Рутокен KeyBox

Общее описание

Рутокен KeyBox — система, предназначенная для внедрения, управления и учета аппаратных средств аутентификации пользователей в масштабах предприятия. Рутокен KeyBox обеспечивает централизованное управление средствами аутентификации в течение всего жизненного цикла, ведет учет средств криптографической защиты информации и аудит их использования. Система также позволяет быстро и самостоятельно решать проблемы пользователей без обращения к администраторам, в том числе за пределами предприятия.

Задачи

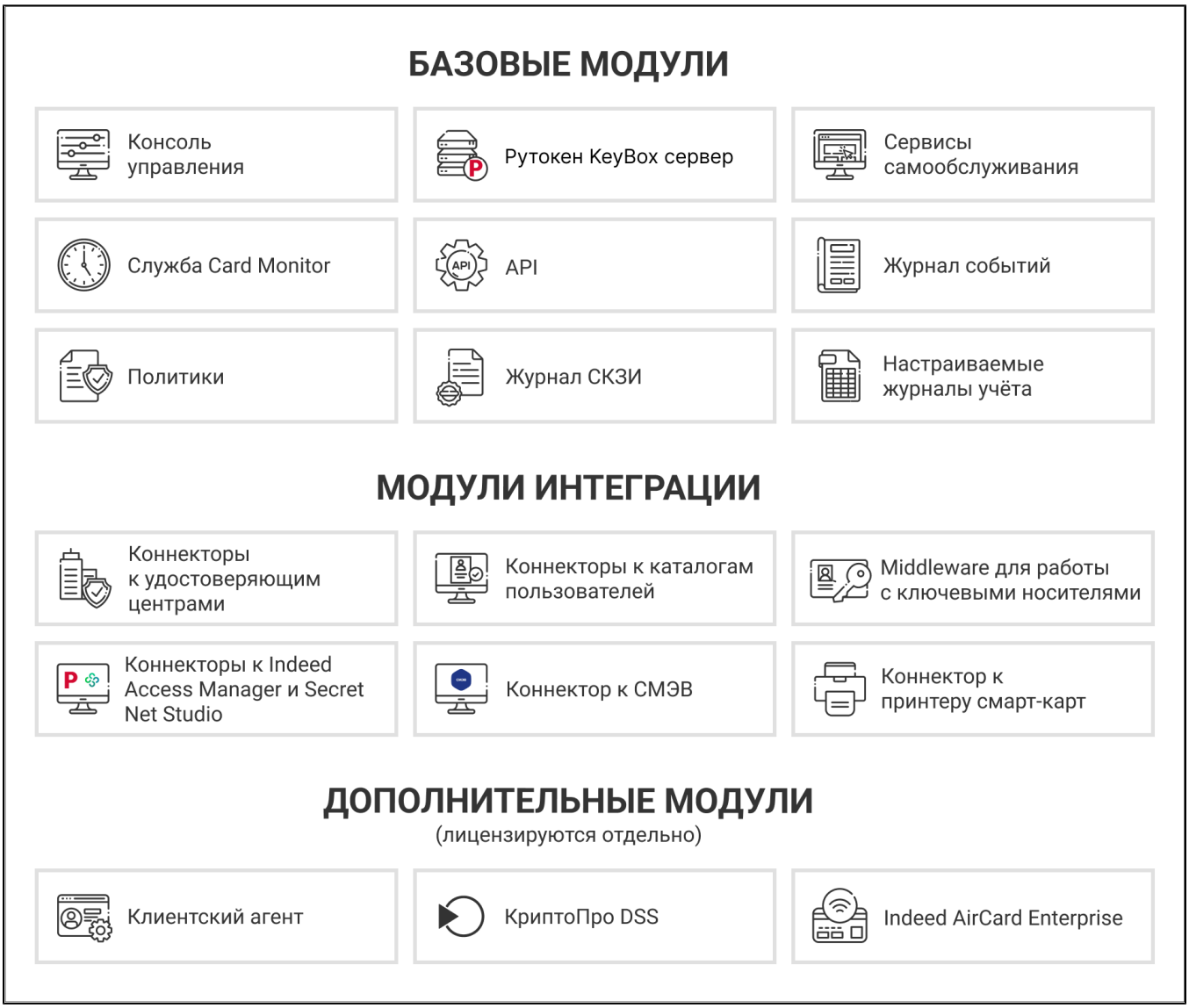
Сокращение издержек компании на рутинные операции обслуживания PKI

- Выпуск сертификатов. Рутокен KeyBox 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 веб-приложения. В этом кабинете пользователи, если им разрешено политикой, могут самостоятельно производить выпуск и обновление сертификатов, снижая нагрузку на департамент ИТ.
- Рутокен KeyBox 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.
- Рутокен KeyBox 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.
- Рутокен KeyBox 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 Рутокен KeyBox администратор может отозвать сертификат уволенного сотрудника.
- В состав Рутокен KeyBox входит электронный журнал учета средств криптографической защиты информации (СКЗИ), соответствующий приказу ФАПСИ №152. Используя 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, Рутокен KeyBox позволяет занести информацию о таких сертификатах 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 общего уровня информационной безопасности

