Банк Агророс

Система дистанционного банковского обслуживания

Многопользовательский режим работы

Имя идентифицирует пользователя - человека. Каждый человек входящий в систему ДБО должен использовать только своё личное имя. Пользователей системы ДБО создают сотрудники банка по заявлению клиента. Пароль пользователя удостоверяет принадлежность имени человеку. Пользователь может сам быть клиентом банка (иметь личные счета в банке) и распоряжаться счетами других клиентов (юридических и физических лиц). Ввод имени и пароля предоставляет пользователю ДБО доступ только к счетам физических лиц. Для доступа к счетам юридических лиц пользователю необходимо иметь личный сертификат и предъявить его при входе (подписать входную квитанцию). Сертификат обязательно должен соответствовать пользователю. Невозможно войти в ДБО с чужим сертификатом.

Сотрудник

Сертификат в браузере
только для входа в ДБО

Директор

Сертификат в токене
для входа в ДБО
и подписи документов

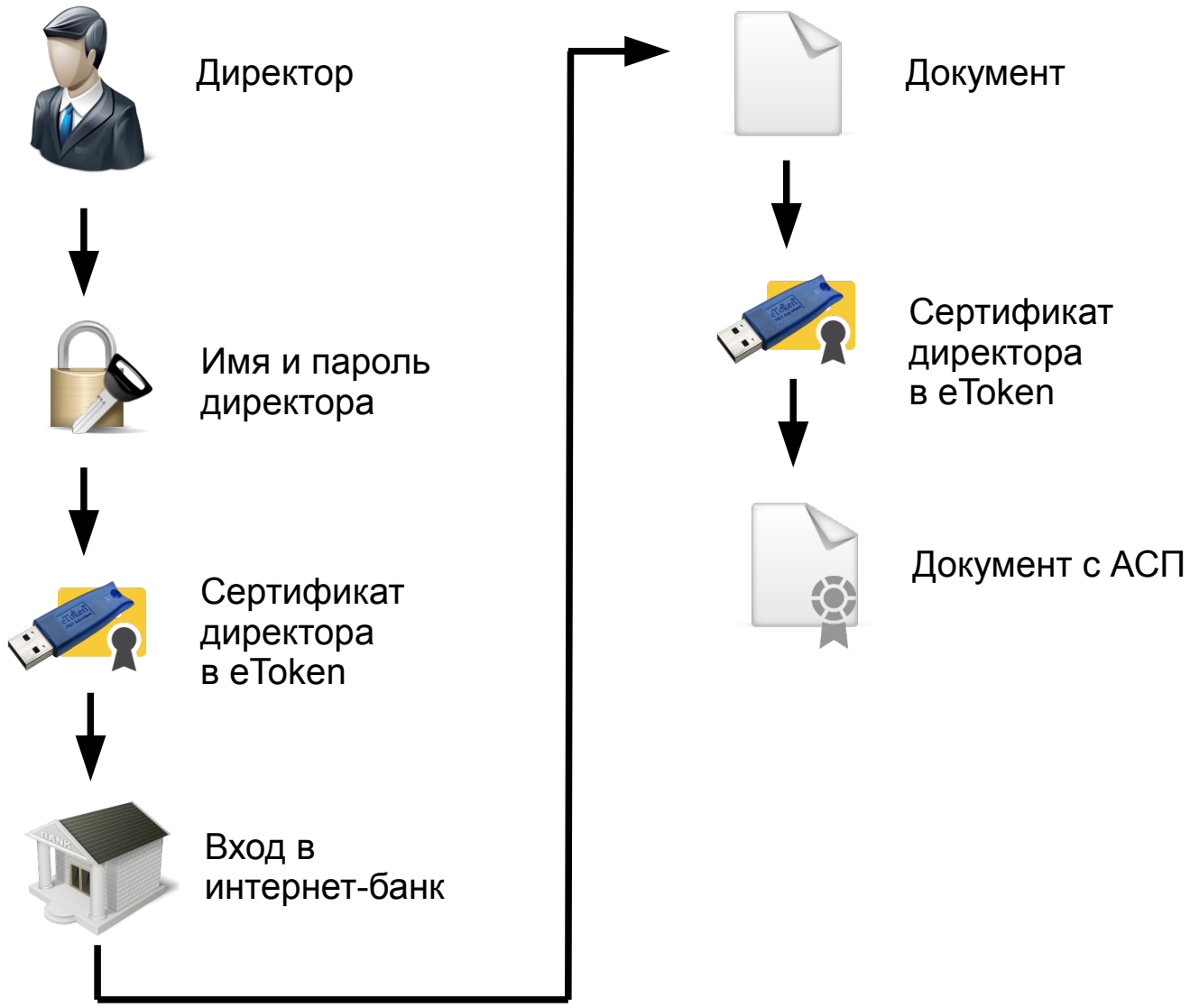
Сертификаты бывают двух видов - для входа и для подписи (универсальный). Сертификаты выдаются банком по запросу пользователя и содержаться в хранилище сертификатов. Хранилищем может быть браузер (компьютер пользователя) или смарт-карта (токен eToken).

