YourID
Trusted Identity Platform

VIGOURSOFT

Updated Proposal For YourID Proof-Of-Concept (PoC)

May 25, 2020 (Post Call on *May 20*)

Background

- The YourID Foundation team intends to create the world's first ever unified trusted Identity Platform, that offers:
  - Technology Agnosticism
  - Cross-Industry Collaboration
  - Shared Governance
  - Password-less Security
- This unified platform will be made up of a combination of ID technologies and will be endorsed by a group of founding participating enterprises that would also consume and offer the services of this platform to their users/consumers
- YourID will be presenting the idea for a PoC to the participating enterprises, for establishing the possibility and viability of such a unified ID platform
- VigourSoft has been asked to present their proposal for this initial PoC based on the requirements shared by YourID

VIGOURSOFT

PoC Objective

- Test the first phase of the YourID platform and obtain feedback about all the different aspects related to the initial features, user experience, integration process, etc. for later improvement.

- Collect all the different requirements, information, ideas and desired functionality per vertical that could provide added value to improve their engagement and interoperability with the subsequent benefit to the customer and YourID platform.

- All this information will be used to plan and prioritize the next features, including customer and business benefit.

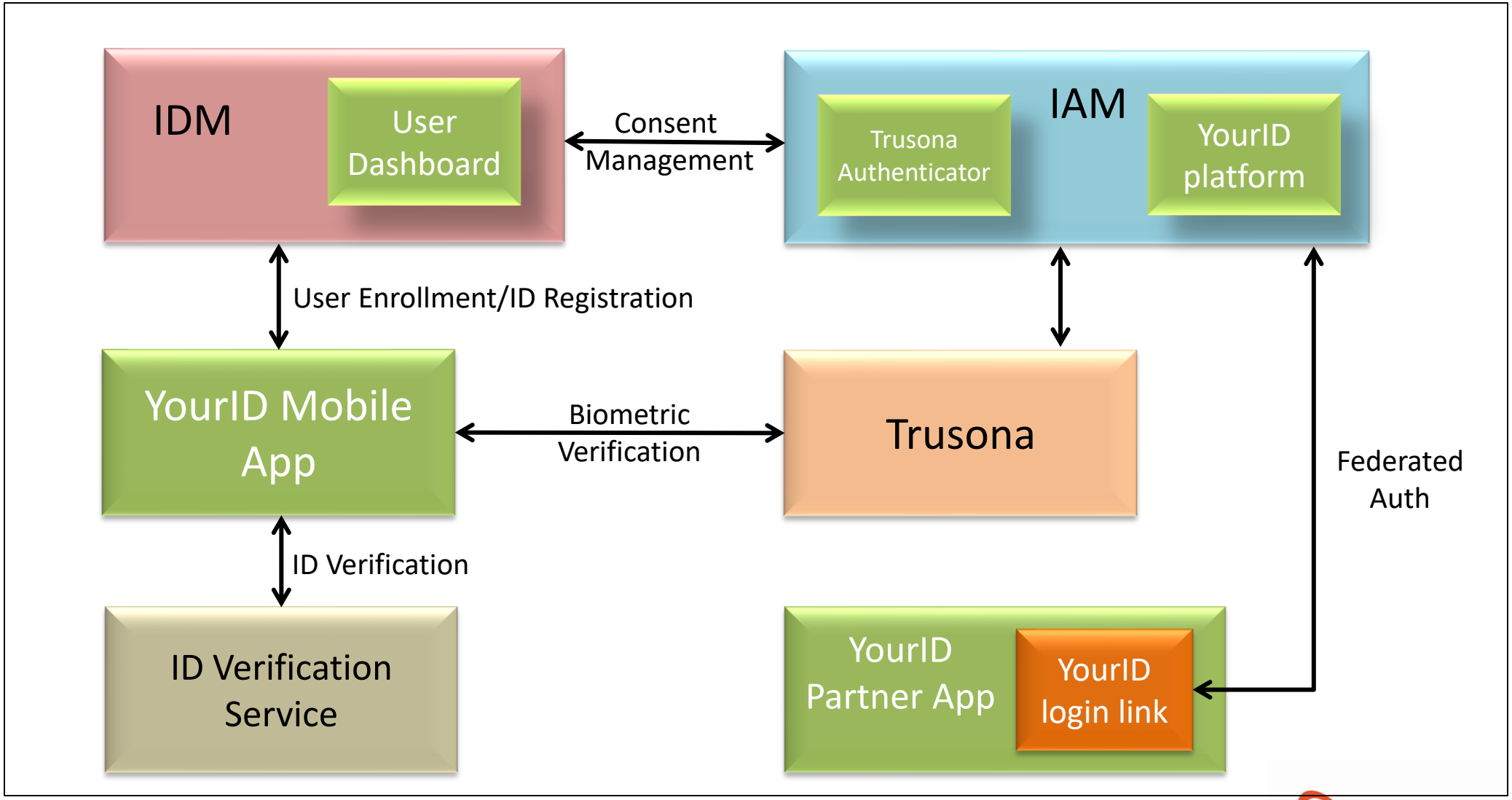
VIGOURSOFT

PoC Functionality

1. YourID Mobile App
    1. Enrolment
    2. Passwordless Login
    3. Biometrics
    4. ID Document Enroll
    5. Consent Management
2. YourID Access
    1. Login and access
    2. Consent
3. YourID User Dashboard (IDM WebApp)
    1. User profile management
    2. User consent management
    3. User device management
    4. ID document management

