2015 CEE-SEC(R)
Software Engineering Conference in Russia

IBM Bluemix Identity Mixer Service

Облачный сервис авторизации и аутентификации на основе доказательств с нулевым разглашением

Пётр Каламбет,

Тимур Усатый

Version 0 8 6

ВВЕДЕНИЕ

Тимур Усатый

Примеры задач

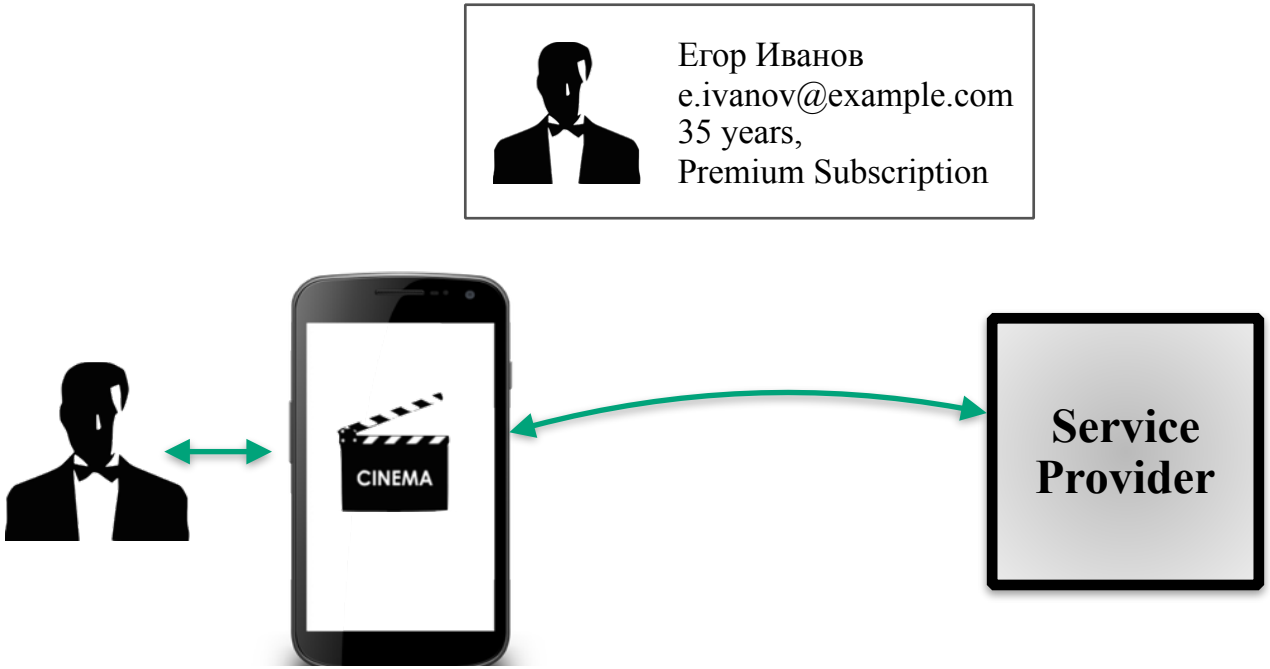
Карты лояльности

Онлайн кинотеатр

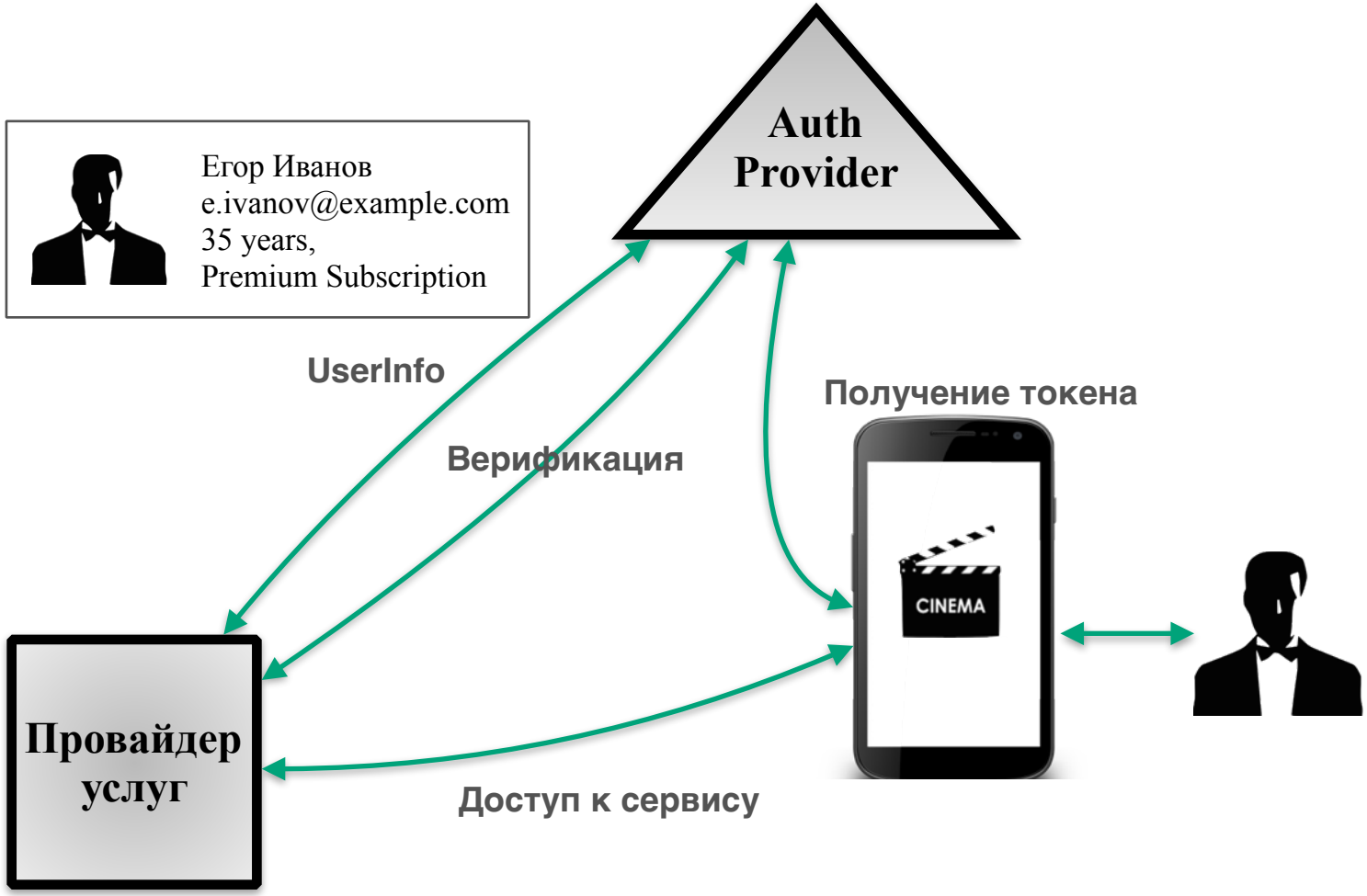
Электронное голосование


Примеры
Сопопросы
Голосование
Электронный
Электронное
Электронные выборы
правительство

