INDEED ID

White Paper

Indeed Certificate Manager

Централизованное управление инфраструктурой открытых ключей

www.indeed-id.ru

Содержание

Эффективное применение инфраструктурой открытых ключей **3**

Indeed Certificate Manager 3

Сокращение издержек 3

Повышение безопасности 4

Состав Indeed Certificate Manager **5**

Базовые модули 5

Indeed CM Сервер 5

Консоль администратора 5

Инструменты самообслуживания 5

Журнал событий 6

Хранилище данных Indeed CM 6

Card Monitor 7

Модули интеграции 7

Коннекторы к Удостоверяющим Центрам 7

Коннекторы к каталогам пользователей 7

API 7

Middleware 8

Коннектор к Indeed AM 8

Коннектор к принтеру смарт-карт 8

Дополнительные функции 8

Журнал СКЗИ 8

Клиентский агент 8

Indeed AirKey Enterprise 9

О компании Индид **10**

Эффективное применение инфраструктурой открытых ключей

Инфраструктура открытых ключей (Public Key Infrastructure, PKI) предлагает решение многих проблем информационной безопасности:

- Замена устаревшей парольной аутентификации на строгую двухфакторную при доступе в операционную систему и приложения (VPN, VDI и др.);
- Цифровая подпись и шифрование электронной почты;
- Применение квалифицированной электронной подписи для соответствия требованиям регуляторов и обеспечения юридически значимого документооборота;
- Шифрование данных: файлов, дисков, и другой информации.

Но сопровождение самой инфраструктуры открытых ключей порождает ряд новых задач:

- Выпуск сертификатов пользователей в соответствии с их задачами: необходимо обеспечить наличие на смарт-карте пользователя требуемых для его работы сертификатов, не предоставив при этом избыточных сертификатов;
- Управление пользовательскими PIN-кодами устройств (смарт-карт и USB-токенов): политики сложности PIN-кодов, регулярность их смены;
- Контроль сроков действия сертификатов, своевременное их обновление;
- Ведение учета смарт-карт и USB-токенов, закрепление их за сотрудниками;
- Ведение журнала учета средств криптографической защиты информации (СКЗИ) для соответствия требованиям регуляторов;
- Разблокировка заблокированных устройств, когда пользователь забывает свой PIN.

Эффективное применение PKI невозможно без качественного решения описанных задач. Для этих целей применяются специализированное программное обеспечение класса Card Management System (CMS).

Indeed Certificate Manager

Программный комплекс Indeed Certificate Manager (Indeed CM) представляет собой централизованную систему управления инфраструктурой открытых ключей. Indeed CM позволяет привести процессы использования PKI в соответствие с потребностями бизнес-подразделений, ИТ департамента, службы безопасности и внешних регуляторов.

Сокращение издержек

Indeed Certificate Manager призван сократить издержки компаний на рутинные операции обслуживания PKI:

- Выпуск сертификатов. Indeed CM автоматически формирует список сертификатов для выпуска на основе механизма политик использования PKI. Все пользователи, подпадающие под действия одной политики получают идентичный набор настроек и сертификатов. Операции по созданию запросов на сертификаты, их выпуску и записи на ключевой носитель выполняется в автоматизированном режиме.

- Рядовым пользователям системы предоставляется удобный кабинет самообслуживания, выполненный в формате web-приложения. В этом кабинете пользователи, если им разрешено политикой, могут самостоятельно производить выпуск и обновление сертификатов, снижая

нагрузку на департамент ИТ.

- Indeed CM отправляет почтовые уведомления администраторам и пользователям на заданные события системы. Например, администратор и/или пользователь получают уведомление о приближении окончания срока действия сертификата, что позволяет вовремя обновить сертификат и избежать простоев в работе.

- Indeed CM позволяет производить разблокировку заблокированного носителя без визита пользователя к администратору. Такая разблокировка может быть выполнена до или после входа пользователя в операционную систему, а также с или без явного участия администратора.

- Indeed CM предоставляет программный интерфейс (API) через который он интегрируется со сторонними системами. Такая интеграция расширяет возможности по автоматизации процессов использования сертификатов и ключевых носителей. Например, по событию из системы класса Identity Management Indeed CM может отозвать сертификат уволенного сотрудника.