Сертификат для входа выдается по запросу пользователя отправленному со своего рабочего места. Сертификат для входа позволяет входить в ДБО, видеть счета юридических лиц, создавать документы но не позволяет подписывать документы.

Сертификат для подписи создается в токене. По желанию пользователя запрос на сертификат в токене может быть отправлен пользователем самостоятельно либо подготовлен сотрудниками банка. Сертификат для подписи позволяет входить в ДБО, видеть счета юридических лиц, а так же подписывать документы аналогом собственноручной подписи (АСП). Для доступа к сертификату хранящемуся в токене нужно вводить пароль токена.

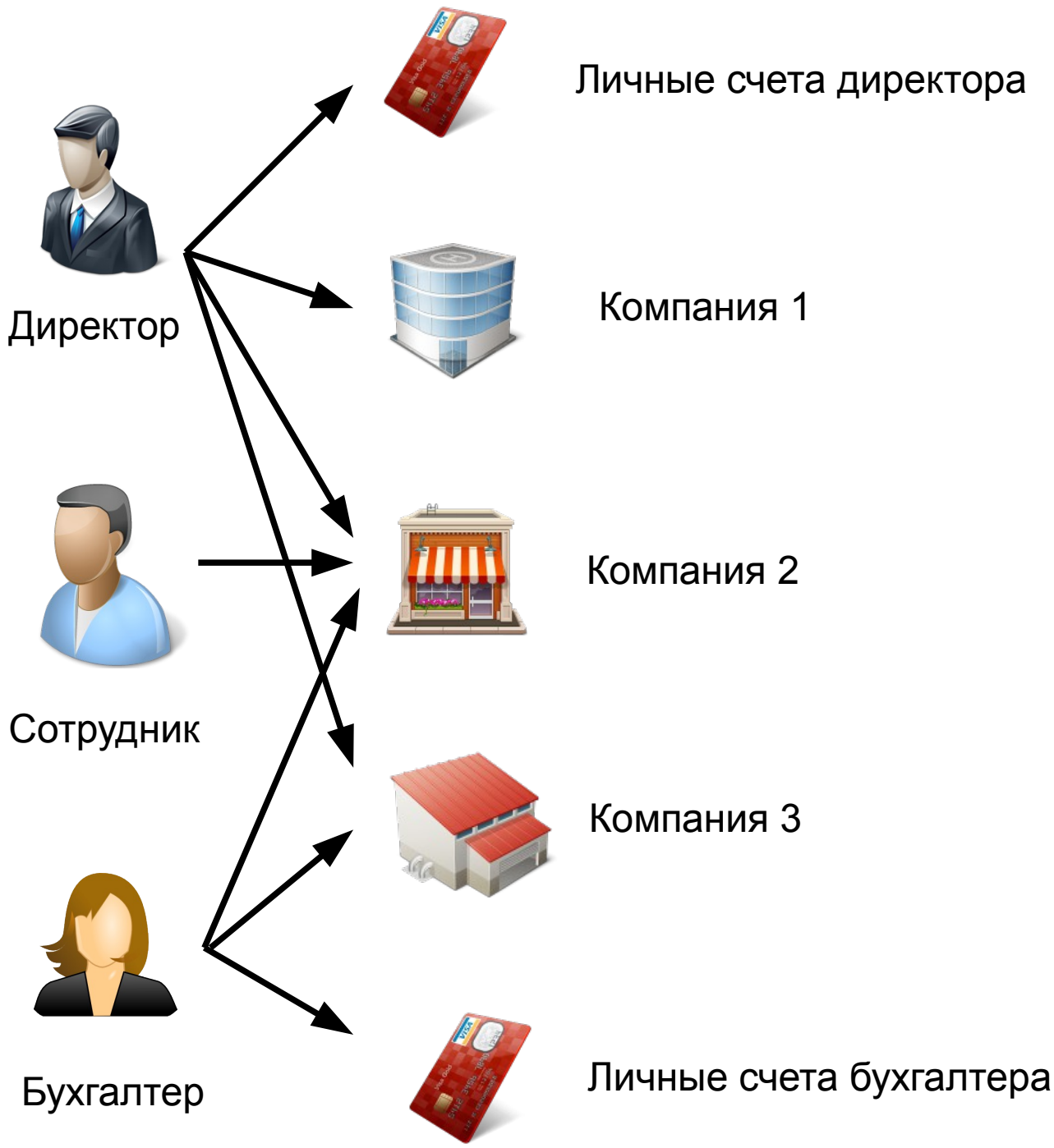
Вход в систему

Подписывание

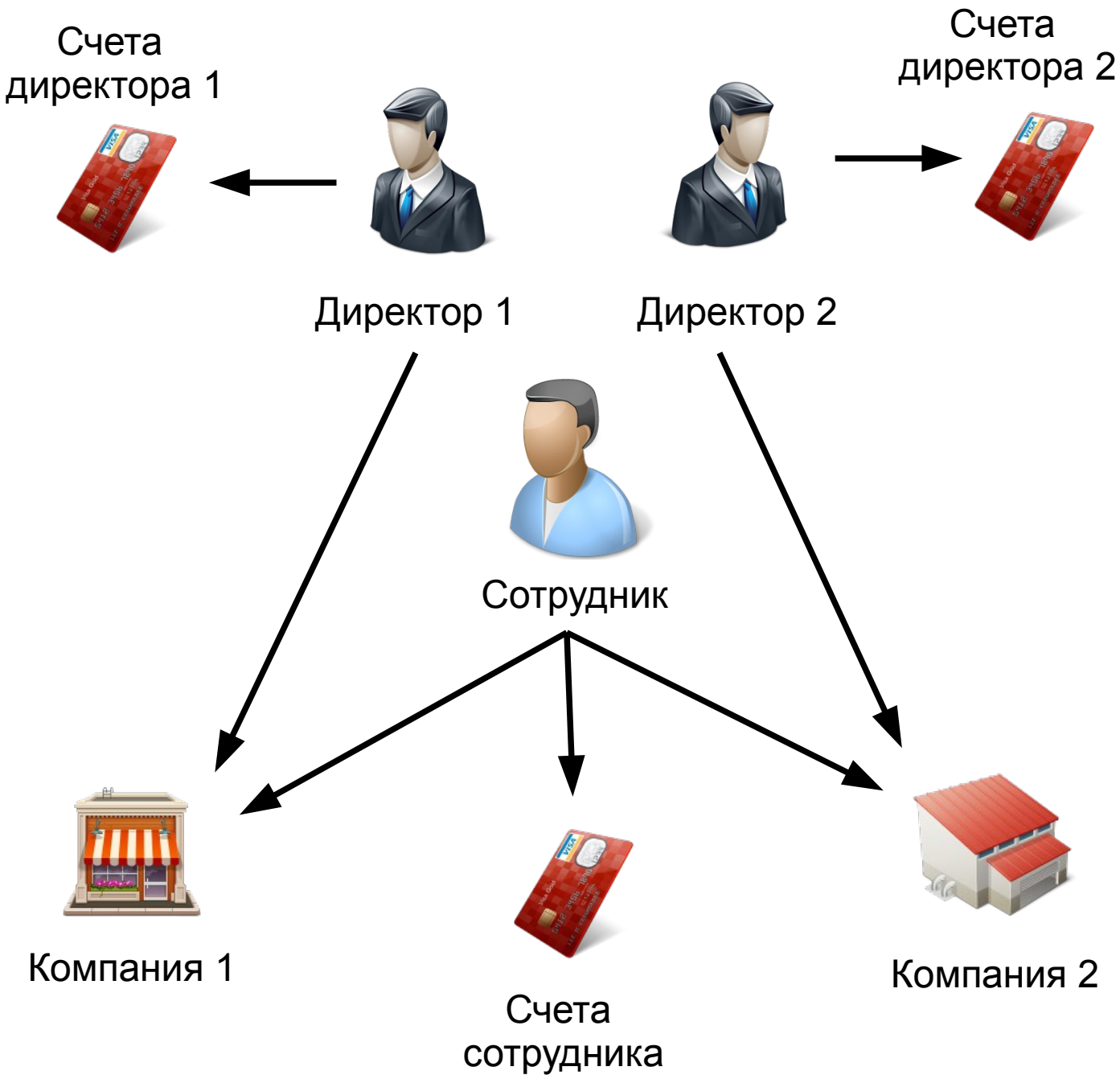


Пользователь с правом подписи (директор), вошедший в ДБО со своим сертификатом, имеет полный доступ к системе, видит счета всех клиентов, предоставленных ему в распоряжение, в том числе и свои личные счета. Может подписывать документы АСП.

Пользователь без права подписи (сотрудник), вошедший в ДБО со своим сертификатом, видит счета всех клиентов, предоставленных ему в распоряжение, может создавать новые документы, но не может их подписать. Для подписывания документов директор может подключить свой токен к компьютеру сотрудника, вести пароль токена и подписать документ. После чего токен можно отключить и сотрудник продолжит работу. Директор так же сможет подписать созданный сотрудником документ на своем рабочем месте, как описано на предыдущей странице. Кроме того, возможна временная передача токена и пароля на токен сотруднику. Использовать токен директора для входа сотрудник не сможет, так как не знает пароль директора. Извлечь (скопировать) сертификат из токена так же невозможно. Сотрудник сможет использовать токен только для подписи документов от имени директора и только до тех пор пока токен находится у сотрудника.



В ситуациях когда несколько пользователей связано с несколькими клиентами важно понимать какой доступ будет иметь каждый из пользователей. В данном примере директор без сертификата увидит только свои личные счета, с сертификатом дополнительно счета всех трех компаний. Бухгалтер без сертификата увидит только личные счета бухгалтера, с сертификатом - так же счета компаний 2 и 3 но не компанию 1. Сотрудник без сертификата не увидит никаких счетов, поскольку счетов физических лиц у него нет, он не является клиентом банка. С сертификатом сотрудник увидит только счета компании 2, поскольку к другим клиентам доступ сотруднику не предоставлен.



Если один сотрудник ведет счета нескольких компаний есть несколько путей для организации работы. Во-первых, директора лично могут подписывать созданные сотрудником документы. Во-вторых, директора могут передать токены и пароли на них сотруднику. В этом случае сотрудник сможет подписывать документы каждой из компаний от имени каждого из директоров соответственно, но сами директора лишаться возможности видеть счета подчиненных компаний. Без находящихся в токенах сертификатов директора увидят только свои личные счета. Сотрудник, даже имея токены директоров, не увидит их личные так как не знает пароли на вход. В-третьих, каждый из директоров может дать сотруднику доверенность на «управление счетом в электронном виде».

Если организация работы компании требует обязательного участия в отправке документов двух первых лиц, то система ДБО может быть настроена на использование двух (и более) аналогов собственноручной подписи. На схеме сотрудник без права подписи создает документ. Директор и бухгалтер собственными сертификатами (со своих рабочих мест) подписывают документ. Банк примет документ только после получения двух подписей. Передача токенов между пользователями в данной ситуации технически возможна но не имеет смысла, поскольку две подписи разными людьми нужны для независимого контроля за отправкой документов. Если фактически отправку выполняет один человек, то достаточно одного АСП.

Директор может дать сотруднику доверенность на «управление счетом в электронном виде». Это позволит сотруднику получить личный сертификат для подписи документов и использовать собственный аналог собственноручной подписи (АСП). При этом каждый из директоров сохраняет право подписывать документы своей компании. То есть АСП директора и сотрудника будут равнозначны. Доверенность не дает право сотруднику подписывать бумажные документы.