



IDENIUM

Защита информации

**Система биометрической идентификации пользователей
корпоративных сетей и приложений**

BioLink



IDepiut: Назначение и функции



- **защита информации от несанкционированного доступа**
 - замена громоздких и уязвимых паролей
 - надежная и безопасная биометрическая идентификация при доступе в ОС и приложения, в том числе с помощью терминального входа

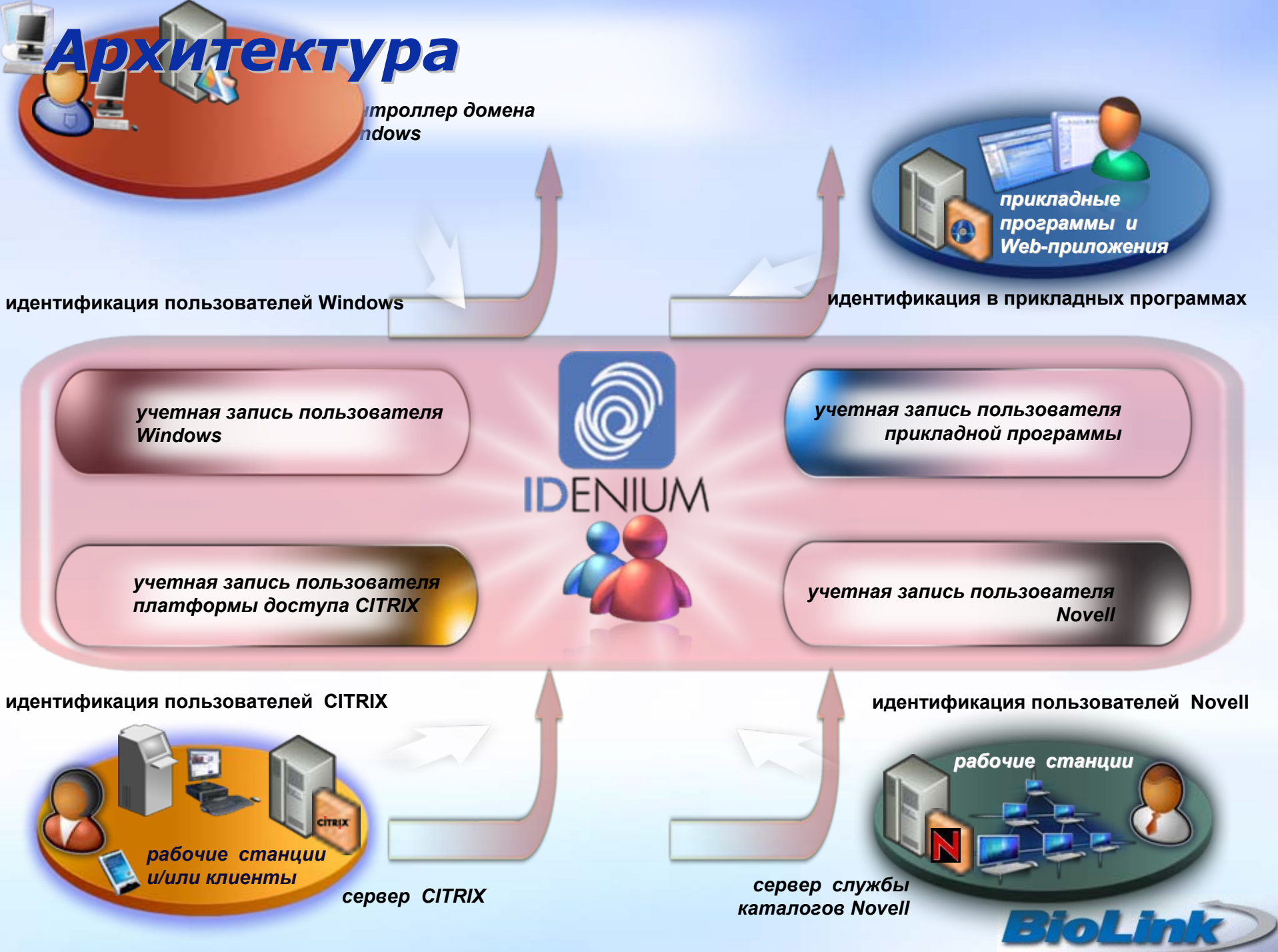


Назначение и функции



- **централизованное управление правами и полномочиями пользователей**
 - однократная регистрация
 - администрирование жизненного цикла учетных записей
 - отпечаток пальца — единый идентификатор для доступа в сеть, к прикладным программам, электронной почте, ресурсам Интернет
- **протоколирование событий доступа, мониторинг и аудит**

