

УДК 004.42

## ПОДСИСТЕМА SINGLE SIGN-ON ДЛЯ ПЛАТФОРМЫ ONEVIZION

Купчинский В.А., студент гр. ИТм-171, 2 курс

Научный руководитель: Чичерин И.В., к.т.н., доцент

Кузбасский государственный технический университет

имени Т.Ф. Горбачева

г. Кемерово

В современном мире в век быстро развивающихся технологий, информация играет важную роль. Огромное значение информации представляет для бизнеса, потребности которого постоянно меняются, и конкуренция в котором велика. Большие предприятия располагают огромным количеством данных, которое помогает им оставаться конкурентоспособными и даже лидировать на рынке. В наше время таким предприятиям не обойтись без использования различных сервисов или информационных систем для управления информацией и ее хранения. Важной задачей таких систем является защита данных от несанкционированного доступа за счет ограничения доступа к ним. С использованием системы единой аутентификации и авторизации доступ к информации в сервисах станет более безопасным и контролируемым, а также это добавит удобства конечным пользователям ввиду отсутствия необходимости хранить и запоминать данные аутентификации для разных сервисов.

Платформа OneVizion представляет собой веб-приложение, которое решает проблему управления сложно-связанной информацией различного типа данных. Разработанная платформа интегрирует управление информацией, прогнозирование, управление документами, управление задачами и картографирование Google с целью предоставления полнофункционального программного решения для управления [1].

Был проведен анализ рынка стандартов единой аутентификации и авторизации для корпоративного сегмента, но в виду поступления требования клиента компании OneVizion использовать стандарт SAML для реализации подсистемы Single Sign-On, в данной работе будет использоваться именно SAML.

Целью работы является разработка подсистемы Single Sign-On с использованием стандарта SAML для платформы OneVizion.

Согласно сформулированным требованиям разрабатываемая подсистема должна содержать следующий функционал:

Со стороны идентифицирующего провайдера требуется:

1) Поддержка формата NameID типа EMAIL;

Со стороны сервисного провайдера (подсистема Single Sign-On):

1) Поддержка нескольких идентифицирующих провайдеров;

2) Поддержка различных алгоритмов подписи;

3) Поддержка подписи метаданных;

4) Поддержка возможности загрузки метаданных с заданного URL или

напрямую из XML файла.

5) Возможность выбора идентифицирующего провайдера для прохождения аутентификации на странице аутентификации платформы OneVizion;

6) Уведомление об ошибке в случае неудачной аутентификации на странице аутентификации платформы OneVizion;

7) Уведомление об ошибке в случае возникновения проблем на стороне платформы OneVizion на странице аутентификации платформы OneVizion;

8) Возможность автоматического перенаправления на идентифицирующего провайдера при переходе пользователя в платформу OneVizion;

9) Возможность стандартной аутентификации с использованием пары логин-пароль при включенной возможности из п.8 на странице аутентификации платформы OneVizion;

10) Сохранение в журнал ошибок детальной информации о произошедших проблемах;

11) Возможность настройки SAML через платформу OneVizion, а именно:

a. Добавление/удаление/изменение идентифицирующих провайдеров;

b. Выбор алгоритма подписи;

c. Возможность установления сертификата/приватного ключа для подписи в формате X.509 (PEM кодировка);

d. Возможность отключения формы стандартной аутентификации с использованием пары логин-пароль на странице аутентификации платформы OneVizion;

e. Возможность выбора идентифицирующего провайдера по умолчанию (при переходе в платформу OneVizion пользователь будет автоматически направляться именно на него);

В результате выполнения проекта был разработан интерфейс для конфигурирования идентифицирующего провайдера (рис. 1). Форма конфигурации включает в себя указание имени провайдера (видимое пользователю), выбор источника XML данных (HTTP(S) URL адрес или ручная вставка содержимого XML), выбор идентификатора сущности из списка,

загруженного непосредственно из XML и указание является ли данный идентифицирующий провайдер выбором по умолчанию.

The screenshot shows the 'Administer SSO Providers' interface. At the top, there are buttons for 'Add', 'Edit', and 'Delete'. Below is a table with columns: ID, SAML Provider Meta Source, SAML Provider Meta URL, SAML Entity ID, Default Provider, and Enabled. A row is selected with ID 10009102124, SAML Provider Meta URL https://idp.ssocircle.com, SAML Entity ID https://idp.ssocircle.com, Default Provider Yes, and Enabled Yes. A modal dialog titled 'Edit SSO Provider' is open, showing the configuration for this provider. It includes fields for SSO Provider Type (SAML), Name (SSOCircle), SSO Provider Certificate Chain (Setup), SAML Provider Meta Source (HTTP(S) URL), SAML Provider Meta URL (https://idp.ssocircle.com), SAML Provider Meta XML Data (Setup), SAML Entity ID (https://idp.ssocircle.com), Default Provider (checked), and Enabled (checked). A warning message at the bottom states: 'Warning! Changes will take effect after server restart.' At the bottom of the dialog are 'OK', 'Cancel', and 'Save/Apply' buttons.

*Рис. 1. Таблица и форма конфигурирования Single Sign-On провайдера*

Для общих настроек сервисного провайдера были добавлены т.н. системные параметры (рис. 2), а именно группа «Single Sign-On» и набор из более 10 настраиваемых параметров.