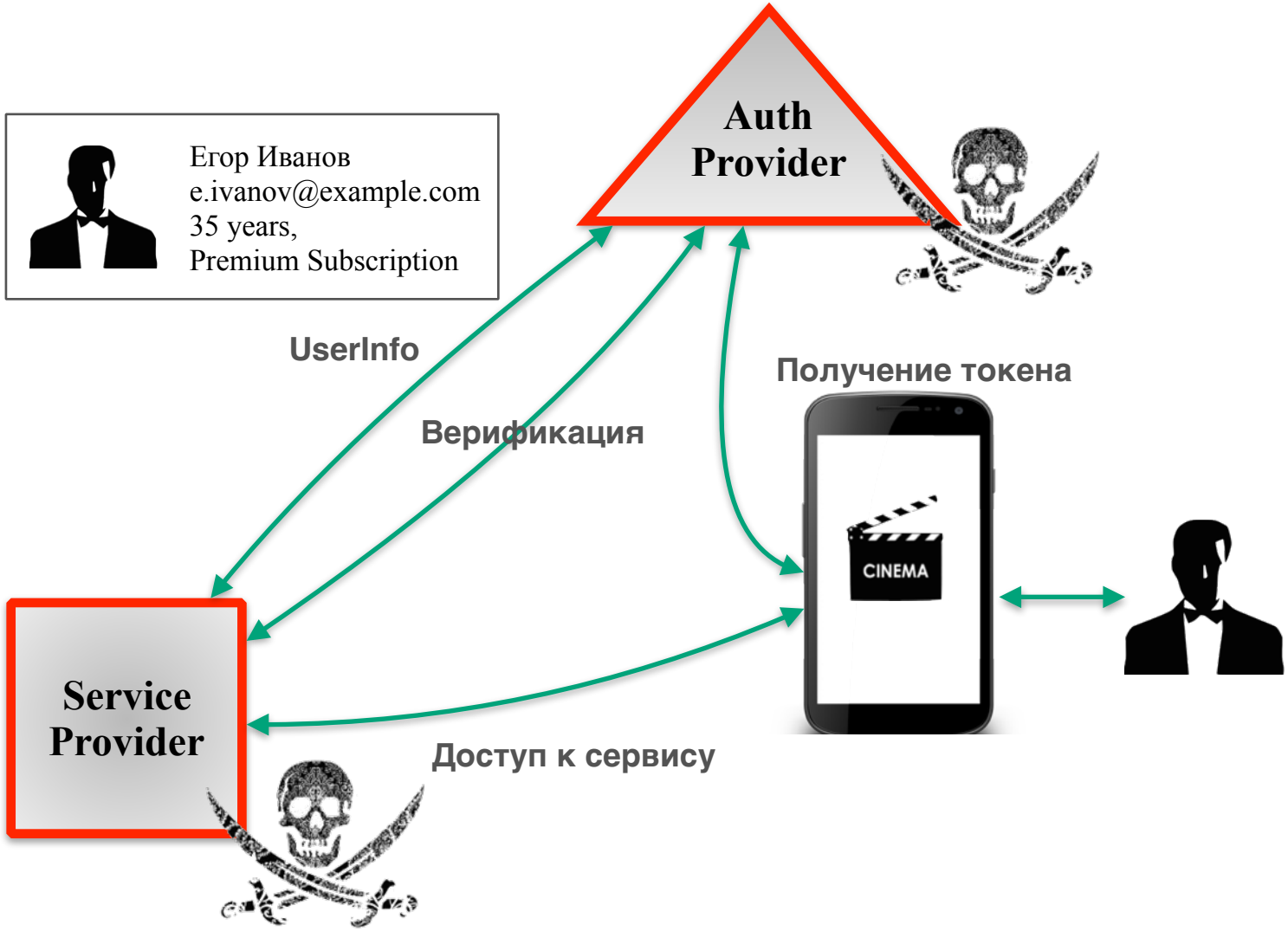
Проблема анонимности



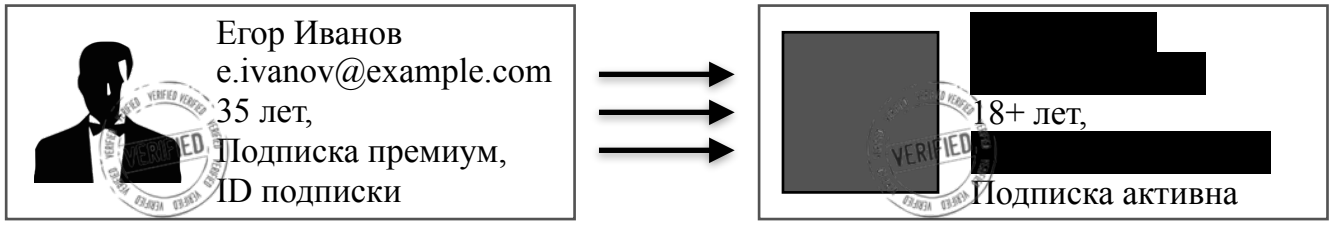
Проблема анонимности



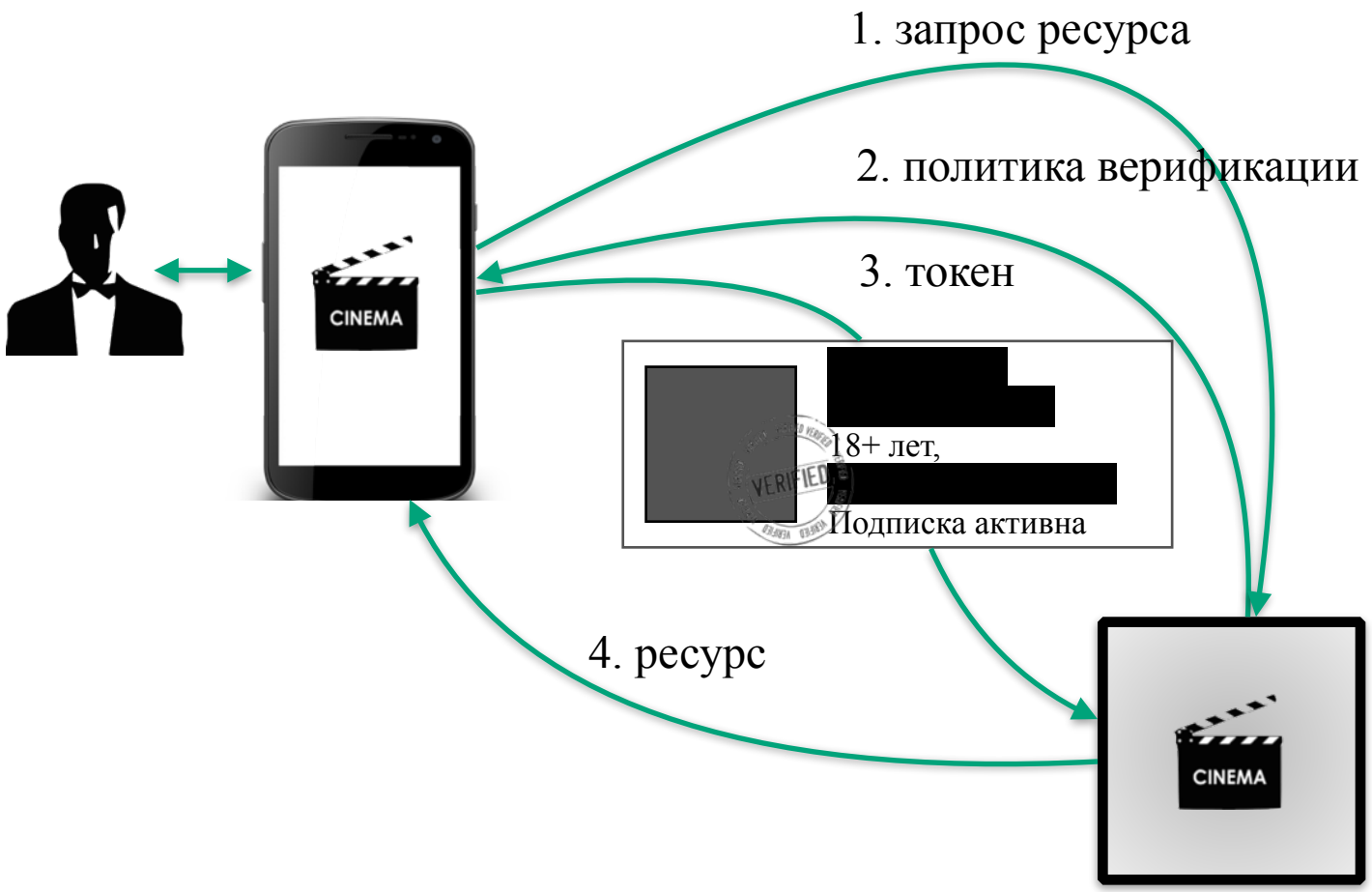
Проблема анонимности



Минимальное раскрытие данных



Пример верификации на основе IDMX



Агенты

Выпускающий агент / Issuance authority

Осуществляет выпуск креденциалов, т.е. группы атрибутов заверенных сертификатом выпускающего органа, согласно заданной спецификации процесса выпуска

Электронный кошелёк / Credential Wallet

Защищённое приложение для хранения данных пользователя (на телефон с защищенным элементом или на смарт-карте). Участвует в процессах выпуска и проверки значений атрибутов