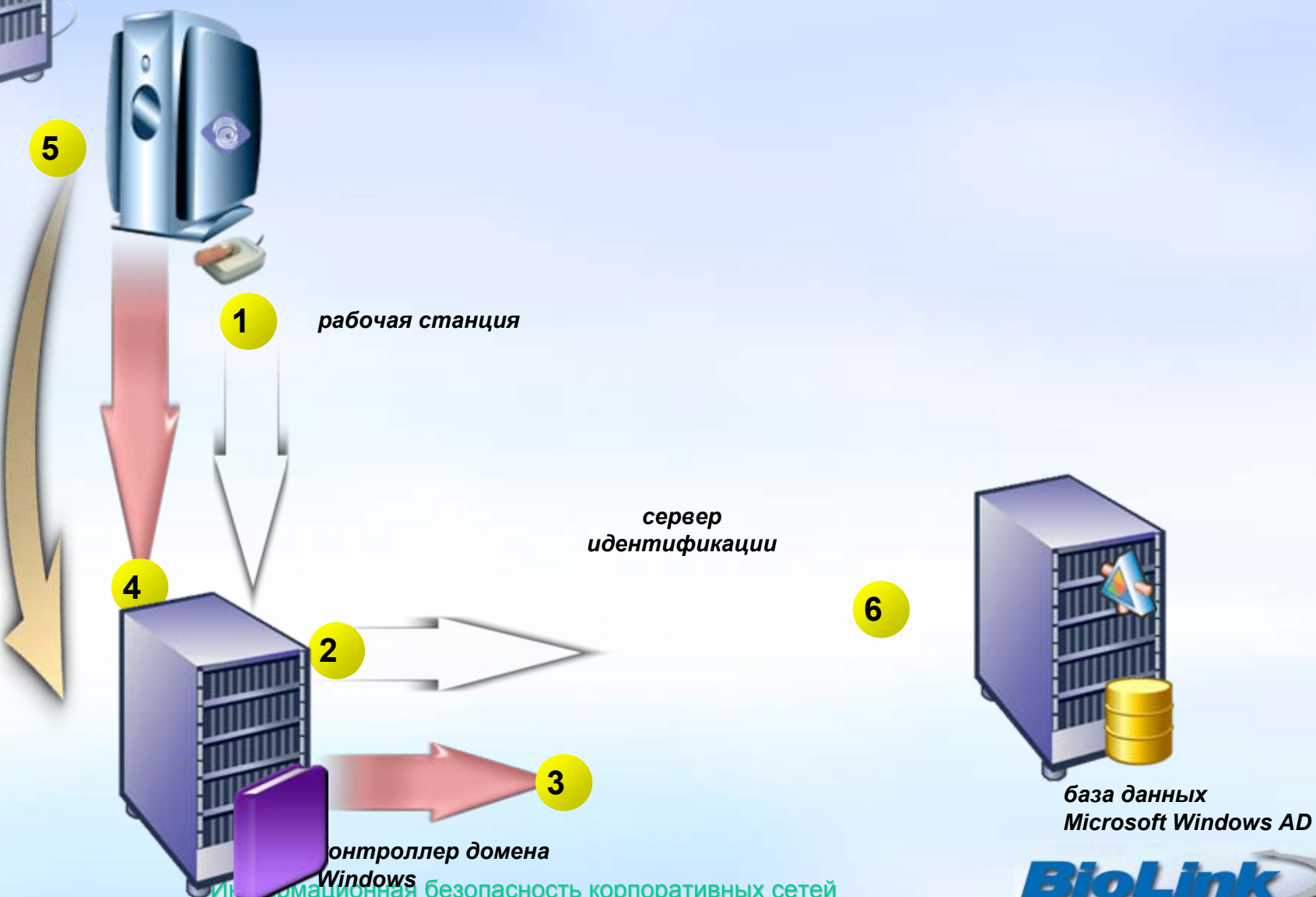
Архитектура



администрирование — синхронизация
информации между различными базами данных

3 4

for Active Directory





- **серверное программное обеспечение**
 - IDenium Server
 - синхронизатор паролей

