Подключение к центру сертификации Microsoft через RutokenKeyBox.MSCA.Proxy

Рутокен KeyBox может взаимодействовать с центрами сертификации Microsoft, располагающимися за пределами домена, в котором находится сервер Рутокен KeyBox. Например, конфигурация, когда у одной организации есть несколько независимых доменов с самостоятельными центрами сертификации в каждом, а Рутокен KeyBox развернут только в одном из этих доменов. При выпуске устройства Рутокен KeyBox обращается к MS CA Proxy, а тот, используя сертификат Агента Регистрации, передает запрос на целевой центр сертификации.

Для установки и настройки приложения MS CA Proxy выполните следующие действия:

1. Создайте во внешнем для Рутокен KeyBox домене сервисную учетную запись для работы с центром сертификации Microsoft (см. Создание сервисной учетной записи для работы с Microsoft CA).
2. Настройте для сервисной учетной записи из п.1 шаблон Агент регистрации (см. Настройка шаблонов сертификатов) и выпустите для этой учетной записи сертификат по этому шаблону (см. Выпуск сертификата Агент регистрации (Enrollment Agent)).

   Сертификат **Агент регистрации** должен располагаться в **хранилище сертификатов рабочей станции (Local computer)**, на которой установлен компонент IndeedCM MS CA Proxy.
3. Установите компонент **IndeedCM.MSCA.Proxy.msi** из дистрибутива (располагается в каталоге RutokenKeyBox.Server) на рабочей станции в домене с внешним УЦ.

   Системные требования для установки компонента совпадают с требования для установки сервера Рутокен KeyBox.
4. Откройте в редакторе Блокнот, запущенном от имени администратора, файл конфигурации MS CA Proxy — **C:\inetpub\wwwroot\cm\mscaproxy\Web.config**.
5. Укажите в секции **caProxySettings**:
   - Имя центра сертификации в параметре **ca**.
   - Данные учетной записи (логин и пароль), обладающей сертификатом **Агент регистрации** в параметрах **userName** и **password** соответственно.
   - **Отпечаток** (Thumbprint) сертификата **Агент регистрации** в параметре **enrollmentAgentCertificateThumbprint**.
     Пример заполненной секции:

     ```
     <caProxySettings ca="servercm.external.com\EXTERNAL-CA" userName="EXTERNAL\serviceca" password="p@ssw0rd"
     enrollmentAgentCertificateThumbprint="dbd1859d27395860843643ebe17e2ee3fc463aba"/>
     ```
6. Сервер Рутокен KeyBox использует Windows авторизацию в случае инсталляции на ОС Windows и авторизацию по сертификатам в случае инсталляции на ОС Linux.
   - При использовании Windows авторизации (инсталляция на Windows Server):
     - в параметре **allow users** укажите сервисную учетную запись из домена, в котором установлен IndeedCM MSCA Proxy, например, созданную в п.1.
       Пример заполненной секции:

       ```
       <authentication mode="Windows" />
       <authorization>
           <deny users="?" />
           <allow users="EXTERNAL\serviceca" />
           <deny users="*" />
       </authorization>
       ```
   - При использовании авторизации по сертификату (инсталляция на ОС семейства Linux):
     - Параметру **authentication** укажите значение **"None"**, а также закомментируйте секцию **authorization**.
       Пример заполненной секции:

       ```
       <authentication mode="None" />
       <!--
           <authorization>
               <deny users="?"/>
               <allow users="*" />
               <deny users="*" />
           </authorization>
       -->
       ```
     - В секции **appSettings** параметру **authorizeByCertificate** укажите значение **"True"**, а в параметре **allowedCertificateThumbprints** укажите отпечаток клиентского сертификата, разрешенного к предъявлению сервером Рутокен KeyBox.

Улучшенный ключ (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности клиента** (Client Authentication) и быть установлен в хранилище сертификатов сервера Рутокен KeyBox.
Пример заполненной секции:

```
<appSettings>
    <add key="authorizeByCertificate" value="true" />
    <add key="allowedCertificateThumbprints" value="aba8b93d73343f2182e3c1c40482b2ae2d75b6ec"
/>
</appSettings>
```

7. **Сохраните** изменения в файле и закройте файл конфигурации.