Агент-верификатор / Verifier

Предоставляет пользователю список предикатов для формирования доказательства, проверяет корректность сформированного пользователем токена В процессе взаимодействия с пользователем, доказывается или опровергается наличие требуемой комбинации значений атрибутов пользователя

Агенты

Отзывающий агент / Revocation authority

Управляет отзывом уже выпущенных атрибутов пользователя
Если задействован механизм отзыва, тогда пользователь должен доказать, что его атрибуты, предоставляемые в процессе проверки (verification), не были отозваны

Инспектор / Inspector

В некоторых случаях полная анонимность может провоцировать пользователя на совершение противоправных действий В таком случае значения некоторых пользовательских атрибутов могут быть специальным образом зашифрованы (открытым ключом доверенного инспектирующего агента) В процессе расследования, инспектор может получить доступ к точным значениям атрибутов, расшифровав их с помощью своего секретного ключа

Агенты и взаимодействия между ними

Выпускающий агент

Отзыв

Отзывающий агент

Хранитель кредениалов

Выпуск

Информация об отзыве

Отзыв

Проверка

Инспектор

Запрос и инспекция некоторых атрибутов

Верификатор

Процессы выпуск креденциалов (issuance)

В самом простом варианте выпускающий агент имеет доступ к значениям атрибутов креденциалов пользователя В более сложном, атрибуты выводятся из существующих так, чтобы выпускающий агент не имел к доступа к их значениям Это т н слепой режим выпуска (blinded issuance) В этом случае выпуск осуществляется в интерактивном режиме

Выпуск атрибутов

Шаг 1 Выпускающий агент предоставляет пользователю политику выпуска данных (credentials issuance policy)

Шаг 2 Пользователь формирует и отсылает специальный токен (issuance token), который уже включает в себя презентационный токен (presentation token) Презентационный токен должен удовлетворять условиям политики выпуска данных

Шаг 3 Пользователь получает новые креденциалы

Процессы верификация (verification)

В процессе проверки отдаются только запрашиваемые данные, которые необходимы и достаточны для удовлетворения условиям политики предоставления данных Более того, такие токены не позволяют определить принадлежность одному пользователю, а также не позволяют сопоставить любой такой токен с исходными данными, которые были выпущены для пользователя Также могут запрашиваться не сами данные, а набор производных по данным например, проверить выражение, что возраст пользователя менее 18 лет Так же в некоторых случаях может быть добавлено требование привязки к одному и тому же секретному ключу

Проверка / верификация атрибутов

Шаг 1 Пользователь получает от верификатора политику предоставления данных (presentation policy), в которой описывается, какие значения каких атрибутов пользователь должен предоставить

Шаг 2 Если необходимые данные (credentials) уже были выпущены для заданного пользователя ранее, то в этом случае пользователь формирует специальный токен, удовлетворяющий условиям политики предоставления данных

Шаг 3 Пользователь может получить ответ, пройдена ли проверка

Процессы инспекция (inspection)

Анонимность пользователей может приводить к нежелательным последствиям, таким как рассылка спам-сообщений, публикациям оскорблений и прочим противоправным действиям пользователя в сети В этом случае может помочь процесс инспекции, который позволяет определить точные значения некоторых атрибутов пользователя в рамках, например, полицейского расследования В политике предоставления данных для каждого атрибута пользовательских данных прописывается условие в каких случаях и для каких параметров инспектирующего органа может быть проведена инспекция атрибутов

Инспекция атрибутов

Шаг 1 Инспектор получает от верификатора доступ к презентационным токенам потенциальных нарушителей (токен не может быть поставлен в соответствие какому-либо пользователю)

Шаг 2 Инспектор расшифровывает и исследует данные, которые были зашифрованы публичным ключом данного инспектора

Процессы отзыв (revocation)

В некоторых случаях также необходимо выполнить отзыв уже однажды выпущенных креденциалов пользователя Причины креденциалы были скомпрометированы, устарели или пользователь потерял право на их использование Этим процессом управляют отзывающие агенты (revocation authorities), которые отвечают за публикацию актуальной информации об отзыве креденциалов

Отзыв при поддержке выпускающего агента / Issuer-driven revocation

В этом случае отзывающий агент всегда задан в параметрах выпускающего агента Также в процессе проверки, в токене пользователя всегда должно включаться доказательство того, что креденциалы не были отозваны Это выполняется на основе специального атрибута (revocation handle), который содержится в креденциалах пользователя

Отзыв при поддержке верификатора / Verifier-driven revocation

В отличие от первого способа, проверка на отзыв в рамках верификации носит локальный характер (т е , связанный с данным верификатором) В этом случае производится проверка для некоторой комбинации атрибутов креденциалов пользователя

Криптография

Выпуск и проверка атрибутов

В основе схемы проверки подписи Камениш-Лисянской и Брандса, которые лежат в основе технологий IBM Identity Mixer и U-Prove от Microsoft

Привязка креденциалов к определенному ключу выполняется через атрибут, с идентификатором секретного ключа пользователя

Отзыв также может быть реализован с помощью подписанных списков для отзыва креденциалов, через динамические аккумуляторы или через периодические обновления креденциалов с коротким временем жизни

При формировании токена для верификации применяются дискретные логарифмы и преобразование Фиата-Шамира. Последние также применяются для доказательства равенств, неравенства реализованы с помощью доказательств принадлежности заданному диапазону

В фреймворке ABC4Trust реализована поддержка указанных выше и многих других криптографических примитивов

Материалы

1. https://abc4trust.eu

2 Jan Camenish, Maria Dubovitskaya, Robert Enderlein, Anna Lehmann, Gregory Neven, Christian Paquin, Franz-Stefan Preiss Concepts and Languages for Privacy-Preserving Attribute Based Authentication

3 http://www.geo.ru/nauka/khakery-ne-proidut?page=0#article-body

СПАСИБО

Identity Mixer Service in IBM Bluemix

Пётр Каламбет

С чего всё началось?