- **клиентское программное обеспечение**
 - BioLink IDenium Admin Pack
 - BioLink Windows Logon
 - BioLink Password Vault **(NEW!)**
 - BioLink IDenium SDK



Denium Server



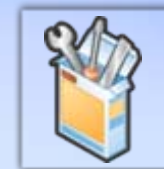
- обрабатывает запросы на идентификацию пользователей, получаемые от рабочих станций
- сравнивает цифровые модели вновь предъявляемого и ранее зарегистрированного отпечатка пальца пользователя
- создает ответные пакеты, содержащие учетные данные пользователя, инициировавшего запрос на идентификацию
- хранит в каталогах AD всю информацию, необходимую для идентификации пользователя операционной системы (включая цифровые модели отпечатков пальцев пользователей)

Синхронизатор паролей



- обеспечивает синхронизацию учетных данных пользователей, хранящихся в каталогах AD и на серверах BioLink IDenium
- должен быть установлен на каждом из контроллеров домена сети

BioLink IDenium Admin Pack



- развертывание компонентов управления IDenium на компьютере администратора сети
- регистрация/перерегистрация биометрических идентификаторов пользователей
- настройка политик идентификации, решение других административных задач
- при создании учетных записей новых пользователей их биометрические идентификаторы можно регистрировать централизованно, используя компьютер администратора



BioLink

Windows Logon



- проверяет подлинность (верифицирует) пользователя при входе в ОС
- передает информацию о пользователе, полученную в результате верификации и необходимую для аутентификации пользователя в ОС

Password Vault (**NEW!**)



- заменяет стартовое окно идентификации пользователя по имени и паролю в любом Windows приложении на идентификацию по отпечатку пальца
- возможность самостоятельной (пользовательской) записи сценариев входа в приложения
- редактирование сценариев входа в приложения администратором системы
- возможность импорта сценариев для централизованного назначения атрибутов доступа в приложение (например, импорт списка паролей в приложение из Excel файла)

BioLink **IDenium SDK**



- позволяет получить программный доступ к компонентам BioLink IDenium для глубокой интеграции механизма биометрической идентификации с разрабатываемыми пользователем прикладным ПО
- позволяет расширить схему AD для хранения в каталогах этой службы идентификационных параметров пользователей прикладных программ
- Позволяет использовать службы BioLink IDenium для регистрации и хранения биометрических данных, вызывая из прикладного ПО запрос на их проверку

Как действует BioLink IDenium



пользователь прикладывает палец к сканеру отпечатков

BioLink Windows Logon преобразует изображение отпечатка пальца в цифровую модель



IDenium Server сравнивает новую модель с ранее зарегистрированной и принимает решение об идентификации пользователя

Как действует BioLink IDenium



при положительном решении
об идентификации формируется пакет
с учетными данными пользователя



эти учетные данные поступают
из каталога AD, их актуальность
обеспечивает синхронизатор паролей



IDenium Server транслирует учетные
данные на рабочую станцию



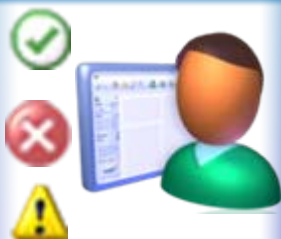
действует ink IDenium



BioLink Windows Logon передает учетные данные системе, инициировавшей запрос на идентификацию пользователя

