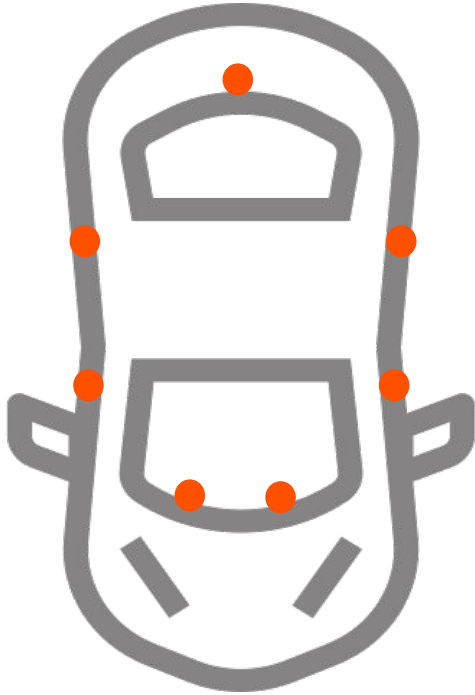# Access Delegation

- Authorizing an application to access your resources on your behalf

- Enables granting access to execute limited actions depending on the need

- Granted permissions can be revoked from the delegates easily
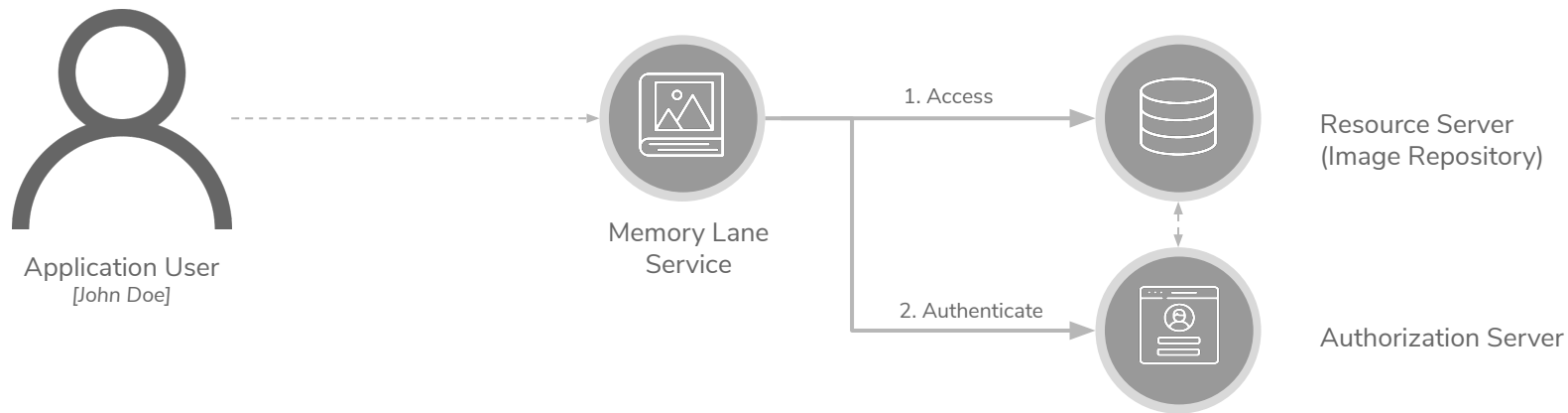
Example: Master Key vs. Valet Key