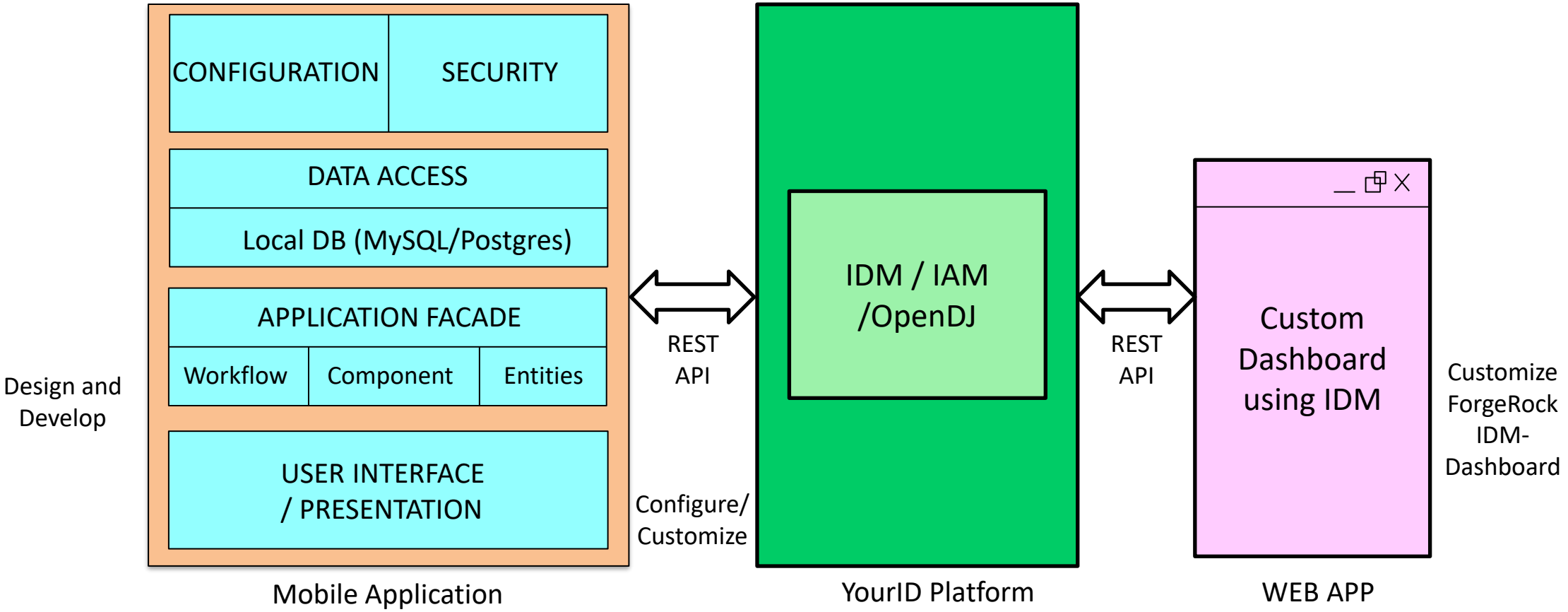
VIGOURSOFT

Proposed Workflow Architecture



VIGOURSOFT

Technical Architecture



VIGOURSOFT

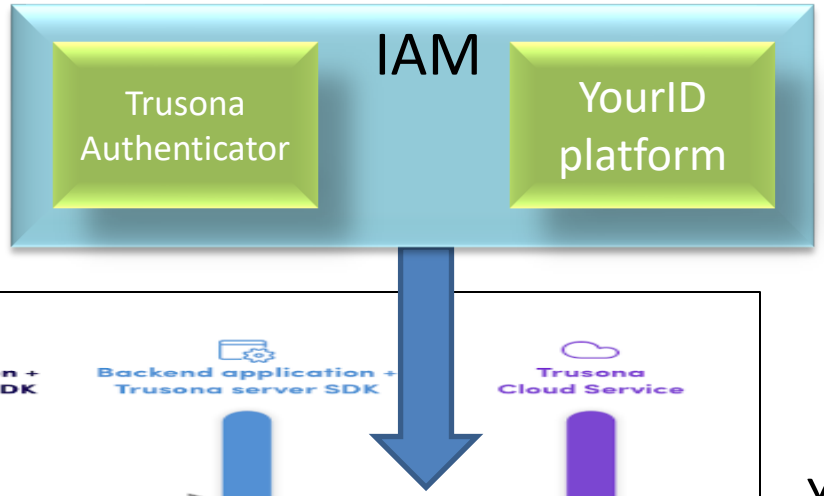
Technical Architecture: Mobile App

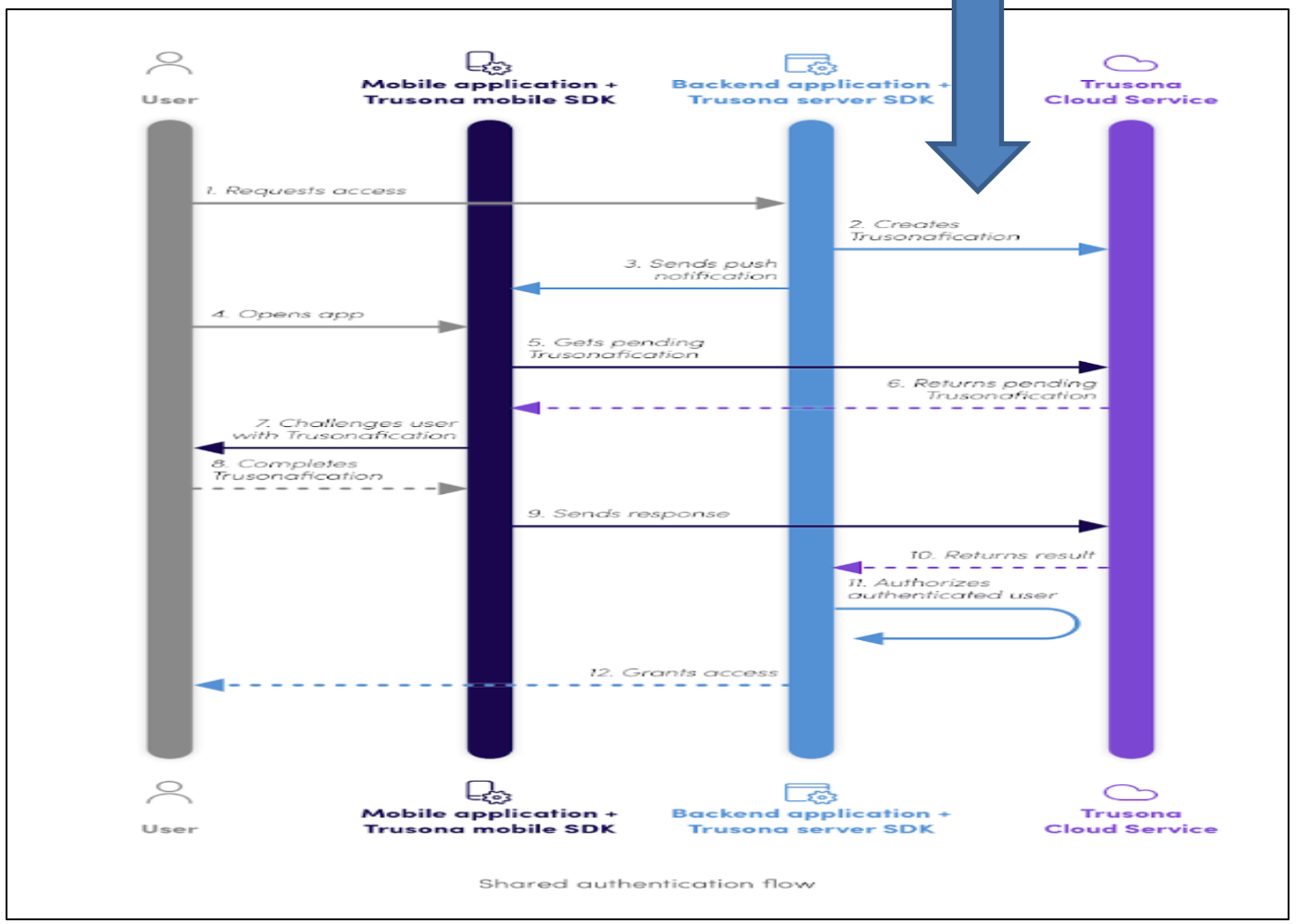
1. **Feature: Enrollment - basic profile (user first/last name, e-mail (validate), phone (validate))**
   a) Design app to take in above 4 inputs and save profile in IDM
      - Call IDM SDK to create user profile

