Single Sign On

Функциональная спецификация

Оглавление

[Терминология 3](#_Toc248234748)

[Требуемая функциональность 4](#_Toc248234749)

[Аутентификация (проверка подлинности) 4](#_Toc248234750)

[Авторизация (предоставление прав) 4](#_Toc248234751)

[Аккаунтинг (логирование действий) 5](#_Toc248234752)

[Look and Feel (скины) 5](#_Toc248234753)

[Централизованное управление внешними подсистемами 5](#_Toc248234754)

[Описание экранов 7](#_Toc248234755)

[Логин в подсистему 7](#_Toc248234756)

[Изменение действий в SSO 7](#_Toc248234757)

[Просмотр преференций в SSO 7](#_Toc248234758)

[Конфигурация групп 7](#_Toc248234759)

[Конфигурация комплектов 7](#_Toc248234760)

[Конфигурация пользователя 7](#_Toc248234761)

[Просмотр логов 8](#_Toc248234762)

[Просмотр логов безопасности 8](#_Toc248234763)

[Навигация по экранам 8](#_Toc248234764)

# Терминология

Подсистема (sub system) – приложение поддерживающее интеграцию с SSO.

Действие (action) – право пользователя на выполнение какого либо действия в подсистеме.

Группа – набор действий, используется для упрощения назначения типичных наборов действия различным пользователям.

Роль – набор групп и действий назначенных пользователю.

Принципал – бизнес роль пользователя в подсистеме подключенной к SSO. Каждому принципалу в подсистеме, соответствует роль в SSO.

Преференция – характеристика отображения визуального интерфейса пользователя вида имя:значение.

Комплект – набор преференций.

# Требуемая функциональность

## Аутентификация (проверка подлинности)

Аутентификация пользователя должна осуществляться таким образом, чтобы пользователь не смог определить, что есть единый центр, используемый для всех контролируемых подсистем.

Sub System

SSO

USER

Authentication

SSO module

Ввиду того что центр аутентификации будет единственным, при недоступности сервера SSO вход в систему будет невозможен. Никаких видимых перенаправлений в браузере пользователя быть не должно. Все возможное общение между SSO и подсистемами должно производится по шифрованным каналам. На последнем обсуждении было предложено использовать подписанные клиентские сертификаты для авторизации подсистемы и ssl канал для общения c SSO.

## Авторизация (предоставление прав)

Одному пользователю могут быть выданы права на несколько подсистем, а так же один или несколько принципалов в одной подсистеме. Конкретная подсистема, на которую будет сформирован тикет со списком возможных действий, должна определятся по тому, с какого именно сайта пользователь пытался произвести логин, без оповещения об этом пользователя. К примеру, пользователь Кирилл имеет права на все подсистемы. Если он пытается логинится на Interpayments то на SSO должен придти уникальный идентификатор подсистемы Interpayments. По данному идетификатору определяется компонент и список разрешенных действий для этого компонента.

USER

login password interpayments

SSO

login password

InterPay

interpayments action list

login password adnet

login password

Adnet

adnet action list

Загрузка и обновление списка разрешенных действий должны производиться автоматически при запуске подсистемы. Таким образом, часть системы SSO должна быть интегрирована в каждое Java приложение.

Sub System

sub system startup

SSO

sub system action list

Authorization

SSO module

Если подсистема уже была зарегистрирована ранее, список действий данной подсистемы должен быть полностью обновлен для всех ролей и пользователей.

Одновременно с определением списка действий – оперделяется список ролей и принципалов – с правами, которых пользователь может войти в данную подсистему. Если у пользователя более одной роли – то ему должен быть предложен список всех доступных ему ролей для выбора. Все действия разрешенные роли, которые присвоены ей при помощи связи роли с группой, по умолчанию разрешены. Все действия, права на которые выданы роли непосредственно через связь роли с действиями, по умолчанию запрещены. Права на действия выданные данным способом должны быть подтверждены на уровне конкретного пользователя.

## Аккаунтинг (логирование действий)

При получения тикета со списком разрешенных действий для конкретного пользователя, на каждое действие может быть установлен дополнительный флаг – произвести логирование этого действия при его вызове пользователем. Логирование производится на стороне SSO. Во избежание постоянного обращения внешних подсистем к системе SSO и создание на сервере аутентификции излишней нагрузки, сброс данной информации должен производиться массово. Сброс логов может быть произведен при наступлении любого из 3-х событий:

* лимит по времени сбора
* лимит по количеству записей
* принудительный сброс (к примеру, при остановке приложения)

## Look and Feel (скины)

Помимо списка допустимых действий SSO будет так же содержать информацию позволяющую изменить внешний вид конечной страницы отображаемой пользователю. Данная функциональность будет разработана во второй фазе. Назначением данной функциональности является возможность изменения стилей отображения и верстки при одном и том же наборе прав.

К примеру, имеется два менеджера, подключенных на одну и ту же подсистему. Один менеджер видит зеленый интерфейс с блочной версткой в зеленой цветовой гамме и логотипом «People can fly». Все пользователи управляемые этим менеджером при входе в данную подсистему будут так же видеть блочную верстку в зеленой цветовой гамме. Второй же менеджер, как и его пользователи – будет видеть красную табличную верстку, с логотипом «Люди умеют летать».

