Обзор существующей технологии

Для входа пользователей в систему «ДЕЛа&ФИНансы» используется распространенный способ регистрации пользователя в программах: в диалоговом окне приложения он должен вводить имя и пароль, по этой паре значений система «понимает» кто входит в неё и какие права ему предоставить. Такая технология называется однофакторная идентификация.

У этой системы – ручной ввод имени и пароля есть слабое место: злоумышленник может узнать эту пару значений (подсмотреть или отследить с помощью специальных программ) и войти в систему под чужим именем с чужими правами и изменить документы, что бы скрыть следы преступления (как правило, кража наличных денег или товара). Разумеется, чаще всего кражи «провоцируются» неправильной организаций работы с документами, распределением ролей и прав доступа, и если организовать безопасную схему работы с документами и контроль, то можно избежать таких проблем. Те не менее за последние годы нашими заказчиками были выявлено несколько случаев изменения данных и краж денежных средств и товара с использованием чужих паролей (пользователей, кому по роду деятельности разрешено изменять документы).

Двухфакторная идентификация пользователей с помощью микропроцессорных карт (Смарт-карт).

После анализа различных технологий мы выбрали технологию, основанную на использовании микропроцессорных карт (Смарт-карт). Смарт-карты поддерживаются на уровне операционных систем и с ними можно работать даже при доступе к программе через сервер терминалов. Такие карты содержат микропроцессор, способный выполнять операции шифрования-дешифрования и защищенную файловую систему. Стандартная технология обмена информаций с такой картой позволяет передавать информацию от неё на сервер и обратно по открытым каналам связи. Это позволяет серверу определить, что это за карта и при этом не скомпрометировать ключи (то есть ни по каналам связи, ни в самом приложении использующем карту ключи шифрования для считывания информации хранящийся на карте не передаются). Дополнительно к этому, информация (файлы) на карте защищаются паролем (PIN кодом). После шести попыток подобрать пароль карта блокируется (в нашем случае она больше непригодна для использования). Создать дубликат карты (скопировать её) без знания системного ключа невозможно (у каждого нашего заказчика будет использоваться свой, уникальный системный ключ). Таким образом, для идентификации пользователя в системе потребуется две вещи: сама карта и PIN код для неё (отсюда и название метода двухфакторная).

Процесс регистрации пользователя в программе

Если для базы данных будет установлено свойство «Регистрация с использованием Смарт-карт». То программа проверит наличие считывателя, если его нет – выдаст сообщение и завершит работу. Если считыватель карт будет найден, то программа предложит вставить карту и ввести её PIN код. После этого программа начнет обмен информацией между сервером базы данных и картой. После того как сервер «опознает» карту в приложение от сервера придет информация о пользователе и его правах, если не «опознает» то сервер базы данных разорвет подключение с клиентским приложением. Регистрация в системе с использованием предыдущих версий программ (тех, которые не умеют работать со Смарт-картами, будет невозможна). Возможна «тонкая настройка», при которой некоторым пользователям можно будет входить без предъявления карты но это снизит защищенность системы.

Выпуск карт для пользователей программы.

Выпускать новые карты и управлять имеющимися картами (создание новых карт, перепрограммирование старых, привязка имеющейся карты к пользователю системы, изменение PIN кода карты) сможет пользователь, обладающий правами на режим «Настройка прав пользователей». Для этого в режиме «Настройка прав пользователей» добавлена новая функция «Создать карту». Для работы с этой функцией потребуется специальная карта «Мастер карта», которая содержит уникальную для каждого предприятия информацию, используемую для программирования остальных карт. Эта карта так же защищена своим PIN кодом. Система потребует у Администратора предъявить эту карту и ввести её PIN код. После этого он может создавать и перепрограммировать карты. Функция программирования карт проста и не требует сложных манипуляций.

Стоимость решения.

Эта технология предлагается как дополнительная опция и не входит в базовую поставку. Стоимость зависит от общего количества рабочих мест системы «ДЕЛа&ФИНансы» эксплуатируемой на всех подразделениях заказчика.

Количество рабочих мест	Стоимость модуля «Использование Смарт-карт для идентификации пользователей», руб.
1-10	10 000-00
11-30	20 000-00

31-50	30 000-00
50 и больше	50 000-00

Для работы со Смарт-картами на компьютерах пользователей потребуется установить считыватели. Стоимость таких устройств от 1200-00 до 1800-00 рублей за 1 шт.

Для каждого пользователя системы потребуется микропроцессорная карта. Стоимость одной карты 150 рублей.