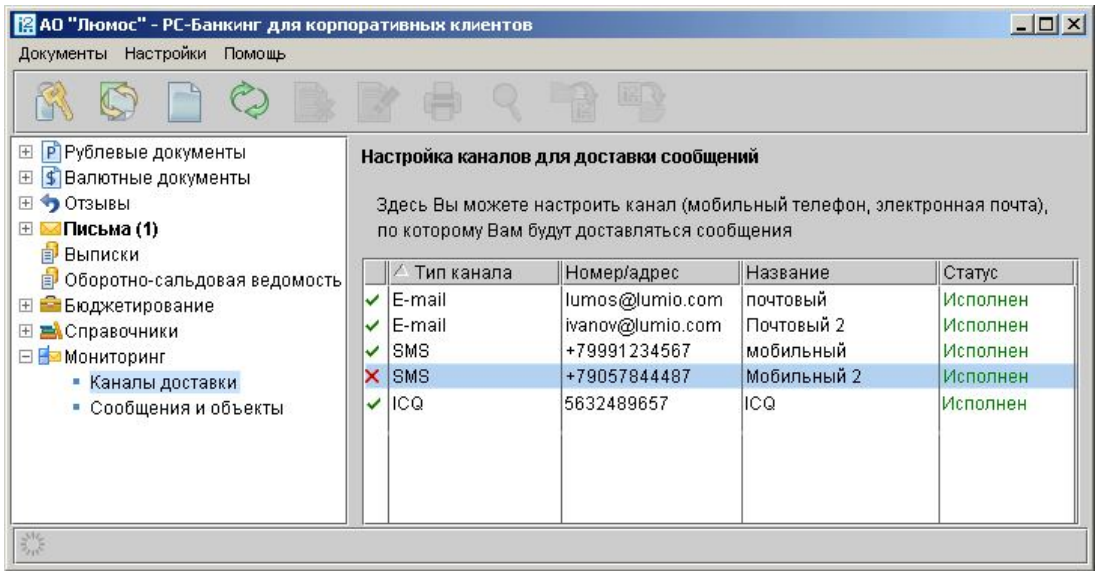


Рис. .1.1. Список каналов доставки сообщений

Создание канала доставки сообщений

Для создания канала доставки вызовите контекстное меню правой кнопкой мыши и выберите пункт Новый. В открывшемся окне *Настройка канала* выполните следующие действия:

- С помощью списка поля *Тип канала* выберите вид канала (SMS).
- Для доставки по SMS введите номер мобильного телефона в международном формате (например, +79164563289) в поле *Телефон* (см. рис. 1.2).
- Введите название, под которым канал доставки будет отображаться в списке, в поле *Название*.
- Выберите язык, на котором будут приходить уведомления, с помощью списка поля Язык. Если необходимо присылать русские сообщения в латинской транслитерации, проставьте метку в поле транслитерация.
- Для сохранения создаваемого канала нажмите кнопку Сохранить.

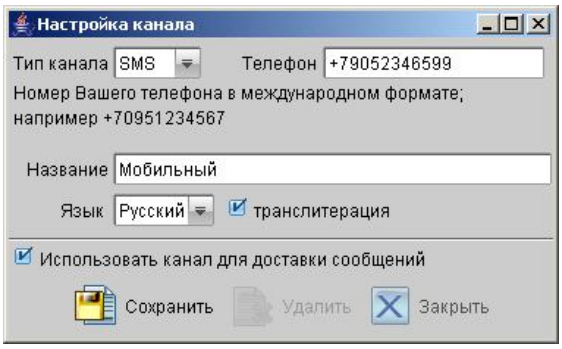


Рис. 1.2. Создание SMS-канала доставки сообщений

Сохраненный канал доставки имеет статус *Подписан*. После проведения синхронизации канал получит статус *Исполнен*.

Управление каналами доставки сообщений

Для редактирования параметров канала доставки сообщений выполните одно из следующих действий:

- выберите в списке требуемый канал и дважды щелкните по нему левой кнопкой мыши;
- выберите в списке требуемый канал, правой кнопкой мыши вызовите контекстное меню и выберите пункт *Редактировать*.

Редактирование параметров канала доставки сообщений производится в окне *Настройка* канала аналогично процедуре создания канала.