Технология IdentityMixer

Большая часть криптографии разработана ещё в 2001 году, но из-за трудностей применения на практике, технология не получила должного внимания публики

https://github.com/credentials/idemix_library

Технология ABC4Trust

В рамках открытого проекта ABC4Trust был разработан фреймворк, который позволяет описывать работу системы с помощью набора спецификаций

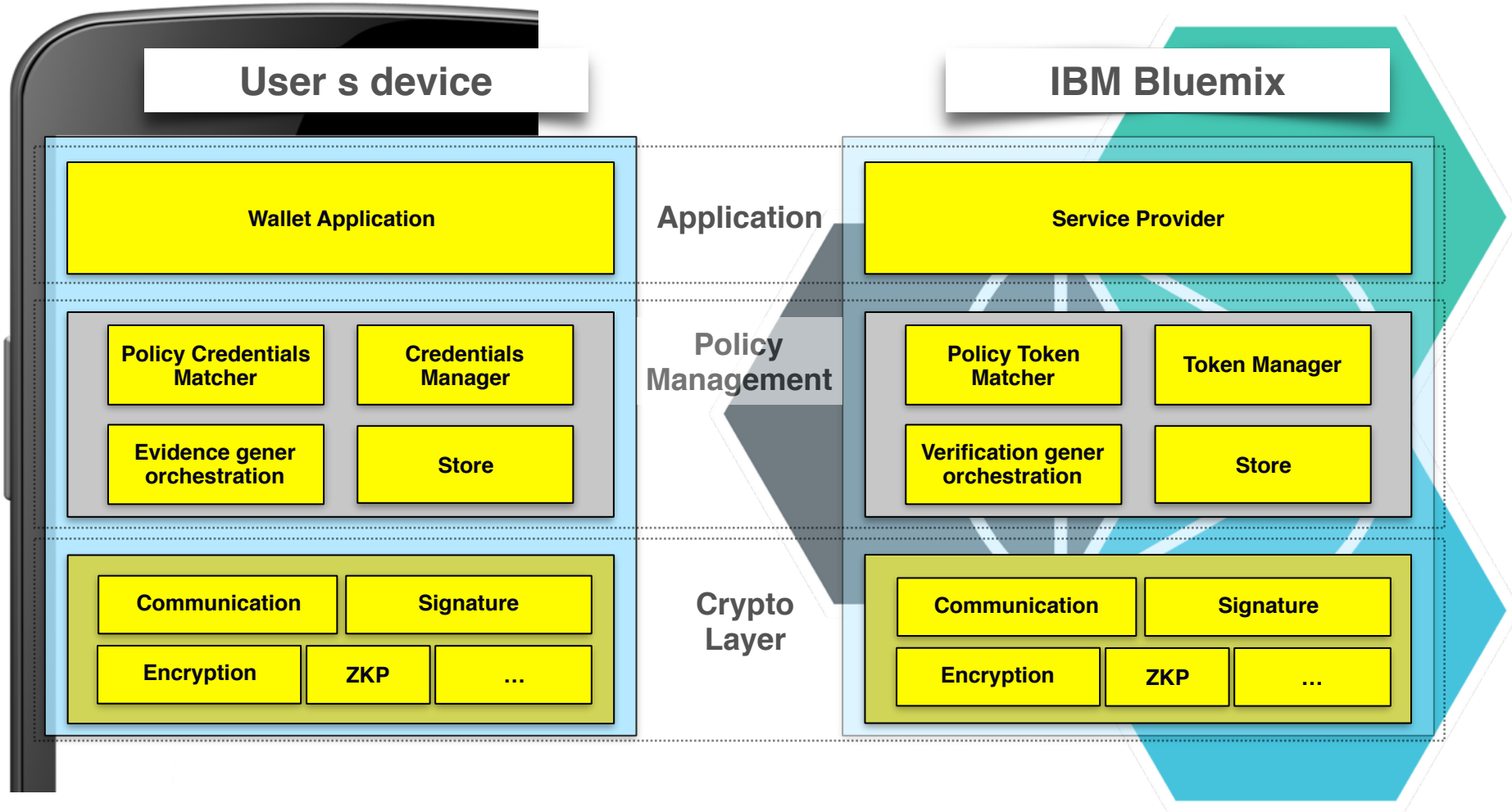
https://github.com/p2abcengine/p2abcengine

Почему сервисы?