The screenshot shows the 'System Parameters' interface. At the top, there are buttons for 'Edit' and search. Below is a table with columns: #, System Parameter, Value, and Description. A section titled 'Single Sign-On (12)' is expanded, showing the following parameters:

#	System Parameter	Value	Description
10009309	EnableSSOLogin	YES	Enable ability to authorize with help of SAML Identify Provider or OpenID Provider. Notes: when changed, all active SSO sessions won't be destroyed. Web server restart is required when parameter changed.
10009315	RequireArtifactResolveSigned	YES	Web server restart is required when parameter changed
10009316	RequireLogoutRequestSigned	YES	Web server restart is required when parameter changed
10009317	RequireLogoutResponseSigned	YES	Web server restart is required when parameter changed
10009313	SSLHostnameVerification	default	Algorithm for verification of match between hostname in URL and hostname in the presented certificate. default - Standard hostname verifier. defaultAndlocalhost - Standard hostname verifier (skips verification for localhost). strict - Strict hostname verifier. allowAll - Disable hostname verification (allow all). Web server restart is required when parameter changed

*Рис. 2. Таблица конфигурирования подсистемы Single Sign-On*

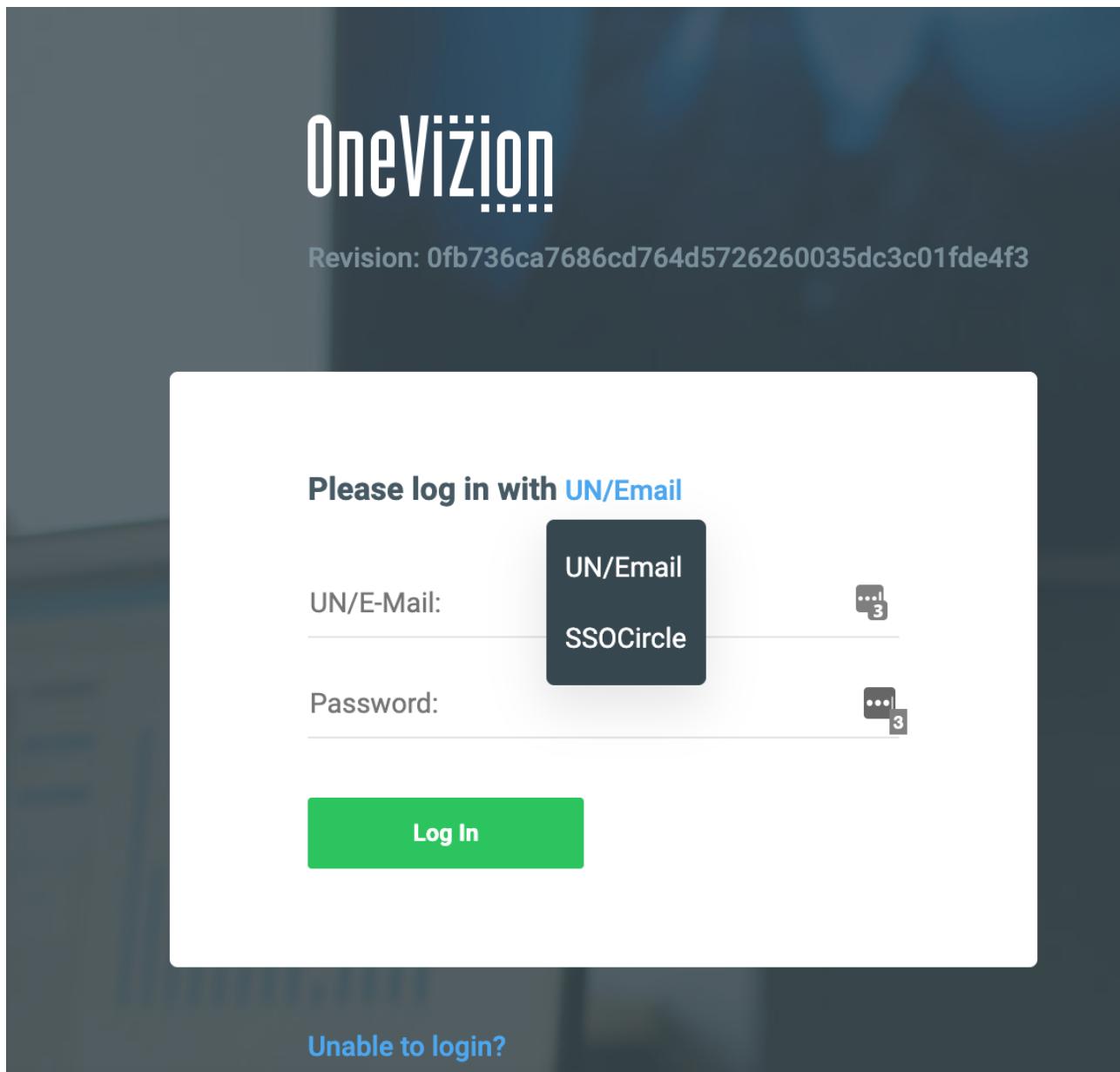


Рис. 3. Форма входа пользователя с выбором способа в платформу OneVizion

В соответствии с требованиями был изменена форма входа пользователя в платформу OneVizion для осуществления возможности выбора способа входа (рис. 3).

Разработанная подсистема удовлетворяет всем поставленным требованиям, была внедрена в платформу OneVizion и прошла этапы ручного тестирования и тестирования в сети клиента компании OneVizion.

### **Список литературы**

1. Павлова, И.С. Компонент графического интерфейса «Конструктор форм» / И.С. Павлова, А.В. Степанюк // Информационно-телекоммуникационные системы и технологии (ИТСиТ-2017): Материалы Всероссийской научно-практической конференции, г. Кемерово, 12-13 октября 2017 г. – Кемерово, 2017. – С. 5-6.