Access Points for the Master Key

Access Points for the Valet Key
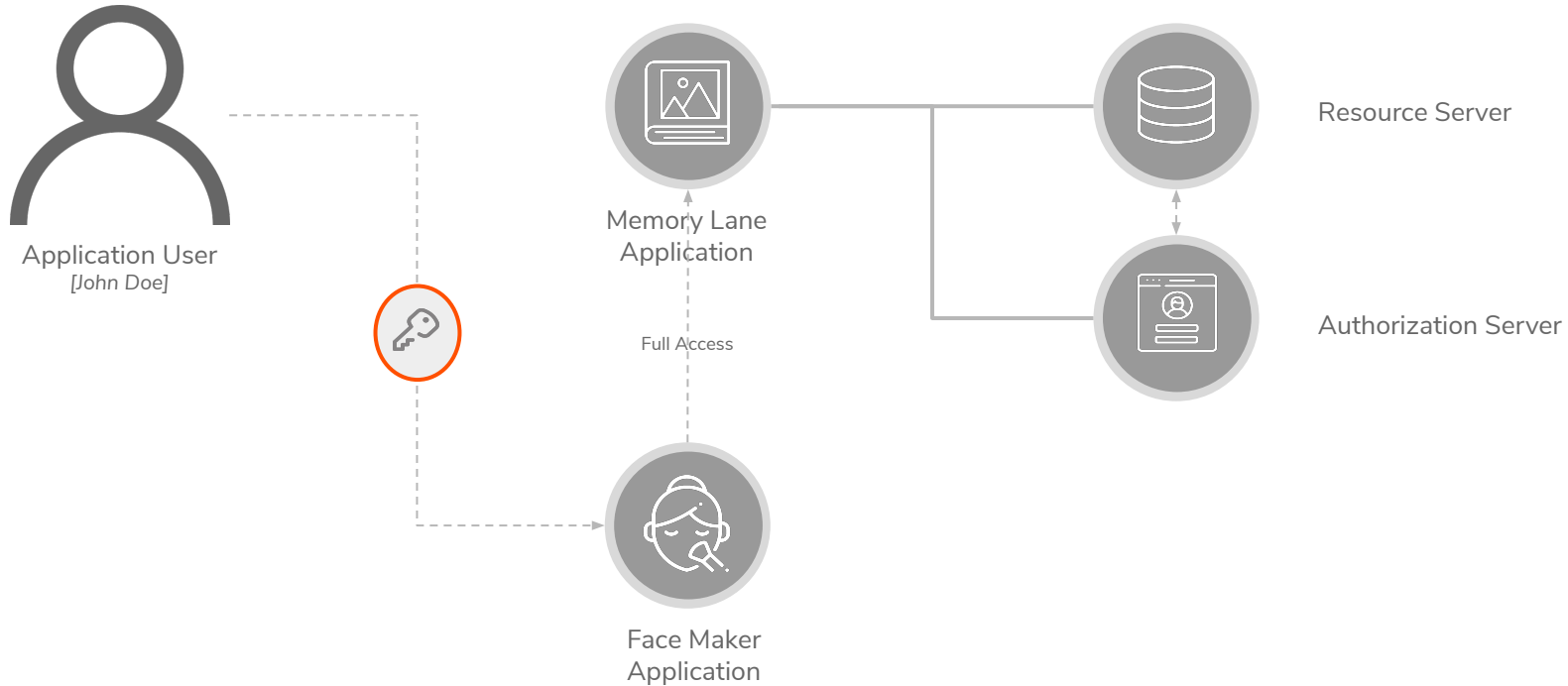
Example: Memory Lane image service

Application User
[John Doe]

Memory Lane
Service

1. Access

Resource Server
(Image Repository)

2. Authenticate

Authorization Server

WSO2 IDENTITY SERVER

Example: Face Maker photo editing service

Example: Face Maker accesses images on behalf of users

Application User
[John Doe]

