permalink: / redirect_from: - /index ---

Полный перечень функциональных возможностей

Назначение

Продукт Unified Identity Management предназначен для централизованной аутентификации и авторизации пользователей в веб-приложениях.

Поддержаны популярные в современном вебе и одновременно безопасные способы проверки учетных данных: пароль, одноразовый пароль, TOTP, ЕСИА, соцсети, Google, ПИН-код, биометрия).

Способы входа могут комбинироваться 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 в центральный сервер, а центральный сервер принимает решение разрешить или запретить доступ) и/или децентрализованного, когда сервисы самостоятельно принимают авторизационные решения на основании утверждений в токене доступа. Среди утверждений могут быть идентификатор пользователя, членство в группах согласно организационной модели, наличие ролей, контактные данные, геолокация, способ входа и другие.

Система записывает подробный аудит действий пользователей в локальную СУБД. Имеется встроенная возможность отправки событий безопасности во внешние системы: Антифрод, ELK, веб-аналитика. Перечень и состав событий строго регулируется.

Unified Identity Management обеспечивает соответствие требованиям ГОСТ Р 57580, OWASP, NIST в части задач аутентификации и авторизации. Перечень функциональных возможностей

Возможности аутентификации конечных пользователей

- По логину и постоянному паролю
- По номеру телефона и одноразовому паролю
- По логину и одноразовому паролю с использованием технологии Time Based Onetime

Password

- Через социальную сеть ВКонтакте, Одноклассники, Facebook, Twitter
- Через поставщиков учетных записей ЕСИА, Google, Microsoft, Яндекс
- Через долгоживущий токен (“запомнить меня”)
- По сертификату КЭП
- С использованием учетной записи в сервере каталогов Active Directory или другом LDAP-совместимом
- Автоматическая аутентификация по номеру телефона в сети телеком-оператора по технологии Header Enrichment
- Автоматическая аутентификация в домене Windows по протоколу Kerberos
- По учетной записи, хранящейся в унаследованной системе с мягкой миграцией учетной записи в БД UIDM
- Использование учетной записи от лица другой учетной записи с ее согласия (мультиаккаунт)
- С использованием комбинации указанных способов

Возможности самообслуживания конечных пользователей

- Саморегистрация с подтверждением email и номера телефона
- Саморегистрация 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 приложения 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 антифрода
- Предоставление API блокировки учетных записей, разрыва сессий, блокировки приложений
- Хранение детального аудита действий в субд. В состав событий 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