2. **Passwordless Login**
   a) The user will be able to scan the QR in the partner app to login without usernames or passwords. (Trusona integration)
   b) OpenAM needs to be configured with authentication module (Trusona) to achieve passwordless authentication.
   c) Authentication flow needs to be integrated with OpenAM
   d) See pic on next slide

VIGOURSOFT

Flow for Trusona Integration





YourID Platform proxies Trusona Service and returns result to partner application

VIGOURSOFT

Technical Architecture: Mobile App (Contd.)

3. **Biometrics** - The app will be accessed by the user using the device biometrics (fingerprint and FaceID as applicable (iOS))

4. **ID Document Enroll** - the user will be able to scan an ID document and validate with his biometrics that the documents is his. (Using SDKs from providers – Keeping it dummy for the PoC)
    a) Scan Driver License – Camera API of the phone to be called to enable this functionality
    b) Call YourID platform APIs to validate the scanned image (Dummy API returns True/False for the PoC scope)
    c) Once scan and verification complete save the ID object in the user profile (IDM).`

VIGOURSOFT

Technical Architecture: Mobile App (Contd.)

5. **Consent Management** - the user will be able to visualize the consented information to the partners
    I. This functionality will be handled via the UMA functionality per partner. UMA 2.0 extends the OAuth 2.0 protocol and gives resource owners granular management of their protected resources by creating authorization policies on a centralized authorization server. We would use OpenAM as the authorization and policy server
    II. The UI should be able to display all UMA policies using https://backstage.forgerock.com/docs/am/6/uma-guide/#to-query-uma-policies
    III. Need to setup OpenAM with UMA (both an OAuth 2.0 Provider service, and an UMA Provider service). https://backstage.forgerock.com/docs/am/6/uma-guide/
6. Mobile application will be in React Native to support cross platform access
7. We assume that basic flow/UX design of mobile app is already in place and mobile screen will be developed as per design shared

VIGOURSOFT

Technical Architecture: YourID Platform

1. Configure OpenID connect provider in IDM
2. Setup the OpenID provider service to be provided by OpenAM (which provides the authorization and authentication both)
3. Create a sample partner web app which provides link “login with YourID”
4. On clicking this link, Trusona and OAuth/OpenID Connect flow gets started in the backend.
5. Consent Window for the user to provide the requested profile information based on scope is obtained
    1. UMA policy (read, view permission) is checked for the ID document being used using https://backstage.forgerock.com/docs/am/6/uma-guide/#to-read-an-uma-policy
    2. If UMA policy doesn’t exist – create it