Memory Lane
Application

Resource Server

Authorization Server

Access token with
Limited Access

Face Maker
Application

WSO2 IDENTITY SERVER
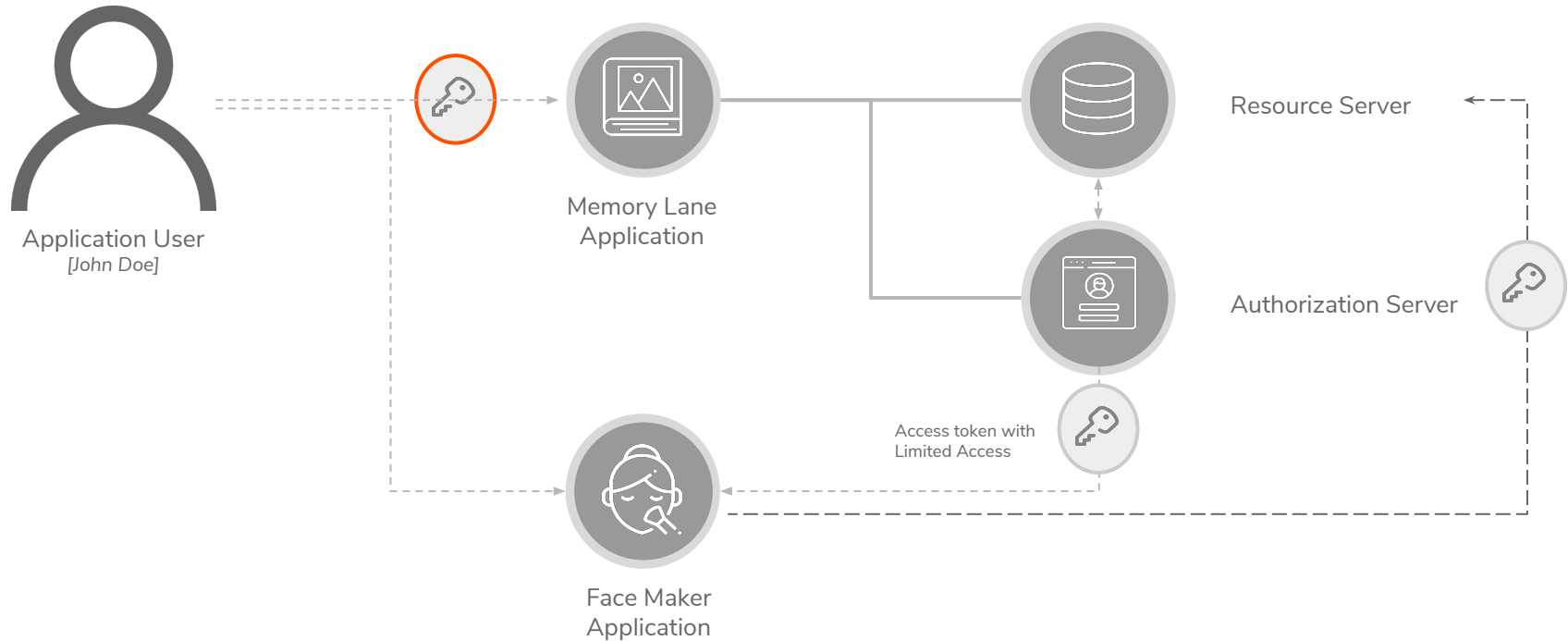
An Overview to OAuth2

What is OAuth2

- An industry-standard, light-weight protocol used for secure access delegation

- Enables applications to access resources without having to using the account credentials at the application site

- Generates tokens with limited access to facilitate accessing resources securely

- Extensible framework to implement new access delegation use cases
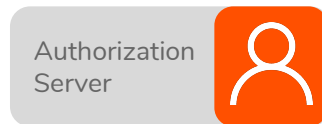
OAuth2 Roles

