Using OAuth to authenticate applications on SAP Ariba Open APIs

OAuth

- **OAuth** is an open standard for authorization
- Allows internet users to authorize websites to access resources on other websites but without giving them the passwords
- Adoption by Google, Facebook, Twitter, Yahoo etc. – widely adopted standard

Why OAuth ?

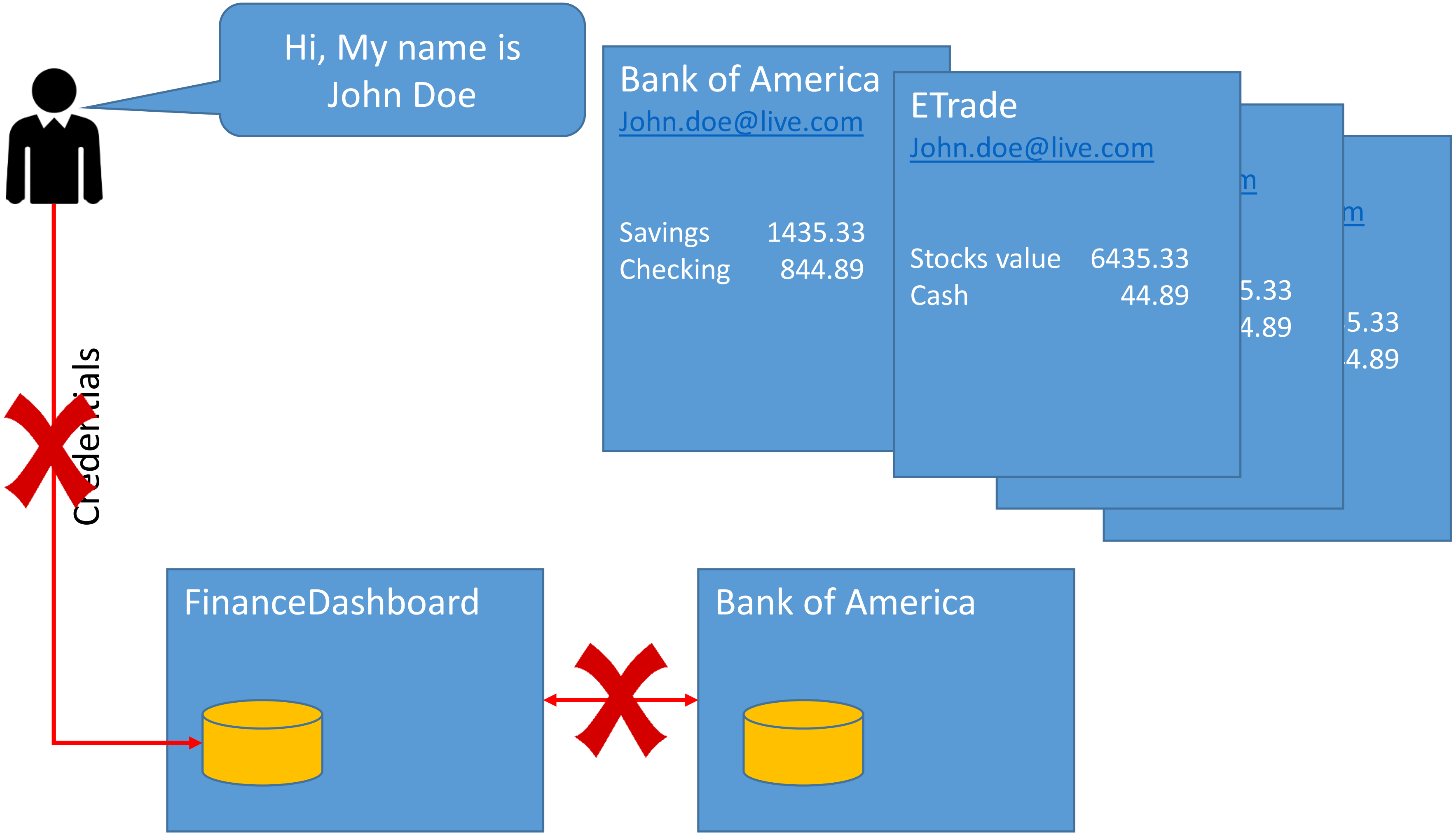
FinanceDashboard.com
John.doe@live.com

Bank of America
  Savings – 1435.33
  Checking – 844.89

Etrade
  Stocks value – 6435.33
  Cash – 44.89

American Mortgage
  Balance – 45389.78

American Express
  Balance – 123.34



Hi, My name is John Doe

Credentials

Bank of America
John.doe@live.com

Savings	1435.33
Checking	844.89

ETrade
John.doe@live.com

Stocks value	6435.33
Cash	44.89

m
5.33
4.89

m
5.33
4.89

FinanceDashboard

Bank of America

Why OAuth (contd.) ?