Клиент может включать и отключать канал. Для этого либо воспользуйтесь пунктом *Вкл./Выкл.* контекстного меню, либо проставьте метку в поле Использовать канал для доставки сообщений окна *Настройка* канала. По отключенным каналам рассылка сообщений не производится. Отключенные каналы в списке отмечаются красным крестом.

Клиент может удалить канал доставки. Для этого воспользуйтесь пунктом *Удалить* контекстного меню или кнопкой  *Удалить* окна *Настройка* канала. При удалении канала доставки созданные для него рассылки также удаляются.

1.2. Настройка рассылки сообщений

Для настройки рассылки сообщений выберите пункт *Сообщения* и объекты категории Мониторинг дерева документов (см. рис .2.1).

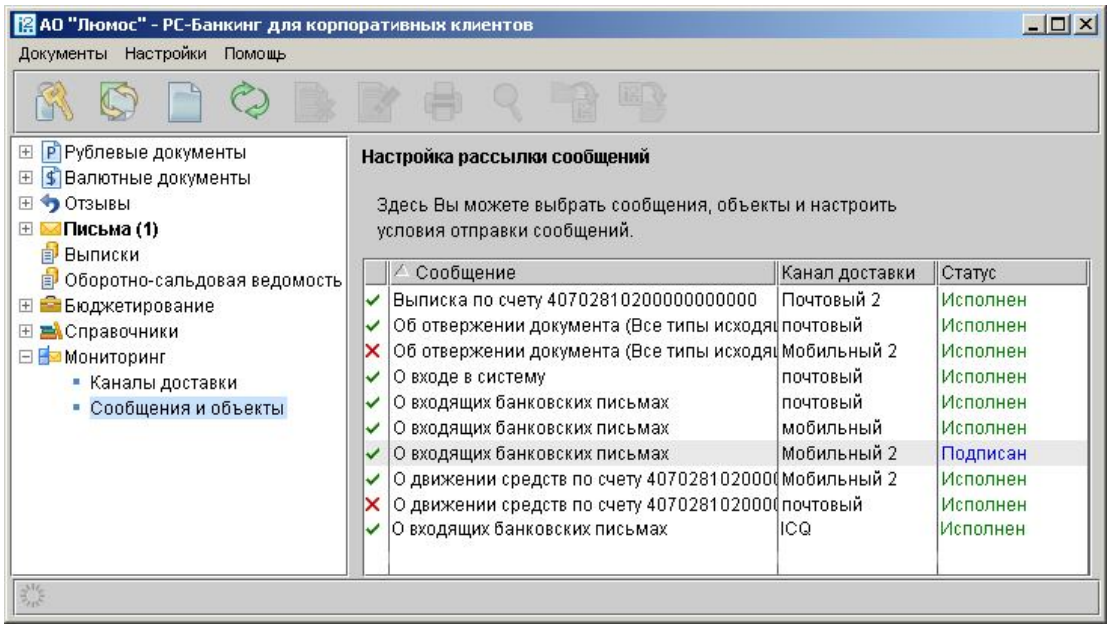


Рис. 2.1. Список рассылок уведомлений

Создание рассылки уведомлений

Для создания рассылки уведомлений вызовите контекстное меню правой кнопкой мыши и выберите пункт *Новый*. В открывшемся окне выполните следующие действия:

- На первом шаге выберите канал доставки с помощью списка поля Канал доставки (см. рис. 2.2.).