VIGOURSOFT

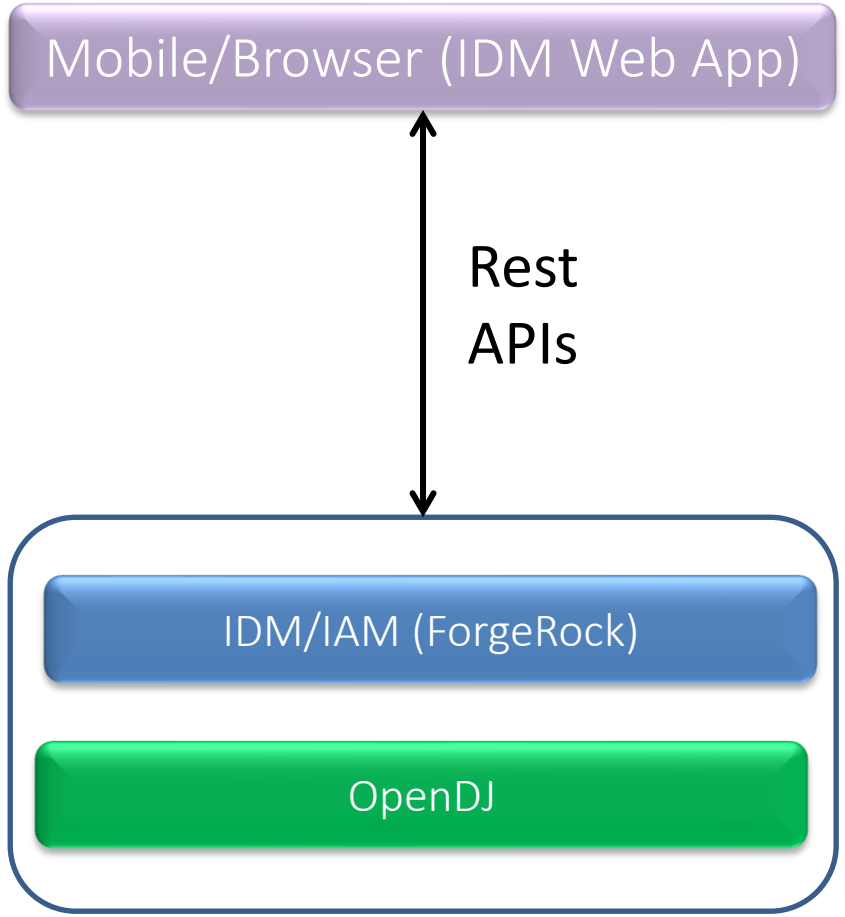
Technical Architecture: User Dashboard (IDM WebApp)

1. IDM UI will have to be customised to display YourID logo and create custom dashboard to display all the below.
2. User profile management
   a) Use IDM profile management
3. User consent management
   a) This will be the same information displayed as in the mobile app consent management.
   b) UI will be created based on IDM widgets
   c) While mobile app will have to be designed differently using UX tools
   d) REST APIs to get the consent data (for both mobile and webapp) will be the same.
4. User device management.
   a) Trusted device setup in IDM
5. ID document management.
   a) Saved as part of user profile (managed object)

VIGOURSOFT

Technology Stack (Proposed)

Front End	Mobile Framework	React Native or Android/iOS (As Appropriate)
Back End	Language/Platform/ Database	IDM/IAM (ForgeRock)
Back End	Cloud Service Provider	AWS
Back End	Storage	S3



Note: Common view for Mobile and Web Application

VIGOURSOFT

Support Matrix (Web based Platform/Mobile App)

Windows	Microsoft Edge. Mozilla Firefox (from V.54). Google Chrome (from V.65).
Mac OS X	Safari (from V.10). Mozilla Firefox (from V.54). Google Chrome (from V.65).

Furthermore, the system is compatible with the following operating systems:

Windows	8 and 10 (32-bit and 64-bit).
Mac OS X	10, 11 and 12 (Yosemite, El Capitan, Sierra).
Linux	Ubuntu and Debian.