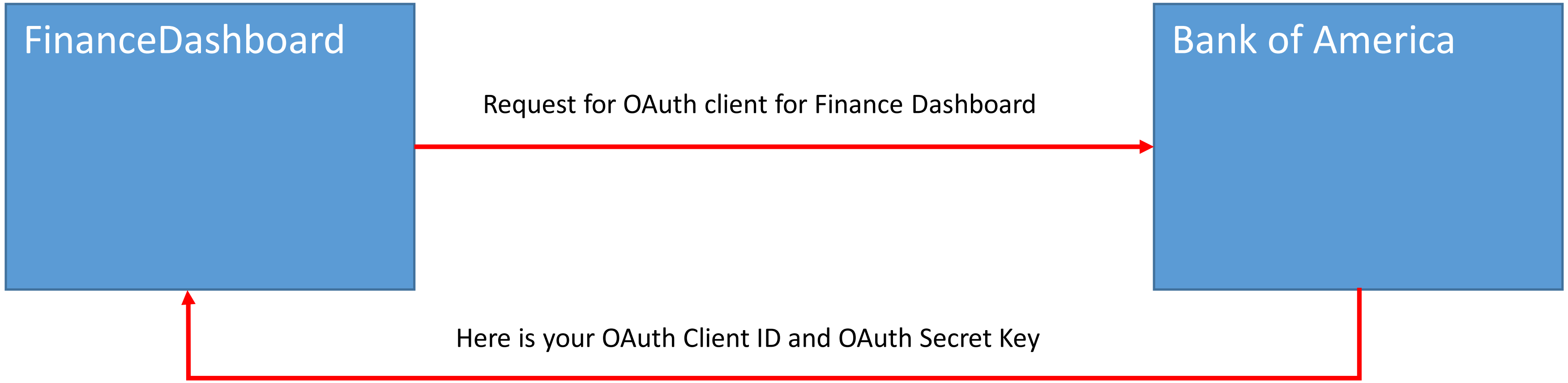
- John Doe
  - Shouldn’t be handing out passwords
  - Credentials can be compromised
  - Credentials have lot of power – balance transfers, bill pay etc.
  - Stop using Finance Dashboard services – revoke, change user credentials
- Bank of America and Finance Dashboard
  - Proliferation of credentials bad for both
  - Users will not trust services offered by Finance Dashboard
  - Finance Dashboard has added responsibility to securely store user credentials

OAuth to the rescue

- John Doe grants limited access to Finance Dashboard to access his data
- Grant takes the form of access token – known only to Finance Dashboard and Bank of America

