Рутокен KeyBox

Общее описание

Рутокен KeyBox — это система, предназначенная для администрирования и управления жизненным циклом ключевых носителей (USB-токенов, смарт-карт и других устройств). Она обеспечивает связь между учетными записями пользователей, средствами аутентификации, приложениями и регламентами ИБ (корпоративной политикой безопасности).

Функциональные возможности системы:

- Управление жизненным циклом ключевых носителей — от постановки на учет и ввода в эксплуатацию до вывода из эксплуатации и списания.
- Управление информацией на ключевых носителях: генерация ключей, запись сертификатов, обновление данных.
- Управление политиками PIN-кодов носителей.
- Учет и контроль носителей с ключами и сертификатами, выпущенными сторонними удостоверяющими центрами.

Архитектура системы

Система состоит из базовых модулей, модулей интеграции и дополнительных функций.

К базовым модулям относятся:

- Консоль администратора;
- KeyBox сервер;
- Card Monitor;
- Хранилище;
- Инструменты самообслуживания;
- Журнал событий.

К модулям интеграции относятся:

- Коннекторы к удостоверяющим центрам;
- Коннекторы к каталогам пользователей;
- Коннектор к принтеру смарт-карт;
- Middleware;
- API.

К дополнительным функциям относятся:

- Журнал СКЗИ;
- Клиентский агент.

Компоненты системы

Рутокен KeyBox состоит из серверной и клиентской части.

Компонентом *серверной части* является Rutoken Server, который состоит из веб-сервисов и вспомогательных утилит.

Веб-сервисы:

- **Management Console** — Консоль управления.
- **Self Service** — Сервис самообслуживания.
- **Remote Self Service** — Сервис удаленного обслуживания за пределами домена.
- **CredProvAPI** — Сервис онлайн-разблокировки и выключения смарт-карт.
- **ICMAPI** — Сервис управления жизненным циклом смарт-карт (для интеграции со сторонним ПО).
- **MSCA Proxy** — позволяет запрашивать и записывать на устройства при помощи Рутокен KeyBox сертификаты со всех УЦ, находящихся за пределами того домена, в котором развернут Рутокен KeyBox.
- **Event Log Proxy** — позволяет записывать события со всех серверов Рутокен KeyBox в единый журнал событий Windows.
- **Indeed Log Server** — позволяет записывать события со всех серверов Рутокен KeyBox в единый журнал событий Windows или базу данных Microsoft SQL.
- **Agent** — Компонент для удаленного выполнения задач (блокировки, разблокировки, смены PIN-кода администратора и т.п.) 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.
- **IndeedCM.CertEnroll.MsCA.exe** – Утилита для выпуска сертификата "Агент регистрации".
- **IndeedCM.CardMonitor.exe** – Утилита мониторинга состояния смарт-карт.
- **IndeedCM.Unblock.exe** – Утилита для разблокировки смарт-карт.
- **IndeedCM.Wizard.exe** – Мастер настройки Рутокен KeyBox.
- **Storage.sql** и **Storage_Indices.sql** – Скрипты наполнения базы данных Microsoft SQL, используемой для хранения данных Рутокен KeyBox.

Клиентская часть состоит из следующих компонентов:

- **Indeed CM Middleware** — компонент, предоставляющий единый интерфейс остальным компонентам системы по управлению устройствами, подключенными к рабочей станции.
- **Indeed CM Client Tools**:

  — **Credential Provider** — компонент для разблокировки смарт-карт, используемых для аутентификации в операционной системе Windows, в офлайн и онлайн режимах.

  — **Indeed CM Unblock** — компонент для разблокировки смарт-карт, которые не используются для входа в операционную систему.

- **Indeed CM Agent** — компонент для удаленного выполнения задач (блокировки, разблокировки, смены PIN-кода администратора и т.п.) на устройствах пользователей.
- **Indeed CM Client Browser Extension** — компонент для поддержки множественных сессий пользователей на терминальном сервере.