In addition, the mobile app works on the following phones (due to restrictions in older versions):

- IPhone 7 or higher and iOS 11 or higher.
- Android Nougat 7.0 or higher.

VIGOURSOFT

Technology Stack – 3rd Party Products To Be Integrated

1. ForgeRock AM 7.0 - For Access Management, UMA provider, OpenID Connect Provider, OAuth 2.0 Provider
2. ForgeRock IDM 6.5 – User profile management, Device management, ID management, Dashboard,
3. Trusona Server (point to existing one)
4. SDK - ID Verification Providers

VIGOURSOFT

Assumptions & Dependencies

1. YourID to provide acceptance and other feedback in agreed timeframe to avoid delay in sprint schedule and final delivery

2. Application development will kick off on confirmation of wireframes and overall agreement on the scope, technical direction and schedule expectation agreement

3. Scalability, Availability, Redundancy will NOT be included in the POC for now (Will have one instance of each of the above technologies installed in AWS)

4. Social login and registration by invitation is Out of scope for functional POC

5. All 3rd party platform and technology licenses will be provided by YourID

VIGOURSOFT

Clarifications Required (For PoC)

1. Is the ID document verification (during the consent flow) part of the functional POC?
    1. OPEN: Still need to confirm
2. What ID verification services are considered for the PoC? (Assuming we will be provided with REST endpoints and the ID document service liaising will be done by YourID)
    1. For now, we will create a dummy ID verification Rest API returning TRUE/FALSE
3. Scalability, reliability, availability requirements? – Out of scope for PoC
4. Licensing and versions for ForgeRock product
5. Is the Trusona Authenticator plugin to be developed by VigourSoft or do we use the off-the-shelf plugin?
    1. Trusona plug-in will be provided by YourID team
6. Need to define scope around:
    1. Requirements around security (TLS/SSL, Signing, encryption, message hashing) – SSL enabled – Default ForgeRock
    2. Logging, auditing, monitoring - Config ForgeRock logging only

VIGOURSOFT

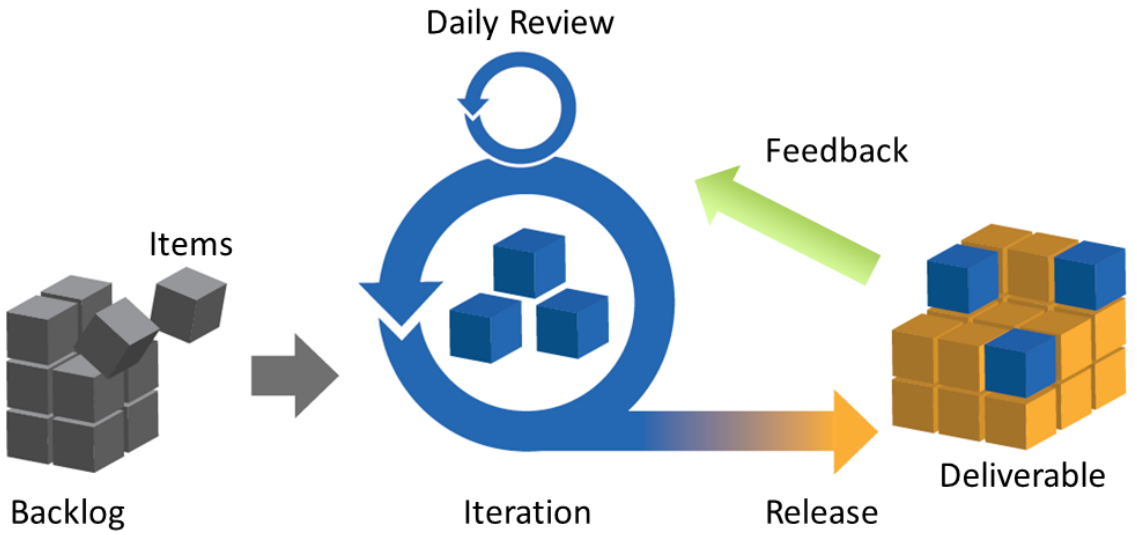
Overall Project Execution - Process

- Agile/Scrum Methodology
  - Sprint tracking
  - 2-3 weeks of each Sprint
- Feedback received in each sprint, will be backlog for next Sprint
- Source code management, code review, Bug tracking (Jira access to YourID team)
- At developer Level- Unit testing
- QA /Integration including UI testing will be done by Senior QA who will be part of Scrum team