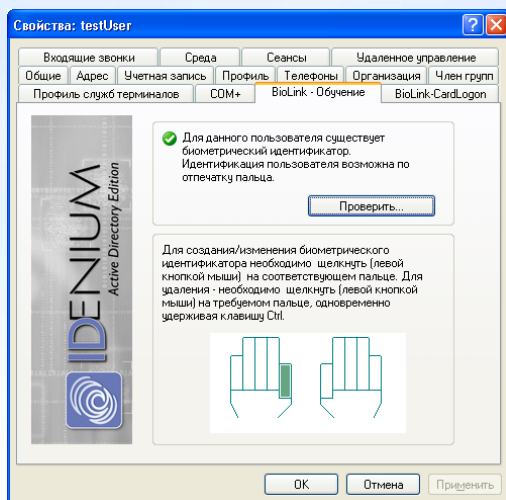


система получает сведения о пользователе в привычном для нее виде — как логин и пароль пользователя



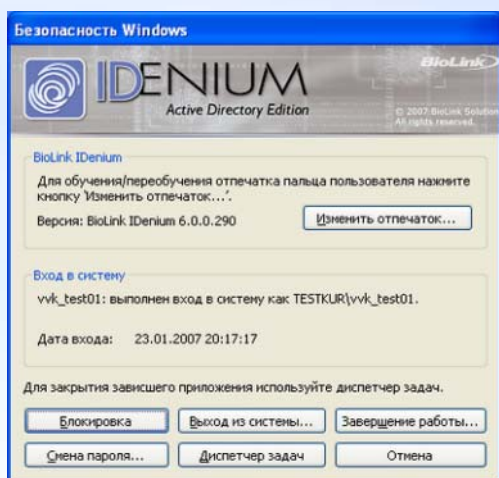
система в обычном для себя режиме проверяет идентичность пользователя и решает вопрос о предоставлении ему доступа к защищаемым ресурсам

Интеграция с Active Directory



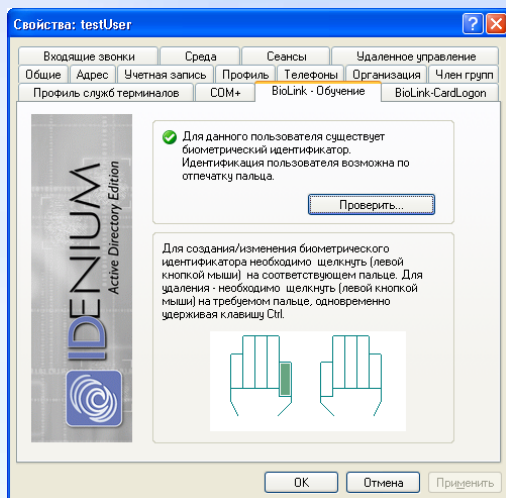
- ❑ централизованное хранение, защита и передача идентификационных данных пользователей средствами AD
- ❑ централизованное управление правами и полномочиями пользователей
- ❑ вкладки BioLink стандартной Microsoft Management Console оснастки Active Directory Users and Computers (ADUC)

Регистрация идентификаторов

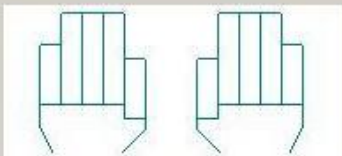


- **одновременно с созданием учетной записи пользователя в AD**
 - при найме нового сотрудника, в присутствии администратора и на его рабочем месте
- **самостоятельная регистрация биометрических идентификаторов пользователем на своем рабочем месте**
 - например, на этапе развертывания сервиса BioLink IDenium

Самостоятельная регистрация

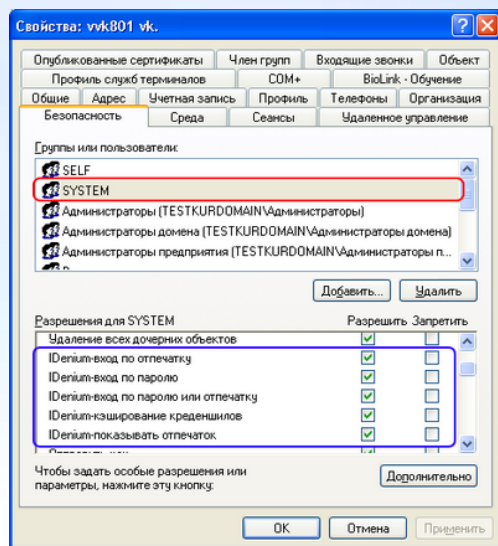


Для создания/изменения биометрического идентификатора необходимо щелкнуть (левой кнопкой мыши) на соответствующем пальце. Для удаления - необходимо щелкнуть (левой кнопкой мыши) на требуемом пальце, одновременно удерживая клавишу Ctrl.