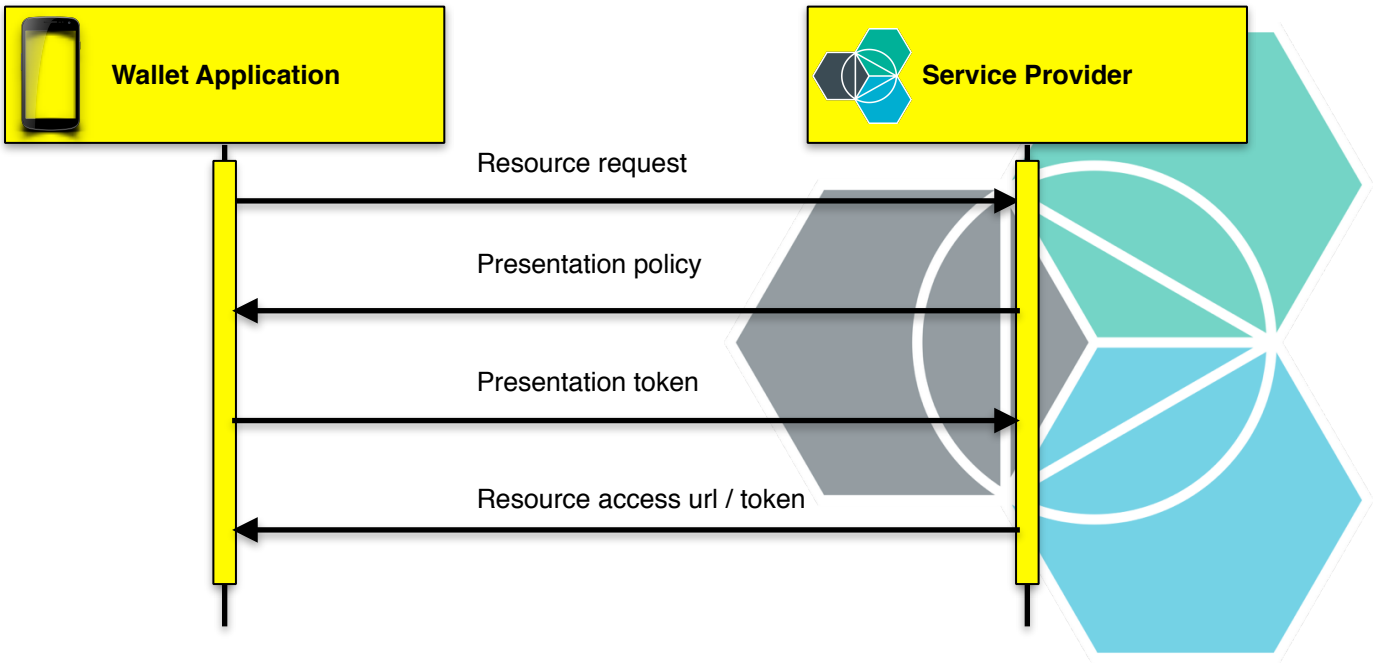
Сервис IdentityMixer на базе облачной платформы IBM Bluemix

Благодаря появлению облачной платформы IBM Bluemix появилась возможность сделать технологию ещё более доступной каждый может создать инстанс сервиса для выпуска или для проверки атрибутов пользователя и сконфигурировать его под свои нужды / требования