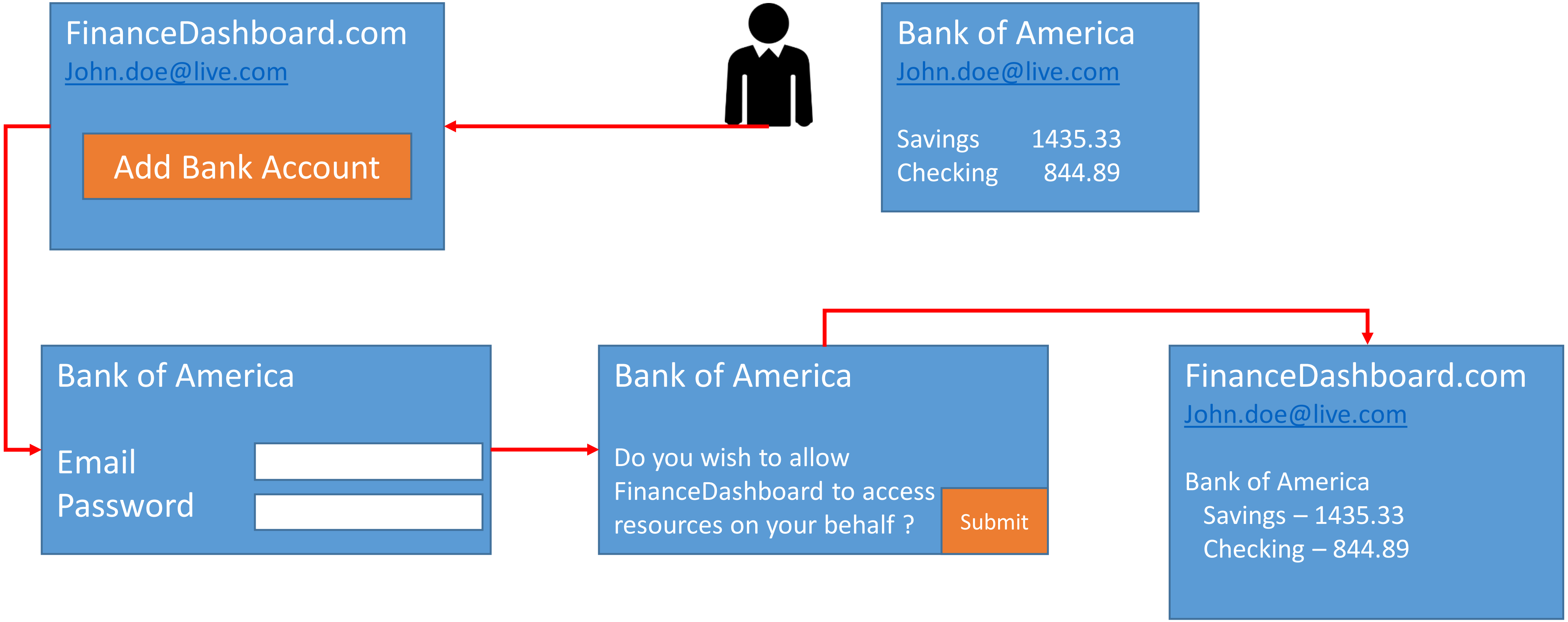
- **OAuth** provides Finance Dashboard a "*secure delegated access*" to BoA resources on behalf of John Doe
- **OAuth** specifies a process for John Doe to authorize Finance Dashboard access to their BoA resources without sharing their credentials

How OAuth is set up ?


FinanceDashboard
Bank of America
Request for OAuth client for Finance Dashboard
Here is your OAuth Client ID and OAuth Secret Key

- System Administrators work together to establish the shared secret – assuming requisite commercial agreements are in place
- Request for OAuth client for Finance Dashboard
- Receives OAuth Client ID and OAuth Secret Key

How OAuth is set up (contd.) ?