VIGOURSOFT

Project Management/Engineering Methodology

1. Agile Scrum methodology for project planning and execution
2. Each Sprint of 2-3 weeks
3. High level Sprint goals/Stories discussed at the start of the sprint.
4. Quick demo of work done in Sprint shown at the end of the sprint.
5. Development/Testing Environment Set up
6. Technology stack, Testing tools etc. decided.
7. Weekly status to be shared with Customer stakeholders

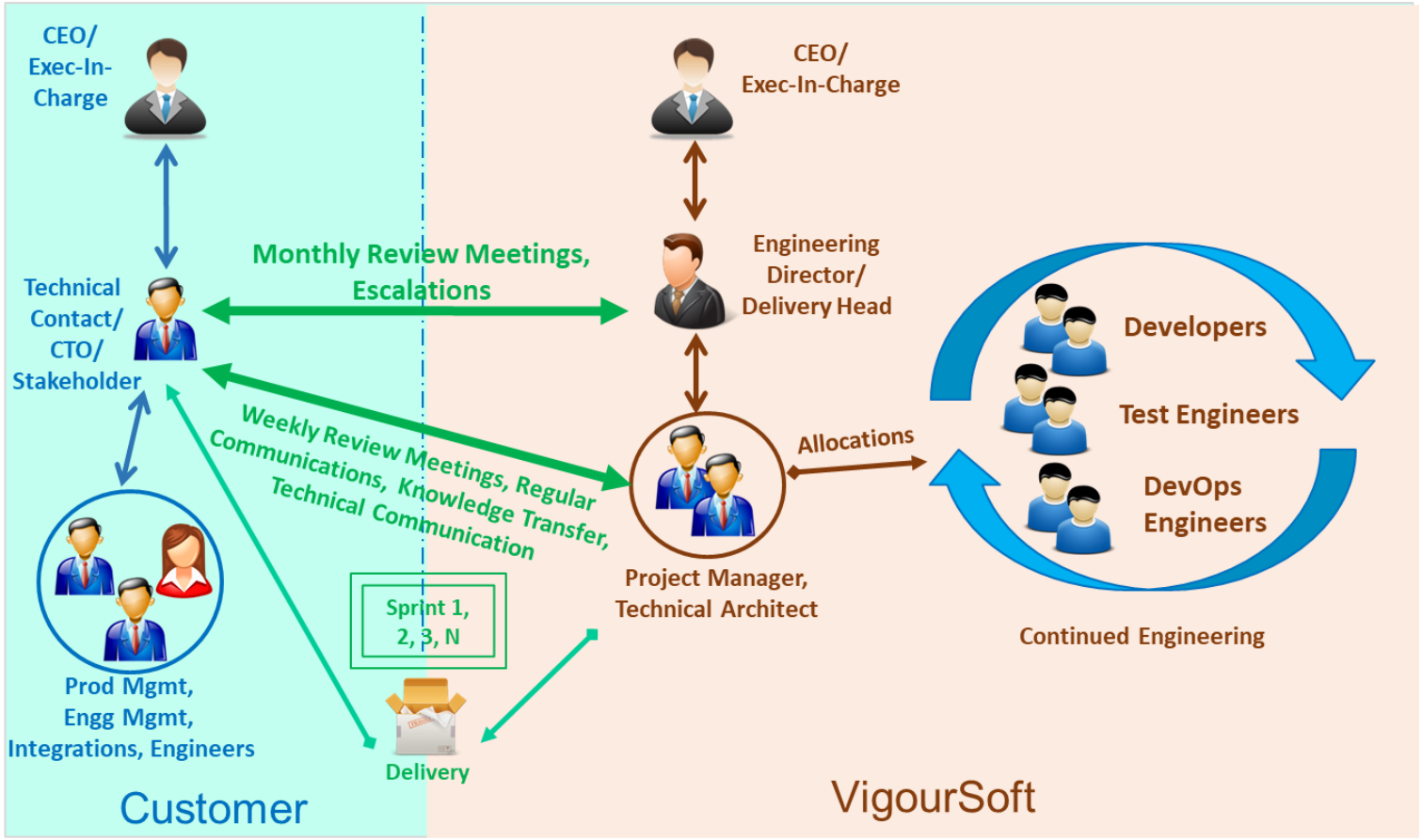


Agile Project Management: Iteration

VIGOURSOFT

VigourSoft Communication Matrix

- Weekly report to Stakeholders
- Sprint Demo (Every 3 weeks)
- Slack, Skype across the team
- Monthly Status/ Review Meeting