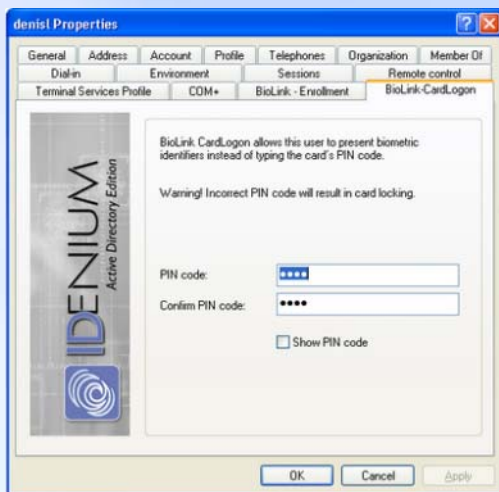
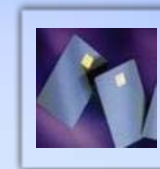
- пользователь выбирает регистрируемый отпечаток
- отпечаток сканируется
- допускается регистрация отпечатков всех 10 пальцев рук
- дальнейшая идентификация — по любому из отпечатков
- ЭТОТ МЕХАНИЗМ — также для перерегистрации отпечатков

Политики идентификации



- **идентификация только по отпечатку**
 - для большинства пользователей
- **идентификация по отпечатку пальца ИЛИ паролю**
 - для администраторов и сотрудников службы информационной безопасности
- **двухфакторная идентификация по отпечатку пальца И паролю**
 - защита доступа к ценным ресурсам
- **по смарт-карте**
 - с заменой ввода PIN-кода карты идентификацией по отпечатку пальца

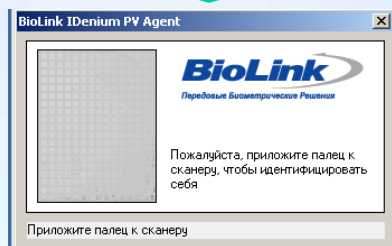
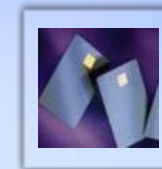
Применение смарт-карт



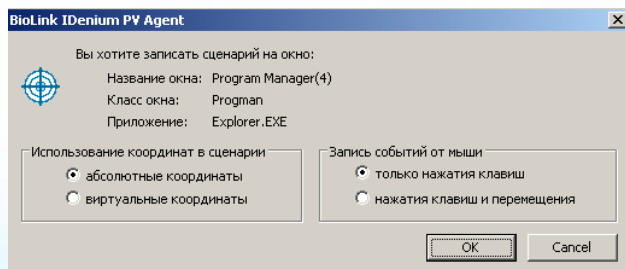
- ❑ В память смарт-карты вносится цифровой сертификат для входа в Windows
- ❑ ввод PIN-кода заменяется биометрической идентификацией
- ❑ офисный USB-сканер BioLink U-Match 5.0 интегрирован со считывателем смарт-карт