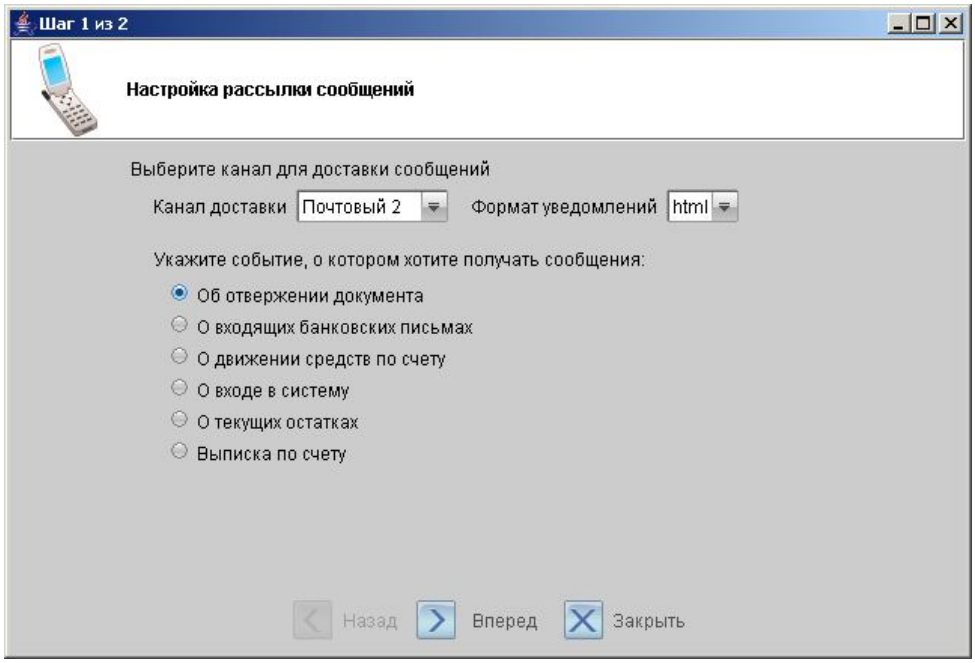


Рис. 2.2. Шаг 1 создания рассылки уведомлений

Выберите тип уведомления:

- Об отвержении документа;
- О входящих банковских письмах;
- О движении средств по счету;
- О входе в систему;
- О текущих остатках;
- Выписка по счету.

Для перехода к следующему шагу нажмите кнопку *Вперед*.

- На втором шаге осуществляется окончательная настройка параметров рассылки для каждого ее типа (см. рис. 2..3).