VIGOURSOFT

High Level Sprint Plan

Sprint	Duration	Sprint-Focus
Sprint 1	2 week	➢ High level requirements discussion and agreement. ➢ Identity (ForgeRock) framework set up, ➢ Cloud (AWS) component Set up and readiness. ➢ Tech stack finalization, finalization of workflow for mobile App.
Sprint 2	3 weeks	➢ UX Design for YourID mobile App (75%) . ➢ YourID Platform (IDM/IAM Config) (35%). ➢ Continuous Testing of earlier and present Sprint items.
Sprint 3	3 weeks	➢ UX Design for YourID mobile App complete and Approved ➢ YourID Platform (IDM/IAM Config)(70%). ➢ Your ID Platform (Service Layer)(35%) ➢ YourID Platform (Trusona integration in OpenAM) (50%) ➢ YourID mobile App (Enrollment) (50%). ➢ Continuous Testing of earlier and present Sprint items.

VIGOURSOFT

High Level Sprint Plan (Contd.)

Sprint	Duration	Sprint-Focus
Sprint 4	3 weeks	➢ YourID Platform (IDM/IAM Config)(100%). ➢ Your ID Platform (Service Layer)(70%) ➢ YourID. Platform (Trusona integration in OpenAM) (100%) ➢ YourID mobile App (Enrollment) (100%). ➢ Continuous Testing of earlier and present Sprint items.
Sprint 5	3 weeks	➢ Your ID Platform (Service Layer)(100%) ➢ Integration of IDM/IAM config/Service Layer ➢ YourID mobile App (Password less Login) (100%) ➢ Continuous Testing of earlier and present Sprint items.
Sprint 6	3 weeks	➢ YourID mobile App (Biometric) (100 % complete) ➢ Your ID Platform (Consent Window) (100%). ➢ YourID mobile App (ID Document enroll) (50 % complete). ➢ Your ID Platform (Sample/Test App).(50% complete) ➢ Continuous Testing of earlier and present Sprint items.

VIGOURSOFT

High Level Sprint Plan (Contd.)

Sprint	Duration	Sprint-Focus
Sprint 7	3 weeks	➢ YourID mobile App (ID Document enroll) (100 % complete). ➢ YourID mobile App (Consent management) (100 % complete). ➢ Your ID Platform (Sample/Test App) (100% Complete). ➢ Continuous Testing of earlier and present Sprint items.
Sprint 8	3 weeks	➢ All component Testing (Volume Testing/Use case Flow/Integration) ➢ Final Testing and handover.

VIGOURSOFT

Proposed Project Team

#	Team Structure	Roles	Module
1	Project Manager	Overall project management	All
2	Senior Architect (Application/Infra)	Overall solution design, architecture & infrastructure	YourID Solution
3	IDM Architect	Overall IDM solution design & architecture	ID Solution
4	IDM/ForgeRock Consultant 1	ID Infrastructure, IAM-IDM-ForgeRock development/integration	Platform
5	IDM/ForgeRock Consultant 2	Trusona integration, IAM-IDM-ForgeRock development/integration	Platform
6	API Full Stack Developer	API, Web App, dashboard, development/integration	Web App
7	SaaS Full Stack Developer	Server, Web App, dashboard, development/integration	Web App
8	Senior Android Developer	Android mobile app development	Mobile App
9	Senior iOS Developer	iOS mobile app development	Mobile App
10	UX Designer	Overall visual, screens design	Combined Visual Design
11	DevOps Engineer	Overall DevOps	Combined DevOps
12	QA Lead	Overall QA testing	Combined Testing
13	Junior QA	Overall QA testing	Combined Testing

VIGOURSOFT