FinanceDashboard.com
John.doe@live.com

Add Bank Account

Bank of America
John.doe@live.com

Savings	1435.33
Checking	844.89

Bank of America

Email

Password

Bank of America

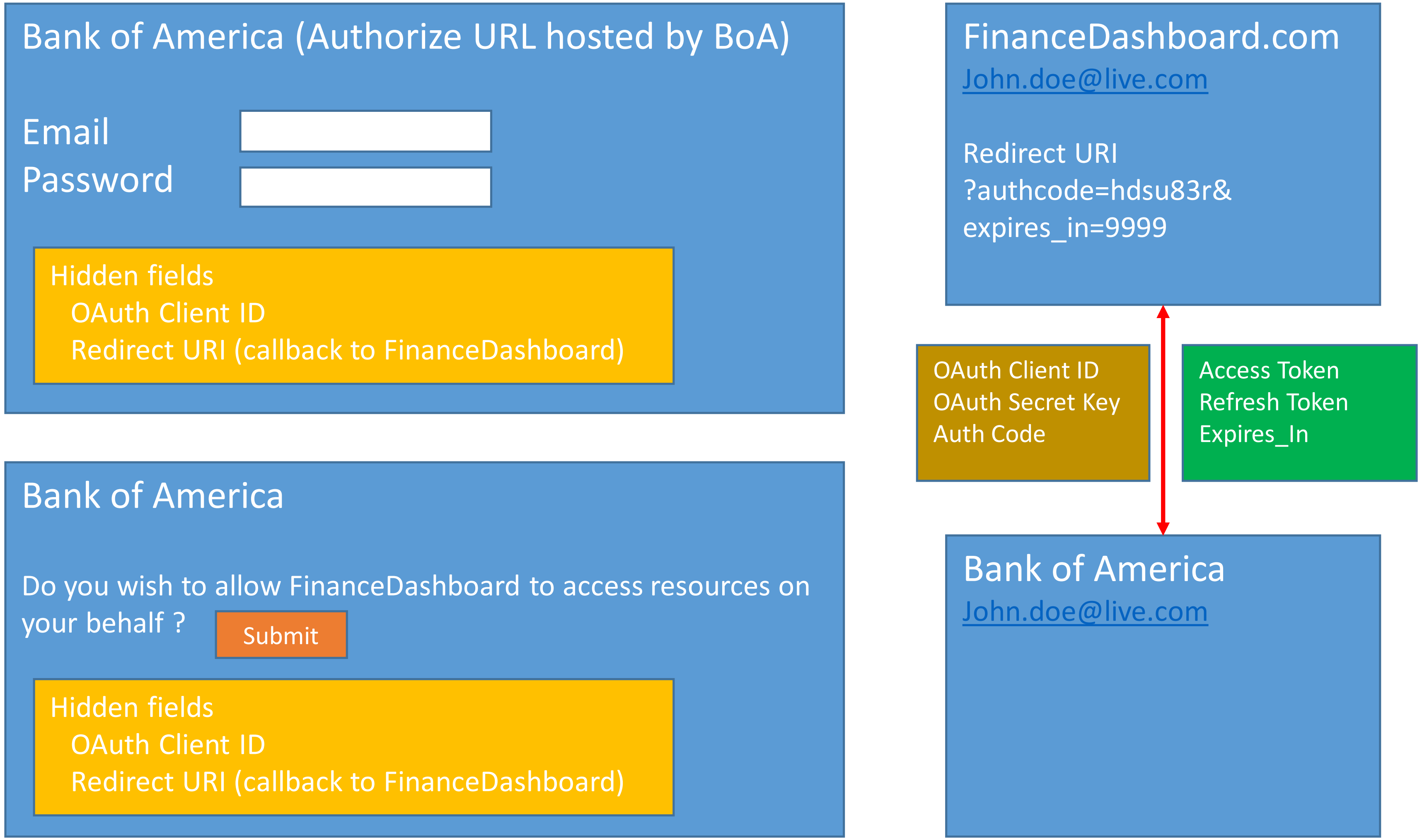
Do you wish to allow FinanceDashboard to access resources on your behalf ?

Submit

FinanceDashboard.com
John.doe@live.com

Bank of America
Savings – 1435.33
Checking – 844.89

OAuth in more detail…



Bank of America (Authorize URL hosted by BoA)

Email

Password

Hidden fields
OAuth Client ID
Redirect URI (callback to FinanceDashboard)

Bank of America

Do you wish to allow FinanceDashboard to access resources on your behalf ? Submit

Hidden fields
OAuth Client ID
Redirect URI (callback to FinanceDashboard)