- В состав Indeed CM входит электронный журнал учета средств криптографической защиты информации (СКЗИ), соответствующий приказу ФАПСИ №152. Использую этот журнал, сотрудники безопасности выполняют требования регуляторов в части учета средств криптографической защиты без применения бумажных носителей и ручного заполнения необходимых данных.

- Учет сертификатов, выданных сторонними организациями. Если в организации применяются сертификаты, выданные сторонними (не собственными) удостоверяющими центрами, Indeed CM позволяет занести информацию о таких сертификатов в базу решения и своевременно напомнить администратору и пользователю о скором истечении таких сертификатов. Это позволяет избежать простоев в работе с банками и торговыми площадками.

Повышение безопасности

Используя Indeed Certificate Manager, компании повышают общий уровень своей информационной безопасности за счет следующих возможностей:

- Централизованное применение политики PIN кодов. При выпуске ключевого носителя на него записываются требования к PIN: сложность, частота смены, глубина истории и другие - набор параметров зависит от модели устройства. Политики хранятся и распространяются централизованно, администраторам не нужно прописывать политики для каждого отдельного носителя.

- Учет ключевых носителей. Каждое устройство - смарт-карта или USB-токен - закрепляются за ответственным сотрудником. Операции по выпуску или обновлению сертификатов на носителе могут выполнить только администратор Indeed CM или сам пользователь - владелец устройства.

- Своевременный отзыв сертификатов уволенных сотрудников. Для того, чтобы оперативно прекращать доступ уволенных сотрудников к информационным ресурсам компании, Indeed CM включает специализированный сервис, который с заданной периодичностью проверяет каталог пользователей и отзывает сертификаты у пользователей, отмеченных как уволенные.

- Гибкая настройка прав на работу с системой. Indeed CM позволяет компаниям определить собственные роли безопасности с настраиваемым перечнем разрешенных операций. Это

позволяет администраторам привести ролевую модель Indeed CM в соответствие с принятыми в компании бизнес-процессами.

- Контроль использования ключевых носителей на ПК пользователей. Indeed CM позволяет компаниям отслеживать, какие носители и кем подключаются к ПК организации. Администратор может жестко закрепить ключевой носитель за пользователем или конкретным ПК. Если система обнаружит несоответствие (например, носитель подключен в сессии нелегитимного пользователя или к неразрешенному ПК), ключевой носитель может быть заблокирован.

Состав Indeed Certificate Manager

Архитектура Indeed Certificate Manager построена по модульному принципу. Каждый модуль реализует конкретный набор функций для решений определенной задачи. Конкретная инсталляция системы может включить все, либо часть модулей, в зависимости от бизнес-потребностей компании. Indeed CM состоит из следующих функциональных и программных модулей.

Базовые модули

Indeed CM Сервер

Сервер - основной компонент инфраструктуры Indeed CM, связывающий все модули системы. Представляет собой ASP .Net приложение, работающее на сервере Internet Information Services (IIS). Indeed CM сервер обеспечивает централизованное управление пользователями системы, репозиторием карт и политиками безопасности. Также сервер обеспечивает выполнение операций разблокировки смарт-карт и журналирования событий.

Консоль администратора

Консоль выполнена в виде web-приложения и предоставляет администраторам и операторам интерфейс для выполнения всех операций по сопровождению PKI: редактировать политики использования ключевых носителей и сертификатов, производить регистрацию и выпуск устройств, просматривать журналы и реестр устройств, настраивать ролевую модель, вести журнал учета СКЗИ и контролировать использование ключевых носителей через клиентские агенты.

Инструменты самообслуживания

Инструменты самообслуживания пользователей включают в себя

- Сервис самообслуживания - web-приложение, доступное пользователям системы для самостоятельного выполнения операция с сертификатами и ключевыми носителями: выпуск, отзыв, обновление, смена PIN-кода и др. Набор доступных операций задается администратором системы.

- Credential Provider - модуль, устанавливаемый на ПК и позволяющий выполнить разблокировку заблокированного ключевого носителя (смарт-карты или токена) на рабочем месте пользователя в online- или offline-режимах без необходимости выполнять вход в операционную систему.

Журнал событий

В журнале фиксируются все события, связанные с жизненным циклом смарт-карт, работой агентов и службы Card monitor, изменением параметров системы. Просмотр журнала доступен в интерфейсе консоли администратора Indeed CM, там же возможно построение отчетов по различным критериям.