Who does what

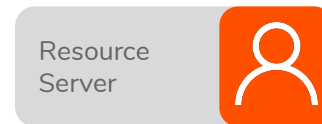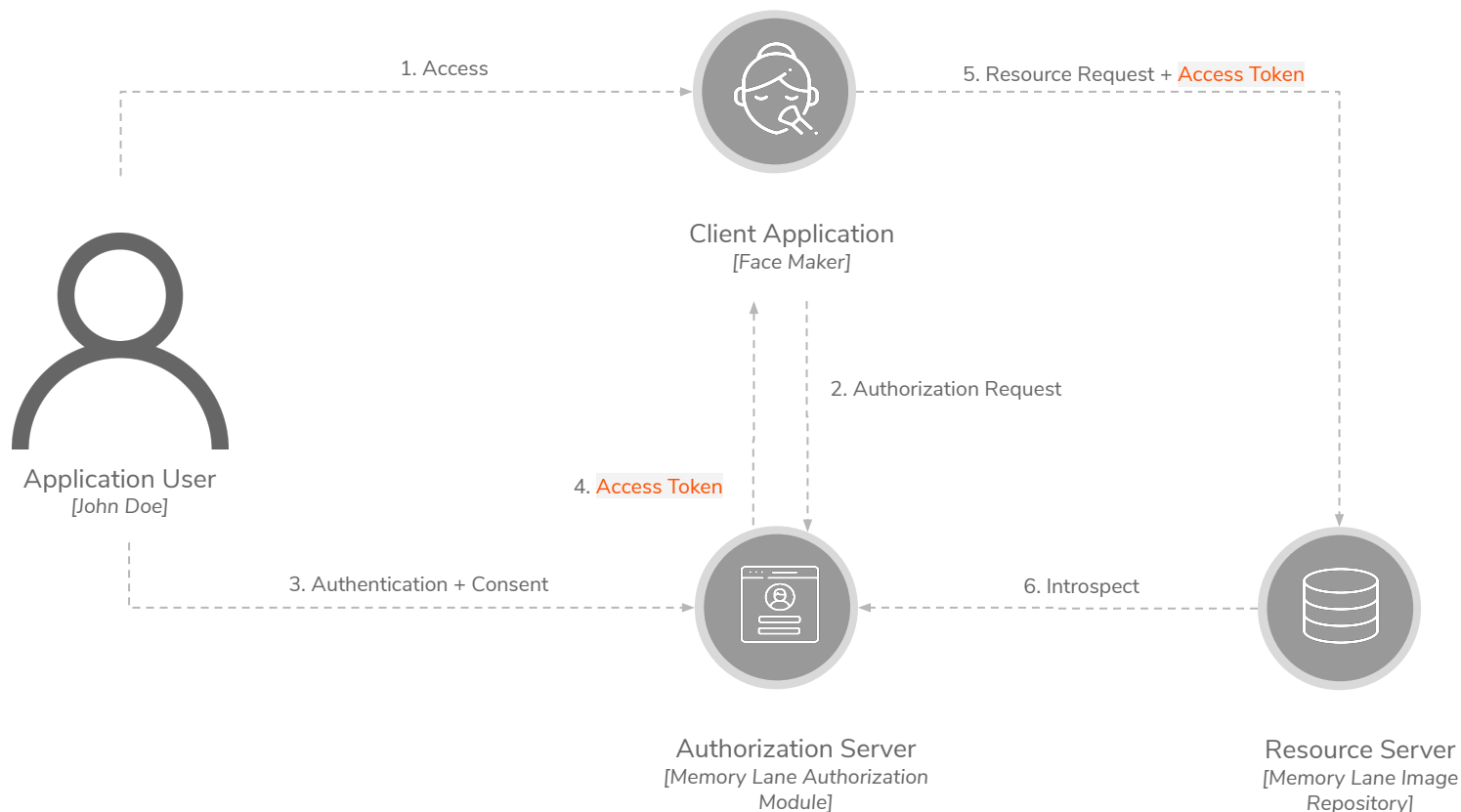| Resource Owner | Client Application | Authorization Server | Resource Server |

[John Doe]

[Messenger/ Face Maker]

[Google/ Facebook/ Memory Lane Authorization Module]

[Memory Lane Repository/ Facebook]

Sample Scenarios

Accessing Third-Party Resources with Access Tokens

1. Access

5. Resource Request + Access Token

Client Application
[Face Maker]

2. Authorization Request

4. Access Token

Application User
[John Doe]

3. Authentication + Consent

6. Introspect

Authorization Server
[Memory Lane Authorization Module]

Resource Server
[Memory Lane Image Repository]

WSO2 IDENTITY SERVER

Limiting Access to Third-Party Resources with Scopes

1. Access

5. Resource Request + Access Token

Client Application
[Face Maker]

2. Authorization Request + Scopes

Application User
[John Doe]

4. Access Token

3. Authentication + Consent

6. Introspect

Authorization Server
[Memory Lane Authorization Module]

Resource Server
[Memory Lane Image Repository]

