Аутентификация в мобильном приложении с использованием ПИН-кода или биометрических данных

Оглавление

Описание

UIDM позволяет реализовать в мобильном приложении сценарии аутентификации с использованием ПИН-кода и/или биометрическим данным, используя механизм долгоживущих идентификационных токенов.

ЗАМЕТКА

Описанная далее функциональность аутентификации с использованием биометрических данных предполагает использование биометрических средств мобильных устройств, на которых работает мобильное приложение. Мобильное приложение не является частью UIDM. В UIDM реализованы и другие механизмы для работы с биометрическими данными; обратитесь в RooX для получения дополнительной информации.

Сценарий аутентификации в мобильном приложении с использованием ПИН-кода или биометрических данных

Аутентификация пользователя по ПИН-коду или биометрии реализуется по следующему сценарию:

ЗАМЕТКА

Реализация сценария на стороне мобильного приложения может отличаться и остается на усмотрение разработчиков мобильного приложения.

1. Пользователь первый раз запускает мобильное приложение. Приложение запрашивает логин и пароль, пользователь вводит их, приложение направляет данные в UIDM.
2. UIDM, если логин и пароль верны, выдает токен доступа приложению, а также дополнительно долгоживущий идентификационный токен (JWT). JWT-токен **НЕ** сохраняется на стороне UIDM; он представляет собой зашифрованную строку в формате JSON, внутри которой, помимо прочего, хранятся идентификатор (principalId пользователя) и время жизни токена.
3. Мобильное приложение запрашивает у пользователя ПИН-код и/или биометрические данные, использует их для шифрования полученного JWT-токена и сохраняет результат в хранилище на мобильном устройстве.
4. Когда пользователь в следующий раз выполняет попытку аутентификации с использованием ПИН-кода или биометрических данных, мобильное приложение загружает токен из хранилища и расшифровывает его с использованием введенного ПИН-кода или биометрических данных.

5. Мобильное Приложение направляет в UIDM запрос на аутентификацию, передавая JWT-токен.
6. UIDM расшифровывает JWT-токен, проверяет, не истек ли срок его действия, находит в БД учетную запись пользователя по principalID пользователя и аутентифицирует его.
7. UIDM возвращает успешный ответ в Мобильное приложение. Если на предыдущем шаге произошла ошибка (например, токен более недействителен), то UIDM передает в мобильное приложение сведения о другом доступном способе аутентификации для продолжения сценария (например, запрашивает ввод логина и пароля)

Компоненты, необходимые для работы функциональности аутентификации в мобильном приложении с использованием ПИН-кода или биометрических данных

Является частью стандартной функциональности UIDM, не требует установки дополнительных компонент

Включение функциональности аутентификации в мобильном приложении с использованием ПИН-кода или биометрических данных

Функциональность не требует специального включения, но в sso-server должны быть настроены ключи для шифрования токенов.