NEW Биометрический вход в приложения Password Vault

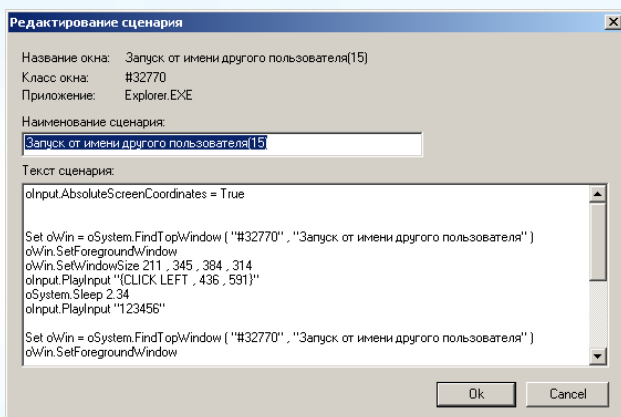
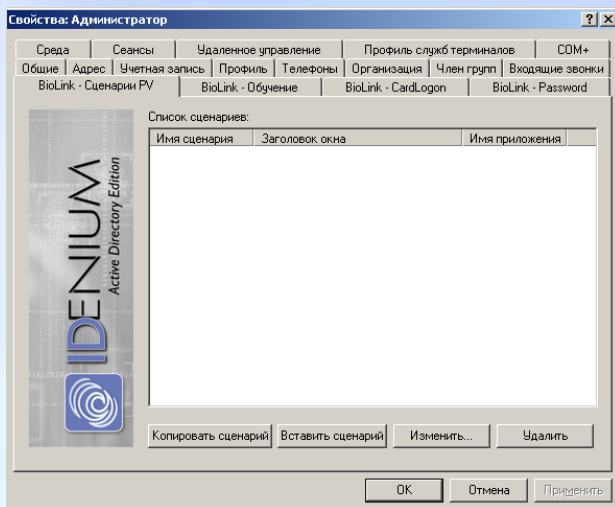
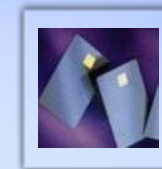


- ❑ динамическая замена (перехват) окна входа в приложение по имени и паролю на биометрическую идентификацию
- ❑ запись сценариев входа на стороне клиента



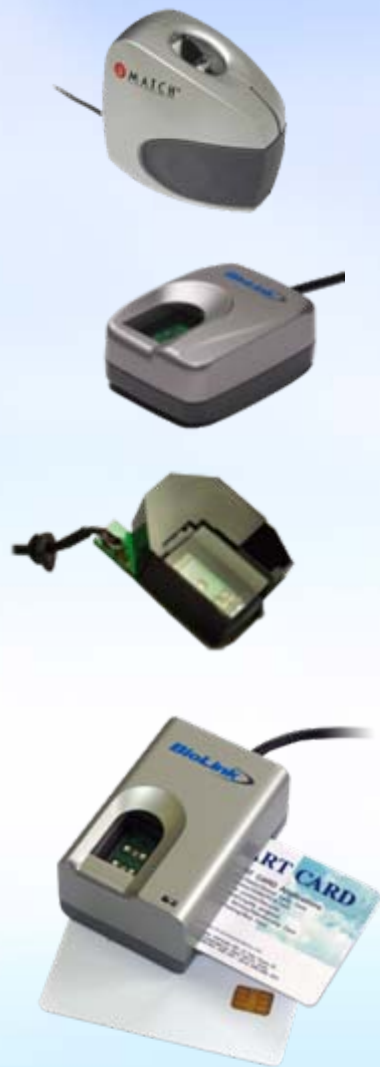
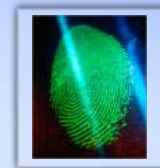


NEW Управление сценариями Password Vault



- ❑ панель управления сценариями входа в приложения для учетной записи пользователя
- ❑ редактирование сценариев входа в приложения (vbScript)
- ❑ управление политикой использования сценариев

Поддерживаемые сканеры отпечатков

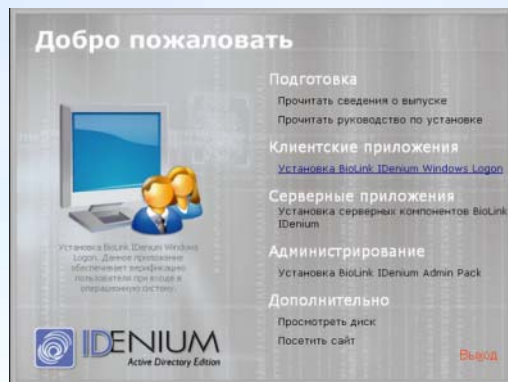


- ❑ **BioLink U-Match 1.0...3.5**
 - ❑ офисные оптические USB-сканеры
- ❑ **BioLink U-Match BI USB**
 - ❑ встраиваемый оптический USB-сканер
- ❑ **BioLink U-Match 5.0**
 - ❑ офисный оптический USB-сканер отпечатков пальцев, интегрированный со считывателем смарт-карт
- ❑ **сканеры компании UPEK**
 - ❑ встроены в ноутбуки и другие мобильные компьютерные устройства