- *Централизованное применение политики PIN-кодов*. При выпуске ключевого носителя на него записываются требования к PIN-коду: 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) закрепляется за ответственным сотрудником. Операции по выпуску или обновлению сертификатов на носителе могут выполнить администратор Рутокен KeyBox или сам пользователь (владелец устройства).
- *Своевременный отзыв сертификатов уволенных сотрудников*. Для того, чтобы оперативно прекращать доступ уволенных сотрудников к информационным ресурсам компании, Рутокен KeyBox 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*. Рутокен KeyBox позволяет компаниям определить собственные роли безопасности с настраиваемым перечнем разрешенных операций. Это позволяет администраторам привести ролевую модель Рутокен KeyBox в соответствие с принятыми в компании бизнес-процессами.
- *Контроль использования ключевых носителей на ПК пользователей*. Рутокен KeyBox позволяет компаниям отслеживать, какие носители и кем подключаются к компьютеру организации. Администратор может жестко закрепить ключевой носитель за пользователем или конкретным компьютером. Если система обнаружит несоответствие (например, носитель подключен в сессии нелегитимного пользователя или к неразрешенному компьютеру), ключевой носитель может быть заблокирован.

Структурная схема



Компоненты системы

Рутокен KeyBox состоит из серверных и клиентских компонентов. В качестве средства хранения данных и настроек решения используется Active Directory, база данных Microsoft SQL или PostgreSQL. Расширение схемы Active Directory не требуется.

Серверные компоненты

Рутокен KeyBox Server является серверным компонентом и включает в себя веб-приложения и вспомогательные утилиты.

Веб-приложения:

- **Management Console** — Консоль управления для администраторов и операторов системы.
- **Self-Service** — Сервис самообслуживания (личный кабинет) пользователя.
- **Remote Self-Service** — Сервис удаленного обслуживания за пределами домена.
- **CredProvAPI** — Сервис онлайн-разблокировки и выключения устройств.
- **API** — Сервис API для управления жизненным циклом устройств (для интеграции со сторонними ПО).
- **MSCA Proxy** — Позволяет запрашивать и записывать на устройства сертификаты с Удостоверяющих Центров Microsoft Enterprise CA, находящихся за пределами того домена, в котором развернут Рутокен KeyBox.
- **Event Log Proxy** — Позволяет записывать события с нескольких серверов Рутокен KeyBox в единый журнал событий Windows.
- **Indeed Log Server** — Позволяет записывать события с нескольких серверов Рутокен KeyBox в единый журнал событий Windows, базу данных Microsoft SQL или PostgreSQL, SysLog.

- **RutokenKeyBox CM Agent** — Сервисы клиентского агента для удаленного выполнения задач блокировки, сброса PIN-кода пользователя, обновления содержимого устройства, очистки или инициализации устройства при его отзыве, смены PIN-кода администратора на устройствах пользователей.

Вспомогательные утилиты:

- **IndeedCM.Agent.Cert.Generator.exe** — Утилита для создания сертификатов клиентского агента.
- **IndeedCM.Persistence.AD.Cfg.exe** — Утилита для создания хранилища данных в Active Directory.
- **IndeedCM.Persistence.KeyGen.exe** — Утилита для создания ключа шифрования базы данных системы.
- **IndeedCM.CertEnroll.MsCA.exe** — Утилита для выпуска сертификата “Агент регистрации”.
- **RutokenKeyBox.CardMonitor.exe** — Служба мониторинга состояния устройств.
- **RutokenKeyBox.Wizard.exe** — Мастер настройки Рутокен KeyBox.
- **Storage.sql** — Скрипт наполнения базы данных Microsoft SQL, используемой для хранения данных Рутокен KeyBox.
- **Storage-Postgre.sql** — Скрипт наполнения базы данных PostgreSQL, используемой для хранения данных Рутокен KeyBox.

Клиентские компоненты

RutokenKeyBox Middleware — компонент, предоставляющий единый интерфейс остальным компонентам системы по управлению устройствами, подключенными к рабочей станции.

RutokenKeyBox Client Tools:

- **Credential Provider** — компонент для разблокировки смарт-карт, используемых для аутентификации в операционной системе Windows, в офлайн и онлайн-режимах.
- **RutokenKeyBox Unblock** — компонент для разблокировки смарт-карт, которые не используются для входа в операционную систему.

RutokenKeyBox Agent — клиентский агент для удаленного выполнения задач (блокировки, сброса PIN-кода пользователя, обновления содержимого устройства, очистки или инициализации устройства при его отзыве, смены PIN-кода администратора) на устройствах пользователей.

RutokenKeyBox Client Browser Extension — компонент для поддержки множественных сессий пользователей на терминальном сервере.