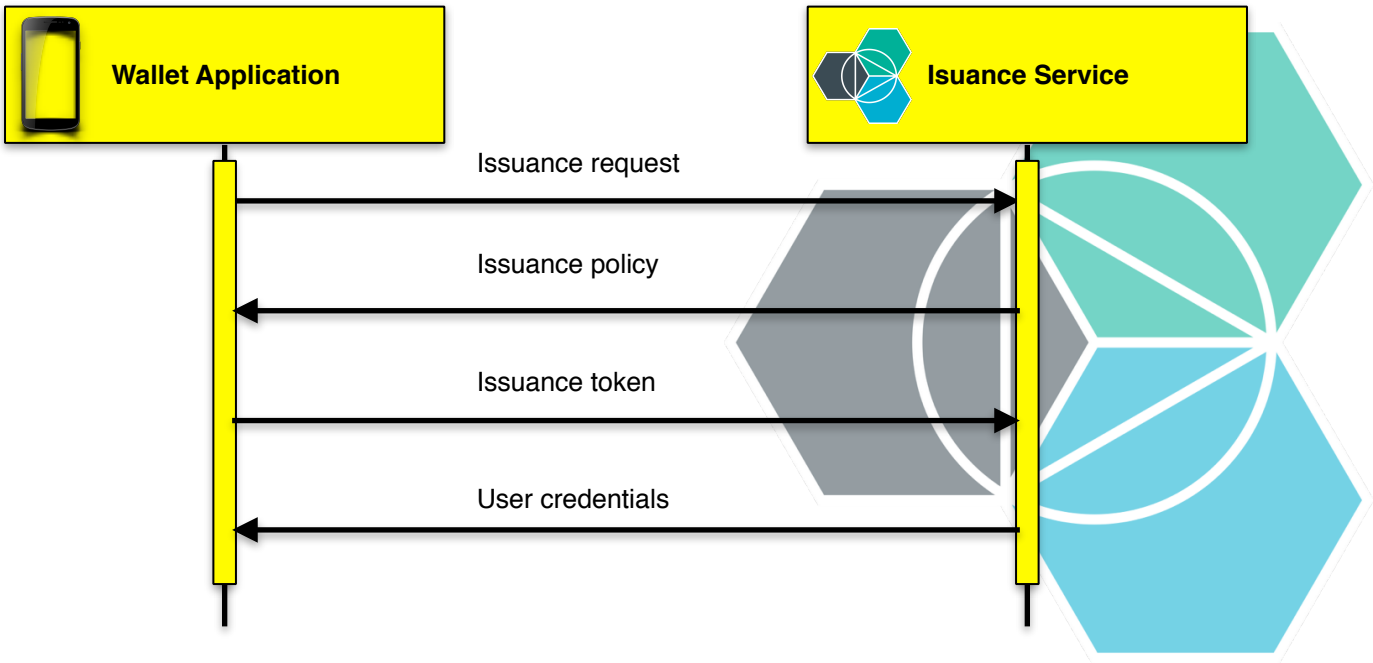
Архитектура



Пример взаимодействия верификация

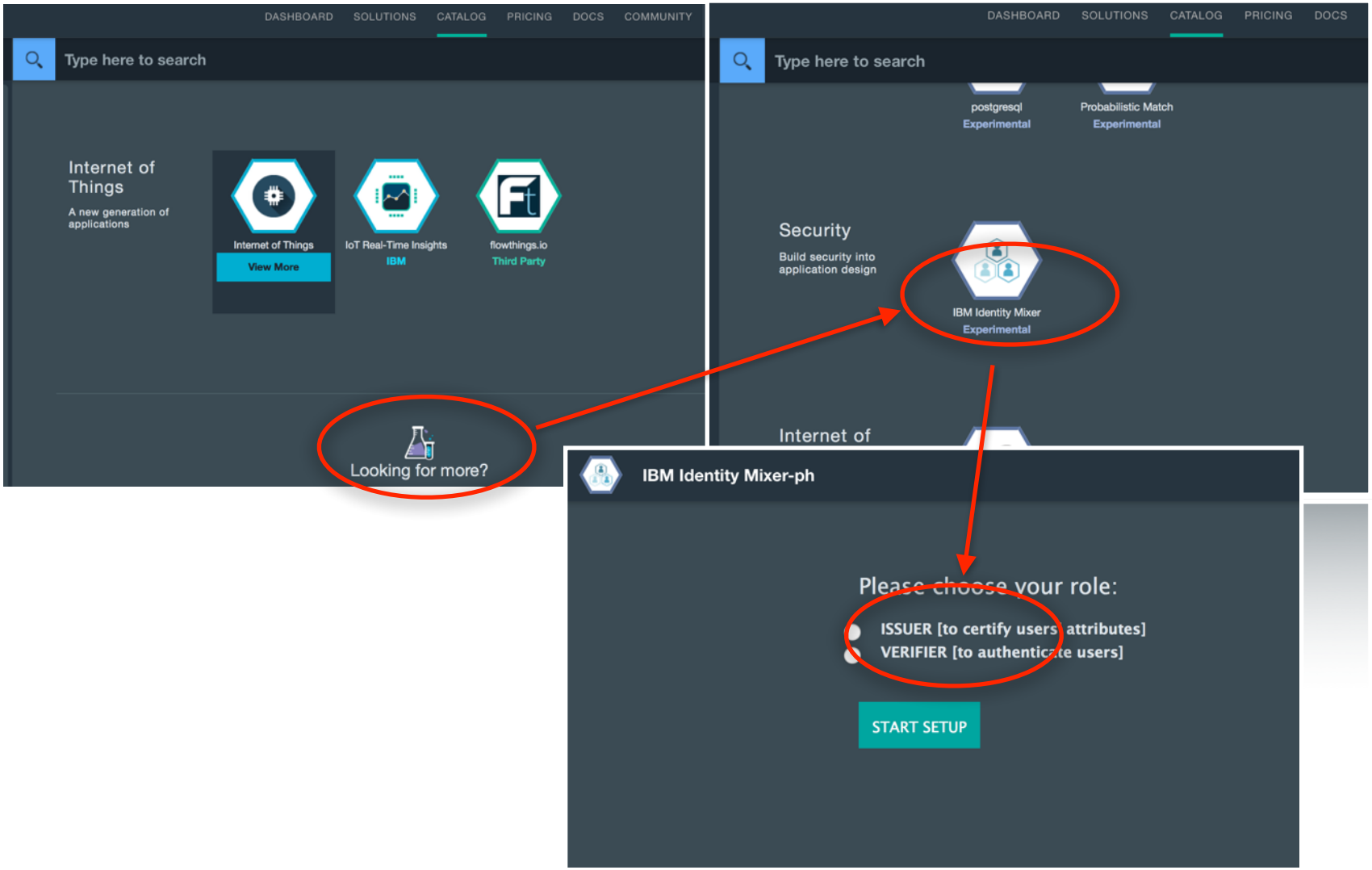


Пример взаимодействия верификация



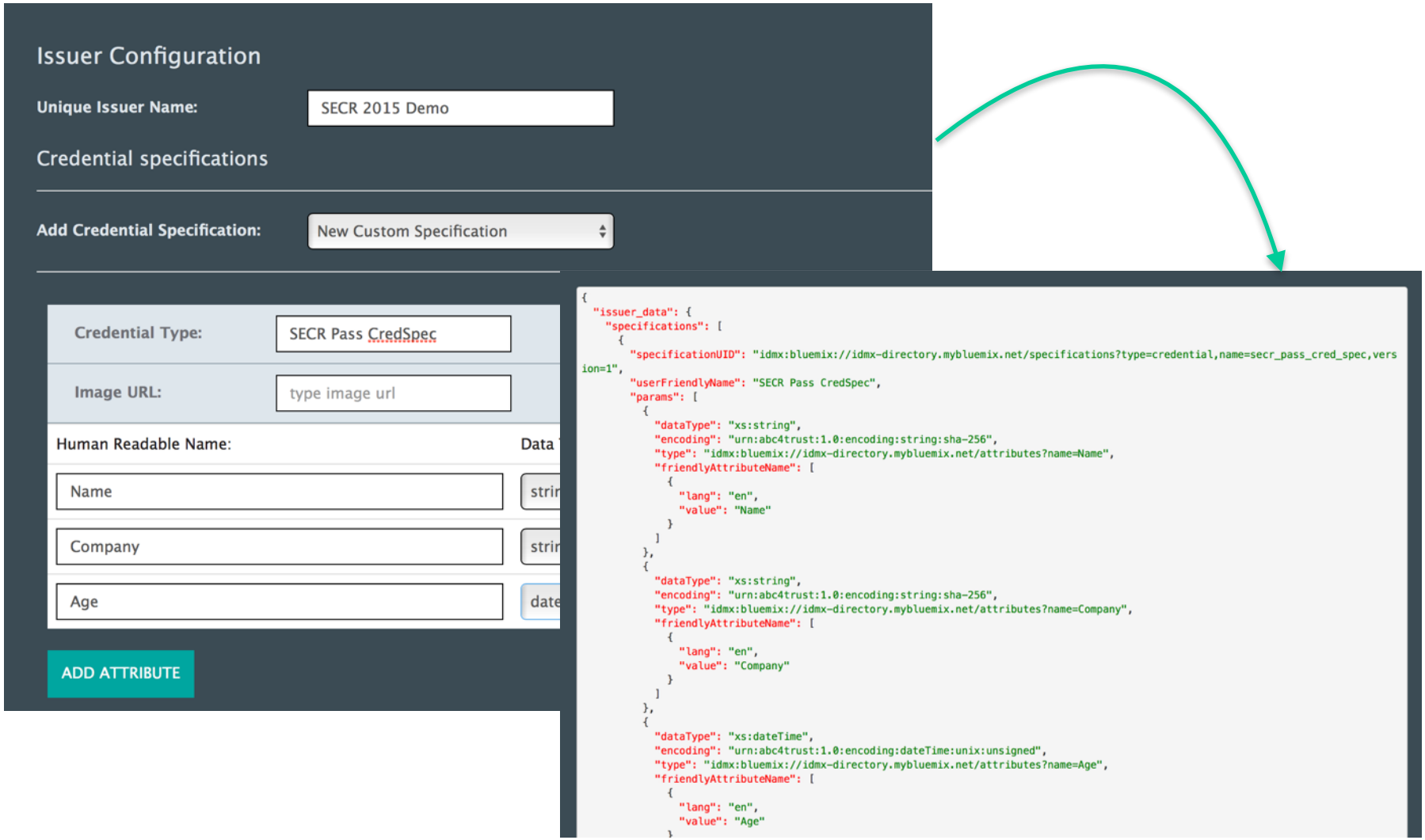
Подключение

Создание нового экземпляра сервиса IdetityMixer



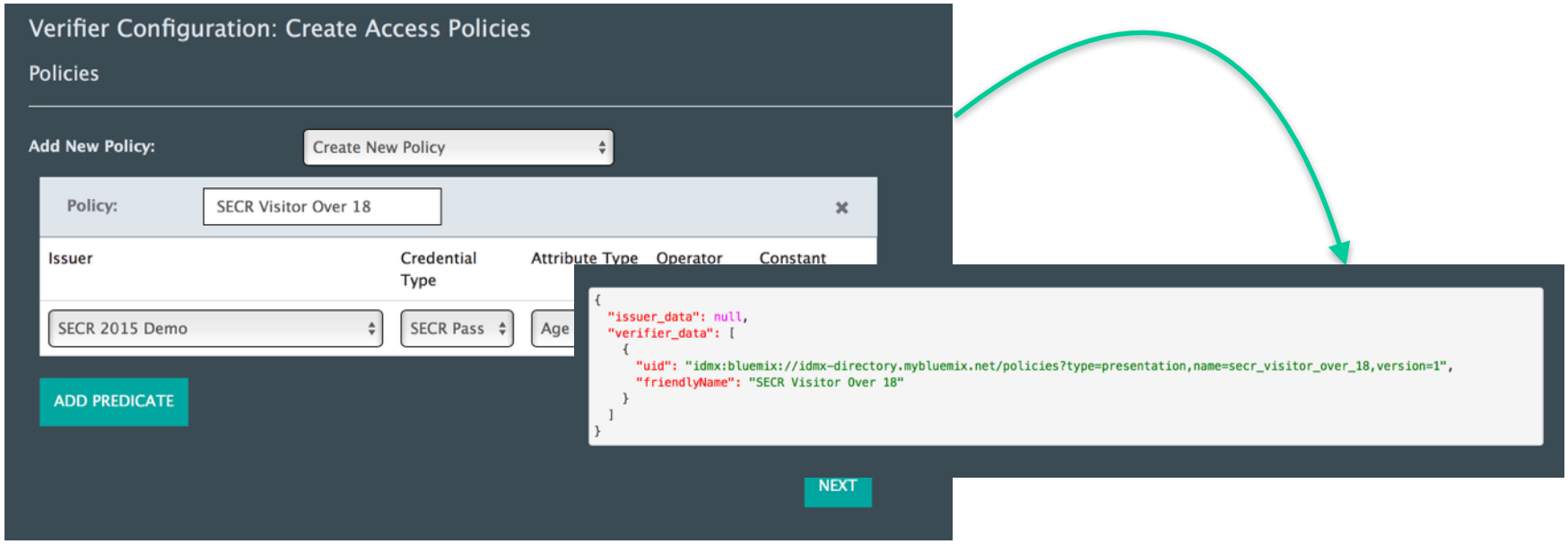
Подключение

Создание нового экземпляра issuer сервиса IdetityMixer



Подключение

Создание нового экземпляра verifier сервиса IdetityMixer



Материалы

1. https://idemixdemo.mybluemix.net демо IBM Identity Mixer
2. https://abc4trust.eu/index.php?option=com_content&view=article&id=187

   более детально про исходные коды Identity Mixer
3. https://www.ng.bluemix.net/docs/services/identitymixer/index.html

   документация к сервису на IBM Bluemix

СПАСИБО