Хранилище данных Indeed CM

Данные Indeed CM (информация об устройствах, сертификатах, настройках системы) могут храниться либо в SQL СУБД, либо в Active Directory. При хранении данных в AD не требуется расширение схемы, все данные локализованы в отдельном контейнере. Данные в хранилище шифруются серверным ключом.

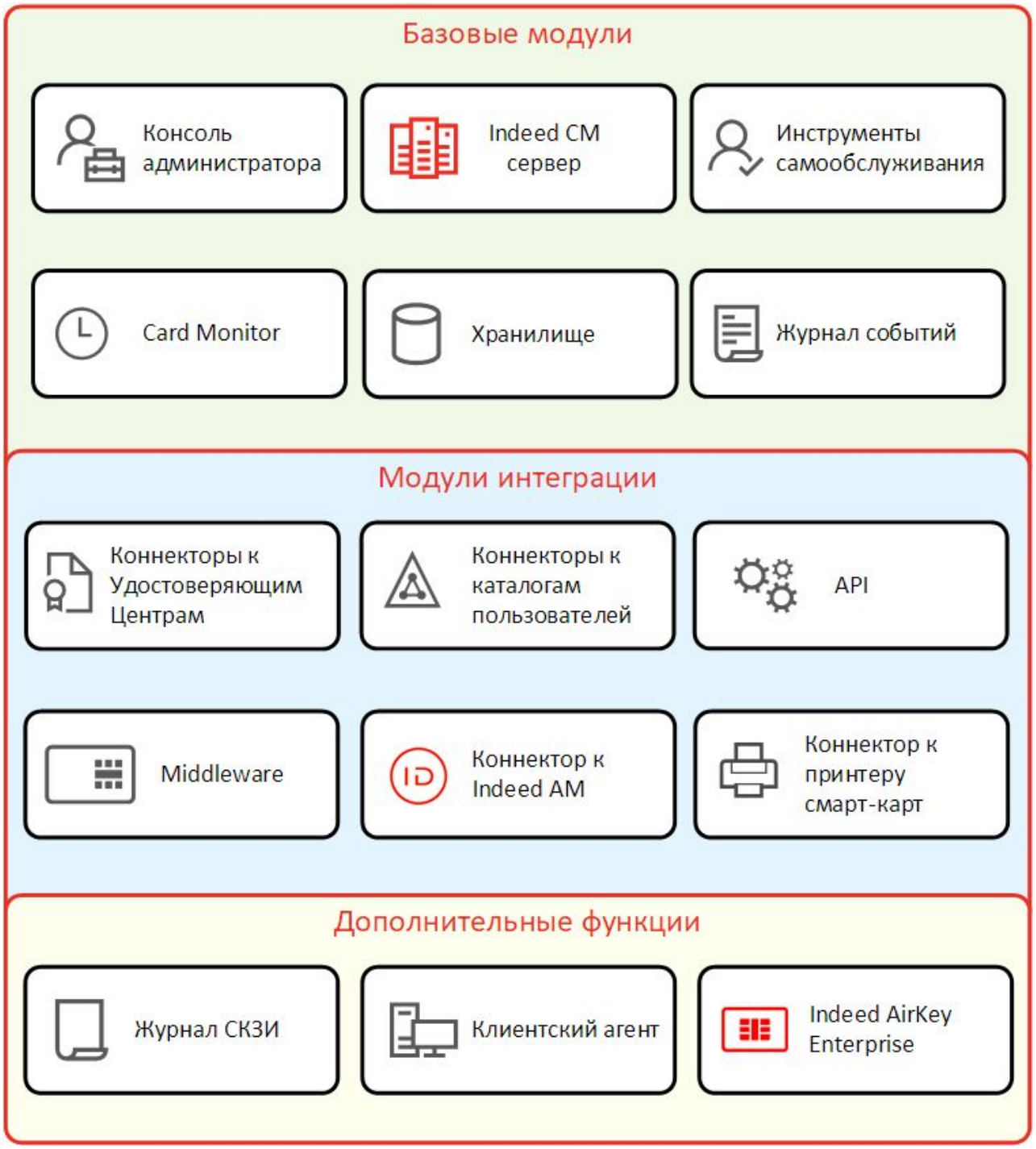

Рисунок 1. Состав Indeed Certificate Manager

Card Monitor

Служба Card Monitor предназначена для выполнения операций по контролю за использованием смарт-карт и USB-токенов и выполняет следующие операции:

- Отзыв ключевых носителей и сертификатов удаленных сотрудников
- Отзыв временных носителей с истекшим сроком действия
- Выключение (опционально) устройств и отзыв сертификатов пользователей, чьи учетные записи Active Directory были отключены
- Установка статуса сертификатов, хранящихся на ключевом носителе (истекает/истек)
- Обновление содержимого ключевого носителя
- Рассылка почтовых уведомлений администраторам и пользователям системы:
    - Истечение срока действия сертификатов пользователей
    - Одобрение/отклонение выпуска ключевого носителя
    - Одобрение/отклонение обновления сертификатов
    - Одобрение/отклонение замены ключевого носителя
    - Изменение политики Indeed CM, действующей на пользователя

Модули интеграции

Коннекторы к Удостоверяющим Центрам

Для связи с Удостоверяющими Центрами (УЦ) в Indeed CM имеются специализированные коннекторы. С помощью этих коннектор Indeed CM выполняет такие операции:

- Получение шаблонов сертификатов
- Создание и отправка запросов на сертификаты
- Одобрение запросов на сертификаты
- Выпуск сертификатов
- Приостановка действия и отзыв сертификатов
- Проверка статуса сертификата
- Создание и обновление данных пользователя УЦ (для КриптоПро УЦ)

Indeed Certificate Manager поддерживают работу с такими удостоверяющими центрами и сервисами электронной подписи:

- Microsoft CA
- КриптоПро УЦ
- КриптоПро DSS

Коннекторы к каталогам пользователей

Indeed Certificate Manager получает информацию о пользователях из стороннего каталога. В качестве каталога пользователей могут использоваться Microsoft Active Directory или база пользователей КриптоПро УЦ.

API

Программный интерфейс (API) Indeed CM используется для управления ключевыми носителями и сертификатами пользователей из сторонних систем, таких как Identity Management (IDM). API предоставляет функции для реализации таких сценариев:

- Автоматического назначения пользователю необходимой политики использования PKI (какие сертификаты нужно выпускать, какие операции с ключевыми носителями доступны пользователю и др.)

- Автоматического отзыва, приостановки или возобновления действия сертификатов пользователя (например, при увольнении, отпуске или смене должности).

Middleware

Indeed CM Middleware - это клиентское ПО, устанавливаемое на рабочие места администраторов и пользователей. Middleware обеспечивает выполнение операций, требующих доступа к носителю: установка и сброс PIN-кода, генерация ключей, запись сертификатов, инициализация и др. Indeed CM поддерживает работу со следующими ключевыми носителями:

- Indeed AirKey Enterprise
- Рутокен, компании Актив
- eToken, компании SafeNet
- ESMART, компании ISBC
- JaCarta, компании Аладдин Р.Д.
- AvestKey, компании Авест
- ID Prime, компании Gemalto
- ePass 2003, компании Feitian.

Коннектор к Indeed AM

Коннектор к системе управления доступом Indeed Access Manager (Indeed AM) автоматически регистрирует ключевой носитель, выпускаемый в Indeed CM, в базе данных Indeed AM. После этого, пользователь сразу может применять свою смарт-карту или USB-токен не только для операций ЭЦП, но и доступа в прикладные информационные системы с помощью Indeed AM Enterprise SSO.

Коннектор к принтеру смарт-карт

Коннектор к специализированному принтеру смарт-карт позволяет значительно сократить время на персонализацию и выпуск большого количества смарт-карт сотрудникам. Indeed CM за одну операцию в пакетном режиме выпускает сертификаты и записывает их на смарт-карты, а также выполняет персонификацию карт с печатью данных сотрудников на них.

Дополнительные функции

Журнал СКЗИ

Журнал учета СКЗИ содержит данные об изготавливаемых СКЗИ и отметки об их использовании. При выпуске сертификата, Indeed CM автоматически добавляет соответствующую запись в журнал. Indeed CM позволяет учитывать любые типы СКЗИ: ключевой документ, дистрибутив, лицензия, документация или пользовательский. Администратор может экспортировать журнал в csv или pdf формате для дальнейшей обработки или предъявления его аудиторам.