Централизованная установка



- осуществляется с рабочего места администратора
- сервер(ы) биометрической идентификации регистрируются в Microsoft Active Directory автоматически
- дополнительный сервер биометрической идентификации
 - отказоустойчивость и балансировка нагрузки





- добавление новых пользователей (или учетных записей), изменение их свойств, удаление
- разрешение/запрет кэширования идентификационной информации на рабочей станции пользователя
- скрытие реального изображения отпечатка, выводимого на экран монитора при сканировании



Системные требования



- Клиентская часть
 - ОС: Microsoft Windows 2000/XP/Vista/**NEW! Windows 7** * 32-bit и 64-bit **
 - Компьютер входит в состав домена Active Directory
- Серверная часть
 - ОС: Microsoft Windows Server 2000/2003/2007
 - **NEW:** любая конфигурация доменов AD (деревья, лес)

* — версия Idenium с поддержкой Windows 7 проходит бета-тестирование и будет доступна для заказа с сентября 2009 года

** — BioLink Password Vault доступен только для 32-битных конфигураций клиентских ОС

Лицензирование



**программные
серверы идентификации**



**лицензия
на рабочие станции**



**лицензия
на пользователей**



**USB-сканеры
отпечатков пальцев**



**DVD-бокс с
инсталляционным диском**



Преимущества BioLink IDenium



БЕЗОПАСНОСТЬ



ЭФФЕКТИВНОСТЬ



НАДЕЖНОСТЬ



МАСШТАБИРУЕМОСТЬ, ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

КОМФОРТНОСТЬ





- ❑ пользователи не знают реальных паролей и не обмениваются ими
- ❑ исключена авторизация по утерянным или похищенным идентификаторам
- ❑ защита режимов экранной заставки и Standby
- ❑ многофакторная идентификация при доступе к особо ценным ресурсам



- минимизируются затраты рабочего времени при авторизации
- идентификаторы не теряются и не выходят из строя
- сокращается нагрузка на администраторов и службу безопасности
- уменьшаются расходы на управление инфраструктурой доступа



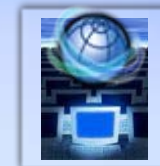
Надежность



- «горячий резерв» серверов биометрической идентификации и балансировка нагрузки между ними
- возможна работа отдельных сегментов сети в автономном режиме с последующей репликацией данных между обслуживающими их биометрическими серверами
- допускается вход пользователя на рабочую станцию по локальному кэшу при временной недоступности сервера или сети



Масштабируемость



- ограничения по числу пользователей отсутствуют
- централизованная инсталляция и управление с рабочего места администратора
- автоматическая регистрация серверов биометрической идентификации в AD
- управление идентификацией — со стандартной консоли AD Users and Computers



- **естественная простота и удобство идентификации**
- **возможна регистрация всех 10 отпечатков пальцев с последующей идентификацией по любому из них**
- **регистрация отпечатков пальцев производится однократно; сам пользователь может в дальнейшем перерегистрировать их**

- сканеры отпечатков пальцев и прикладное программное обеспечение биометрической идентификации на 9 000 рабочих мест
- основной и резервный серверы биометрической идентификации
- интеграция биометрической идентификации в специализированные банковские приложения
- планы применения биометрических технологий в банкоматах

- **биометрическая идентификация пользователей корпоративной сети**
- **биометрическая система функционирует в головном офисе и 30 филиалах**
- **идентификация сотрудников банка при доступе в корпоративную сеть, к финансовым системам, защищенным Интернет-ресурсам**

- **биометрическая идентификация инженеров, конструкторов, техников**
- **интеграция биометрии в специализированные программные продукты, применяемые при проведении опытно-конструкторских работ и в инжиниринге**
- **планы распространения биометрии на филиалы предприятия и использования биометрических систем учета рабочего времени и контроля доступа**



Министерство связи и массовых коммуникаций



- оснащение аппаратными и программными средствами биометрической идентификации рабочих мест сотрудников центрального аппарата Министерства и находящихся в его ведении федеральных агентств и служб
- программный сервер централизованной биометрической идентификации
- проект реализован в два этапа с последовательным увеличением численности пользователей биометрической системы

www.biolink.ru

Защита информации

Спасибо за внимание!