Для упрощения администрирования и распределения пользователям стилей отображения – комплекты, объединяющие свойства отображения, будут иметь древовидную структуру наследования. Конфигурация комплектов будет производиться на стороне SSO. Заполнение комплектов свойствами отображения необходимо производить по аналогии с действиями и ролями при запуске приложения.

## Централизованное управление внешними подсистемами

Главное назначение системы SSO – это централизованное управление правами пользователей на каждой из подсистем. Данная функциональность будет достигаться следующим образом.

* при регистрации списка действий модуль авторизации сохраняет на стороне SSO информацию, при помощи которой возможен коллбэк на подсистему со стороны SSO
* добавление пользователя производится на стороне SSO
* после добавления пользователю можно назначить права на конкретную подсистему, выбор подсистемы производится средствами SSO
* права назначаются посредством выдачи необходимой роли или уточнения роли дополнительными действиями, для выбранного пользователя
* если пользователю необходимо разрешить дополнительное действие, то данное действие, расширяющее роль пользователя должно быть выдано как роли, так и нужному пользователю
* каждая роль имеет в подсистеме аналог в виде принципала внешней подсистемы, список принципалов может быть получен при помощи коллбэк адреса сохраненного подсистемой при доставке в SSO списка прав
* принципал, выбранный пользователем при входе в подсистему, передается в хранимые процедуры совместно с именем пользователя
* при указании принципала производится автоматическое создание пользователя на стороне подсистемы

Таким образом, часть SSO будет находиться не только на стороне Java приложения, но и на каждой БД, контролируемой SSO

# Описание экранов

## Логин в подсистему

Пользователю предлагается ввести данные для авторизации.

Java application server при обращении к SSO получает список принципалов, под которыми пользователь может войти в данную подсистему. Если принципал один происходит автоматический логин. Если принципалов несколько – пользователю выдается экран позволяющий выбрать роль под которой он собирается работать с данной подсистемой в текущий момент времени.

## Изменение действий в SSO

После автоматческой загрузки действий в SSO администратор SSO имеет возможность обозначить необходимость логирования конкретного action. Экран должен предоставлять возможность установки фильтров при помощи которых администратор может выбрать конкретную подсистему – действия которой он хотел бы сконфигурировать.

Список действий, отображаемый на экран – должен быть постраничный ввиду возможно большого объема. При этом по мимо фильтра по подсистеме должна быть возможность указать имя конкретного действия (фильтр с динамической подгрузкой, аналог фильтра – список account number из Adnet). Кроме установки логирования должна быть возможность удаления действия из подсистемы.

## Просмотр преференций в SSO

В отличии от действий кроме просмотра списка преференций других действий не требуется.

## Конфигурация групп

После загрузки списка действия (или его обновления) администратору необходимо объеденить часть действий в группы – для упрощения их назначения пользователям. На экране должны присутствовать фильтры – для выбора подсистемы. Необходимо:

* создание группы
* удаление группы
* клонирование группы
* добавление списка действий в группу
* удаления списка действий из группы

## Конфигурация комплектов

Аналогично конфигурации групп, только работаем с преференциями. Только необходимо учитывать, что комплекты могут быть иерархичными. Так что само отображение есть смысл сделать несколько другим.

## Конфигурация пользователя

Все пользователи контролируемых подсистем первым делом заносятся в SSO и только потом вызовом callback процедур прописываются в каждой подистеме грантованой пользователю. Необходима возможность:

* создание пользователя
* клонирование пользователя со всеми правами с присваиванием ему нового имени
* установка и смена пароля
* блокировка аккаунта
* просмотр списка пользователей со всеми атрибутами согласно БД (locked, logins failed, last login date, username, password)
* поиск пользователя по: имени, роли, комплекту, подсистеме
* просмотр ролей пользователя
* просмотр комплектов пользователя
* назначение пользователю роли
* назначение пользователю комплекта (пока назначение индивидуальной преференции не планируется)
* назначение пользователю действия (список доступных действия должен определятся на основании логики подсистемы и грантованых ролей, действия не грантованное роли, которой обладает пользователь, не может быть грантовано напрямую)

## Просмотр логов

Для отслеживания производимых операций необходим экран для просмотра логов. На экране требуются фильтры по:

* подсистема
* дата
* имя пользователя (фильтр с динамической подгрузкой)
* название опреции (фильтр с динамической подгрузкой)

По умолчанию экран должен отображать логии за последний час. Экран должен быть постраничный.

## Просмотр логов безопасности

Для отслеживания попыток подбора пародей необходим экран для просмотра логов безопасности. На экране требуются фильтры по:

* подсистема
* дата
* имя пользователя (фильтр с динамической подгрузкой)

По умолчанию экран должен отображать логии за последний час. Экран должен быть постраничный.

## Навигация по экранам

Отталкиваться будем от экрана по пользователям.

Логи доступа

Просмотр преференций

Логи безопасности

Изменение операций

Конфигурация группы

Конфигурация комплекта

Конфигурация пользователя