Клиентский агент

Клиентский агент устанавливается на ПК пользователей и контролирует использование смарт-карт, USB-токенов и сертификатов на рабочих местах. Агент выполняет следующие операции:

- Передает на сервер Indeed CM информацию об используемых ключевых носителях - к какому ПК в данный момент подключены токены и смарт-карты и какой пользователь работает на ПК.
- Блокирует сессию Windows или ключевой носитель, в случае нарушения правил использования. Например, смарт-карта может быть привязана к учетной записи пользователя или ПК; если текущий пользователь или ПК не совпадает с назначенными, агент может заблокировать смарт-карту
- Смена PIN-кода пользователя по требованию администратора
- Блокировка носителя по требованию администратора
- Разблокировка носителя
- Обновление сертификатов на носителе
- Удаление информации с ключевого носителя.

Таким образом, агент позволяет администраторам вести аудит использования смарт-карт и токенов и удаленно выполнять операции с ключевыми носителями на ПК пользователя. Также агент может предотвращать несанкционированное использование носителей.

Indeed AirKey Enterprise

Indeed AirKey Enterprise представляет собой программную реализацию смарт-карты, позволяющую выполнять полный набор операций, доступный аппаратным ключевым носителям:

- электронно-цифровая подпись документов;
- шифрование и расшифровка данных;
- двухфакторная аутентификация пользователей (в т.ч. в операционной системе);
- операции по стандартам PKCS#11 и Microsoft CryptoAPI;
- организация доступа в режиме Single Sign-On.

Indeed AK Enterprise полностью эмулирует поведение физической смарт-карты. С точки зрения операционной системы компьютера и целевых приложений, с которыми работает пользователь, Indeed AK Enterprise неотличим от традиционной смарт-карты. Работа Indeed AK Enterprise строится на соответствии штатным протоколам, интерфейсам и механизмам PKI-инфраструктуры. При этом закрытые ключи не передаются на ПК пользователя, а хранятся в базе данных в зашифрованном виде на сервере Indeed AK Enterprise. Криптографические операции выполняются на сервере в системных процессах сервера Indeed AK Enterprise. Для обеспечения безопасности производится шифрование каналов связи между ПК пользователя и сервером с применением асимметричных алгоритмов шифрования по протоколу TLS. На ПК пользователя доставляется уже готовый результат криптооперации (открытый ключ, подписанные или расшифрованные данные).

Использование программной реализации смарт-карты Indeed AK Enterprise имеет следующие преимущества:

Отсутствие аппаратной составляющей
Пластиковые смарт-карты и USB-токены ломаются, теряются, забываются, а также требуют периодической замены. Виртуальная смарт-карта лишена этих недостатков.

Выполнение криптографических операций на сервере
Закрытый ключ не хранится на клиенте, а значит не может быть скомпрометирован вредоносным ПО или злоумышленником.

Полный контроль использования со стороны специалистов ИБ
Все операции выпуска, отзыва, а также подключение виртуальных смарт-карт к ПК пользователя фиксируются в журнале системы. Специалисты ИБ имеют возможность в любой момент времени прекратить использование смарт-карты Indeed AK Enterprise, выполнив удаленный отзыв карты с

уничтожением закрытых ключей.

Удаленная доставка смарт-карты пользователю
Виртуальная смарт-карта доставляется на ПК пользователя удаленно без его участия. Пользователю не требуется лично получать устройство от оператора системы, смарт-карта Indeed AK Enterprise появляется в операционной системе ПК пользователя, как только оператор на своем рабочем месте выполняет операцию выпуска смарт-карты.

О компании Индид

Компания Индид является российским разработчиком программного обеспечения под маркой Indeed Identity. Разрабатываемые нами программные комплексы предназначены для управления доступом сотрудников к информационным ресурсам компании, контроля доступа привилегированных пользователей, а также управлению инфраструктурой открытых ключей и жизненным циклом смарт-карт и USB-ключей. Продукты компании используются в ведущих компаниях России и СНГ в различных отраслях: финансовой, производстве, нефтегазовой, ритейле и телекоммуникационной. Офисы компании расположены в Санкт-Петербурге, Москве, Великом Новгороде и Вильнюсе.

Чтобы получить дополнительную информации о продуктах компании, задать интересующие вопросы и получить консультацию посетите сайт www.indeed-id.ru.