RooX UIDM — решение для централизованной аутентификации и авторизации

Оглавление

Решение RooX UIDM предназначено для централизованной аутентификации и авторизации пользователей в веб- и мобильных приложениях.

Поддерживается более 30 популярных в современном вебе и одновременно безопасных способов проверки учетных данных.

Способы входа могут сочетаться между собой в зависимости от предпочтений пользователя или политик безопасности компании.

Доступ к системам работает по технологии единого входа, когда сессия существует на сервере аутентификации, а между сервисами пользователь переходит бесшовно.

В части авторизации доступна ролевая модель, атрибутная модель доступа.

Возможен режим централизованного предоставления доступа (сервисы делегируют авторизацию центральному серверу, а центральный сервер принимает решение разрешить или запретить доступ) и/или децентрализованного, когда сервисы самостоятельно принимают авторизационные решения на основании утверждений о пользователях (клеймов), содержащихся в выдаваемом ему токене доступа. Среди утверждений (клеймов) могут быть идентификатор пользователя, членство в группах согласно организационной модели, наличие ролей, контактные данные, геолокация, использованный способ аутентификции и другие.

Система подробно протоколирует действия пользователей в локальную СУБД (аудит). Имеется встроенная возможность отправки событий безопасности во внешние системы противодействия мошенничеству (антифрод), ELK и веб-аналитики. Перечень и состав событий строго регулируется.

RooX UIDM соответствует требованиям ГОСТ Р 57580, OWASP, NIST в части задач аутентификации и авторизации.

Возможности аутентификации конечных пользователей

- По логину и постоянному паролю
- По логину и одноразовому (временному) паролю
- По номеру телефона и одноразовому паролю (OTP по sms)
- По номеру телефона и одноразовому паролю (OTP по email)
- OTP в мобильное приложение (push)
- TOTP на внешнем приложении (Я.Ключ, Google Authenticator)

- Биометрия (WebAuthN)
- Биометрия (ЕБС)
- Доверенное «знакомое» устройство
- Magic link (разовая ссылка на email)
- QR-код
- Внешние IDP Government: ЕСИА
- Внешние IDP Government: СУДИР (mos.ru)
- Внешние IDP: ВКонтакте
- Внешние IDP: Одноклассники
- Внешние IDP: Яндекс
- Внешние IDP: X (Twitter)
- Внешние IDP: Google
- Внешние IDP: Microsoft
- Внешние IDP: sso-вход через другой корпоративный сервис
- Клиентский сертификат
- КЭП/УКЭП
- Аппаратные токены
- Автоматическая аутентификация в домене Windows по протоколу Kerberos
- С использованием учетной записи в одном или нескольких серверах каталогов Active Directory или другом LDAP-совместимых
- По учетной записи, хранящейся в другой системе
- Использование учетной записи от лица другой учетной записи с ее согласия (мультиаккаунт)
- Имперсонация (специальная аутентификация под пользователем с использованием админской учетки)
- Автоматическая аутентификация по номеру телефона в сети телеком-оператора по технологии Header Enrichment
- Аутентификация по долгоживущему токену (включая биометрию устройства, PIN-код, графический ключ)
- С использованием комбинации указанных способов

Возможности самообслуживания конечных пользователей

- Самостоятельная регистрация пользователей с подтверждением email и номера телефона
- Самостоятельная регистрация пользователей через ЕСИА
- Сброс пароля пользователем
- Восстановление пароля пользователем
- Смена пароля пользователем
- Принудительная смена пароля по истечении времени жизни или по команде администратора
- Создание и использование долгоживущих API-токенов

Возможности по защите веб-приложений

- Централизованная аутентификация веб-приложений согласно протоколу OAuth2.0

- Централизованная аутентификация веб-приложений согласно протоколу OpenID Connect
- Централизованная аутентификация веб-приложений согласно протоколу OAuth1
- Централизованная аутентификация веб-приложений согласно протоколу SAML
- Централизованная авторизация действий пользователей
- Обмен токенов согласно протоколу Token Exchange
- Бесшовный переход между приложениями с использованием технологии Single Sign On
- Защита важных операций двухфакторной аутентификацией
- Mobile SDK
- Web SDK
- Java SDK

Возможности администрирования

- Управление пользователями (создание, просмотр, блокировка, изменение данных, сброс пароля)
- Управление приложениями (создание, просмотр, блокировка, смена данных)
- Управление политиками аутентификации и авторизации
- Аудит действий пользователей
- Имперсонация в приложениях от лица управляемой учетной записи

Возможности для информационной безопасности

- Отправка событий в системы противодействия мошенничеству (антифрода)
- Предоставление API блокировки учетных записей, разрыва сессий, блокировки приложений
- Детальное протоколирование действий (аудит) с хранением в СУБД. В состав данных протоколируемого события входит субъект доступа, объект доступа, контекстная информация: сетевые адреса, геолокация, свойства браузера или мобильного приложения
- Ролевая, атрибутная модели доступа
- Автоматизация правил предоставление и отзыва доступа. UIDM инициирует выполнение бизнес-процессов, запускающихся по событиям безопасности (регистрация, вход, выход, блокировка) в интеграции с BPMN Camunda или другой по запросу

Архитектурные возможности

- Производительная система записи аудита (асинхронная, партиции)
- Хранение токенов в Tarantool (высокопроизводительная инсталляция)
- Сквозное протоколирование
- Историчная СУБД (мягкое удаление записей, хранение всех версий объектов)
- Мультиорганизационная модель данных
- Микросервисная архитектура
- Горизонтальное и вертикальное масштабирование, в том числе автоматическое при использовании оркестратора Kubernetes или аналогичного
- Использование современного инфраструктурного стека: Docker, ELK, K8S, Vault

Возможности по доработке

- Разработка новых модулей аутентификации
- Изменение UI-представления сценариев аутентификации
- Разработка новых сценариев аутентификации
- В составе продукта имеются SDK: серверная Java (Spring, Pure Java), C#, Android, IOS