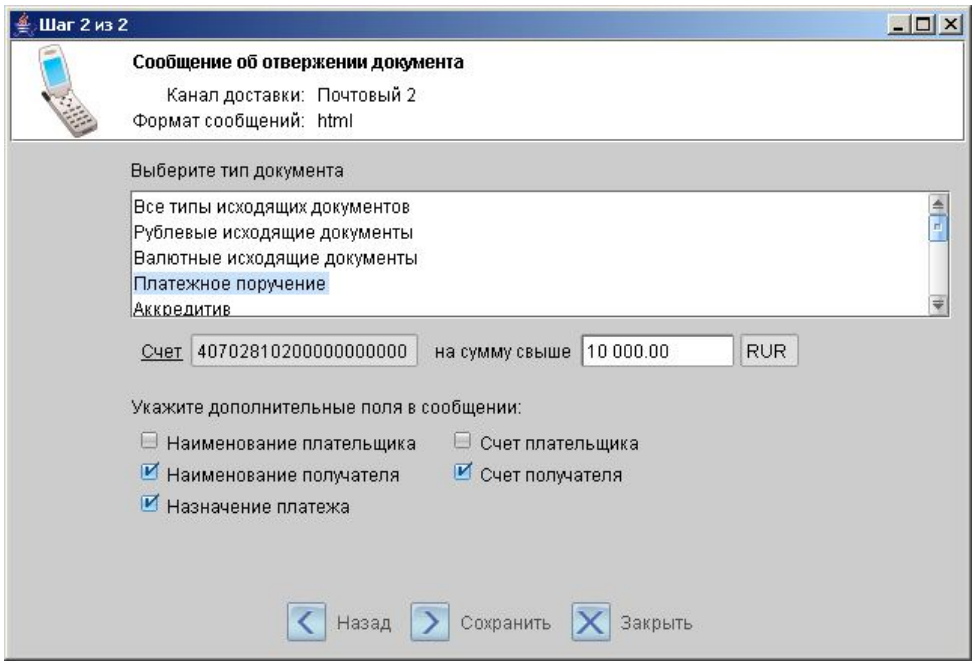


Рис. 2..3. Шаг 2 создания рассылки уведомлений

- Для уведомления об отвержении документа выберите тип документа, об отвержении которого посылается уведомление. Выберите счет, который используется при создании документа (например, счет списания для платежного поручения, счет зачисления для платежного требования и т.д.), с помощью ссылки *_счет*. Введите минимальную сумму в валюте выбранного счета, начиная с которой будет создаваться уведомление. Для каждого типа документа можно указать поля отвергнутого документа, которые будут приведены в уведомлении. Для этого проставьте метки в полях с названиями соответствующих полей.
- Для уведомления о входящих банковских письмах проставьте метки в полях *Тема письма* и *Референс* при необходимости включить содержимое данных полей в текст уведомления.
- Для уведомления о движении средств по счету выберите счет, по которому происходит движение средств, с помощью ссылки *счет*. Выберите тип операции (списание, зачисление или все операции) с помощью списка поля *Тип операции*. Введите минимальную сумму в валюте выбранного счета, начиная с которой будет создаваться уведомление. Для включения полей документа, согласно которому происходит движение средств по счету, в текст уведомления проставьте метки для соответствующих полей документа.
- Для уведомления о входе в систему проставьте метки в полях ФИО сотрудника, ID ключа и Наименование организации при необходимости включить содержимое данных полей в текст уведомления.

– Для уведомления о текущих остатках выберите счет по ссылке *Счет* и укажите время, в которое каждый рабочий день будет отправляться уведомление (часы и минуты).

– Для получения выписки выберите счет по ссылке *Счет* и укажите, за какой день (текущий или предыдущий) посылать выписку. Задайте время, в которое каждый рабочий день будет отправляться уведомление (часы и минуты).

Нажмите кнопку *Сохранить* для сохранения рассылки. Сохраненная рассылка имеет статус *Подписан*. После проведения синхронизации рассылка получит статус *Исполнен*.

Управление рассылками уведомлений

Для редактирования параметров рассылки уведомлений выполните одно из следующих действий:

- выберите в списке требуемую рассылку и дважды щелкните по ней левой кнопкой мыши;
- выберите в списке требуемую рассылку, правой кнопкой мыши вызовите контекстное меню и выберите пункт *Редактировать*.

Редактирование параметров рассылки уведомлений производится в окне, вид которого совпадает с окном Шага 2 создания новой рассылки (см. рис. 2..3). При редактировании рассылки канал доставки и тип рассылки менять нельзя.

Клиент может включать и отключать рассылку. Для этого воспользуйтесь пунктом контекстного меню *Вкл./Выкл.* Отключенные рассылки в списке отмечаются красным крестом.

Клиент может удалить рассылку уведомлений. Для этого воспользуйтесь пунктом *Удалить* контекстного меню.

Возможности SMS Банкинга:

1) Получение одноразового пароля

Для обеспечения безопасной аутентификации корпоративного клиента в системе, а также для предотвращения возможности использования похищенных ключей ЭЦП клиента в «iBank 2» может быть использован механизм многофакторной аутентификация клиента в системе.

Корпоративным клиентам с включенным механизмом «Многофакторная аутентификация» для входа в Internet-Банкинг, а также для синхронизации в РС-Банкинге необходимо будет дополнительно вводить в своих АРМ одноразовый пароль.

2) Система СМС Уведомления

Услуга оперативного информирования позволяет корпоративному клиенту незамедлительно получать информацию о движении средств по его счетам, получать сведения о случаях доступа к системе «iBank2». Предоставляемые клиенту возможности мониторинга являются дополнительным инструментом обеспечения финансовой безопасности клиента.

Клиент может получать следующие типы сообщений:

1. **Об отвержении исходящего документа.** Банк отправляет клиенту сообщение с указанием типа, номера, даты, суммы и причины отвержения документа.
2. **О входящем банковском письме.** Банк отправляет сообщение с указанием темы письма.
3. **О движении средств по счету.** Банк отправляет сообщение с указанием основных реквизитов операции – номера счета, суммы, даты и номера документа, реквизитов плательщика/получателя, назначения платежа.
4. **О входе в систему «iBank2».** В начале каждого сеанса работы в Internet Банкинге, а также при каждой синхронизации РС Банкинга Банк направляет клиенту сообщение с наименованием сервиса, идентификатором ключа ЭЦП и параметрами подключившегося пользователя.
5. **Текущие остатки по расписанию.** Клиент может настроить и получать по расписанию (например, каждый день в 9 часов утра) сообщение о текущих остатках на своих счетах.
6. **Выписка по расписанию.** Клиент может настроить и получать по расписанию выписку об операциях по каждому своему счету.