WSO2 IDENTITY SERVER
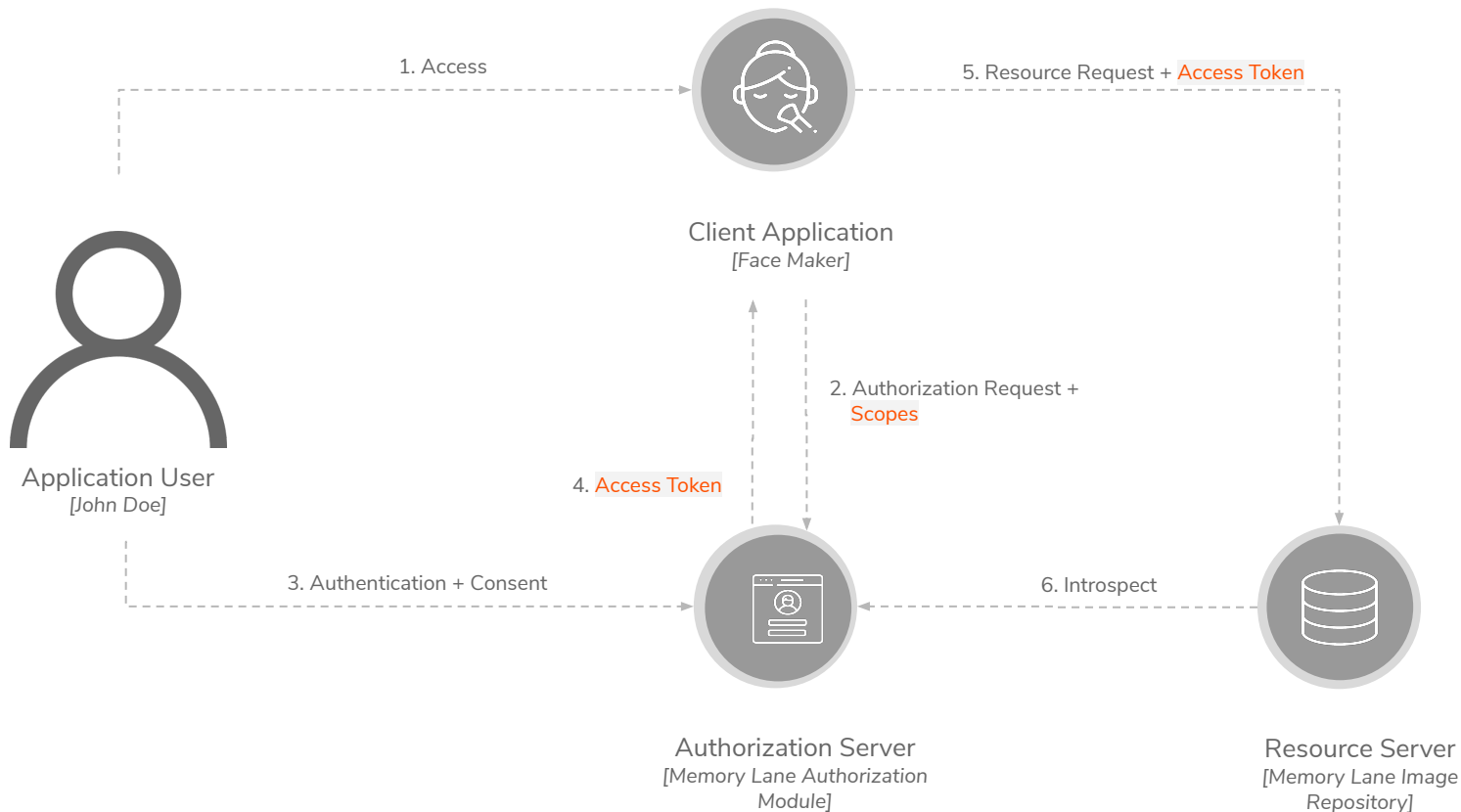
Sustaining the Access Token Validity

Application User
[John Doe]

Client Application
[Face Maker]

Authorization Server
[Memory Lane Authorization Module]

Resource Server
[Memory Lane Image Repository]

1. Access

5. Resource Request + Access Token

2. Authorization Request + Scopes

4. Access Token +Refresh Token

3. Authentication + Consent

6. Introspect

WSO2 IDENTITY SERVER
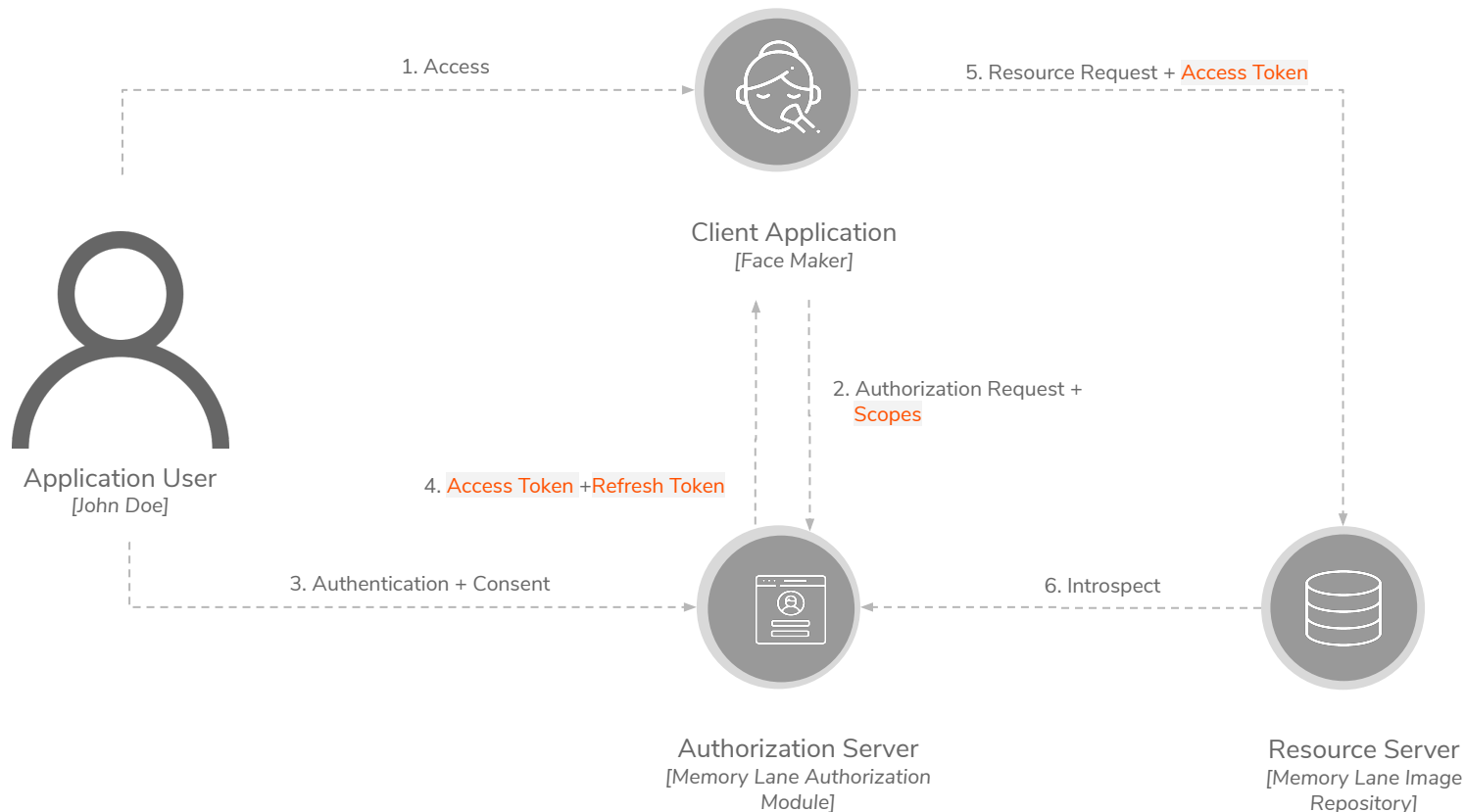
Refreshing Access Token Upon Expiry
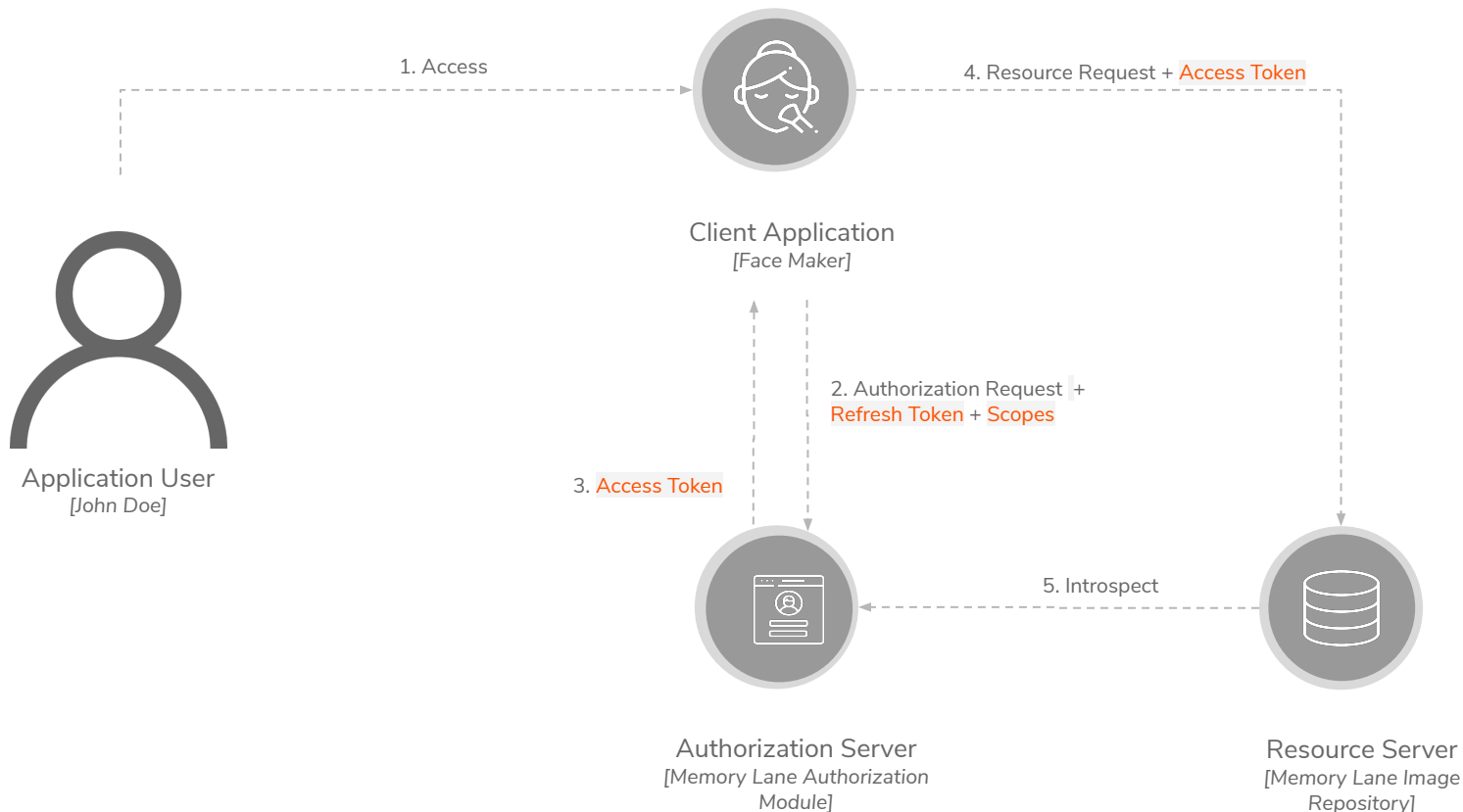
Tokens and Grants

Token Types

Access
Token

Duration: Short
Purpose: Access resources

Refresh
Token

Duration: Long
Purpose: Get new access tokens

Authorization
Code

Duration: One-time
Purpose: Get new access tokens

Grant Types

Authorization Code

Implicit

Password

Client Credential

Refresh Token

SAML2 Bearer

JWT Bearer

Extended

Quick Recap

What you learnt

1. Overview of access delegation

2. Overview of OAuth 2.0 concepts

3. Sample access delegation scenario with

   OAuth 2.0

Any Questions ?

Reach us through the following channels

✉ iam-dev@wso2.org

📑 https://stackoverflow.com/questions/tagged/wso2

\# https://wso2is.slack.com/

Thank You