FinanceDashboard.com
John.doe@live.com

Redirect URI
?authcode=hdsu83r&
expires_in=9999

OAuth Client ID
OAuth Secret Key
Auth Code

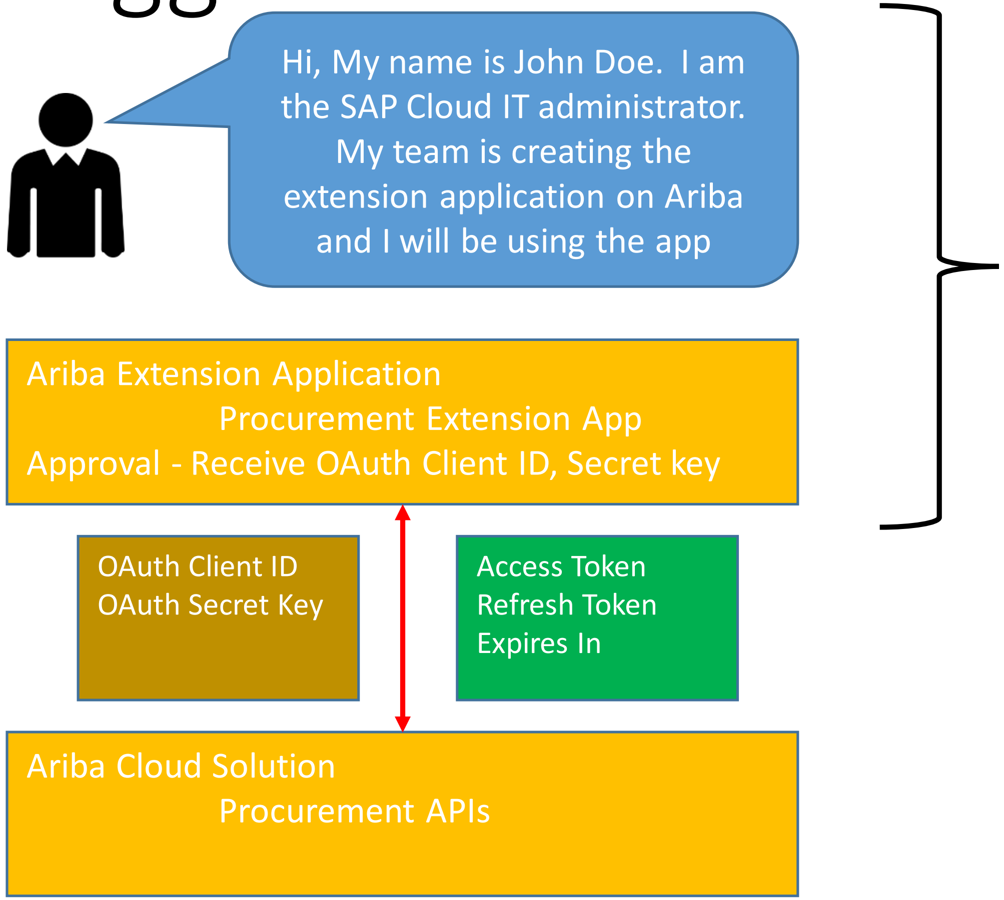
Access Token
Refresh Token
Expires_In

Bank of America
John.doe@live.com

OAuth Players (3 legged OAuth)

Players	Various Names
👤	Resource Owner User
Finance Dashboard	Application OAuth Client Client
Bank of America	OAuth Server OAuth Provider Authorization Server Resource Server

How OAuth is used in SAP Extensions ? 2 legged OAuth



Hi, My name is John Doe. I am the SAP Cloud IT administrator. My team is creating the extension application on Ariba and I will be using the app

Ariba Extension Application
Procurement Extension App
Approval - Receive OAuth Client ID, Secret key

OAuth Client ID
OAuth Secret Key

Access Token
Refresh Token
Expires In

Ariba Cloud Solution
Procurement APIs

One Single Entity
No concept of an owner, user
OAuth Client
Client
Application

OAuth Server
Resource Server
Authorization Server

Requesting OAuth Client ID and Secret Key

- Approval is required
- Only applications approved by the SAP Ariba Open API Platform administration can execute OAuth authentication
- After approval – you will receive the OAuth Client ID, OAuth Secret Key, Application Key
- Application key is mostly for identification – but don’t authenticate or authorize

Name	Ariba Extensions Demo	
Summary	Ariba Extensions Demo - Testing APIs	
Oauth client ID	02d1d0aa-0575-4bab-bc32-92409f851d62	ID of client - public
Application key	e22ab11beb254906acb3ec5d3a651e97	Used for identification - not for authorization or authentication
Oauth secret	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Keep this secret !!

Requesting initial access token

HTTP method	POST
URL	https://api.ariba.com/v2/oauth/token
Headers	Content-Type: application/x-www-form-urlencoded Authorization: Basic <base_64_clientID_clientSecret> Note: No concept of username and password Authorization: Basic XXXXXXXXXXXXXXXXXXXXXXXXXX
Body	grant_type=openapi_2lo

Response	{
	"timeUpdated" : 1483978494962,
	"access_token" : "9b64439a-6aa8-4821-80ef-d6dfb0b6e469",
	"refresh_token" : "f7e8d776-be93-462f-bca1-59067207b22b",
	"token_type" : "bearer",
	"scope" : null,
	"expires_in" : 1440
	}

Refreshing an expired access token

HTTP method	POST
URL	https://api.ariba.com/v2/oauth/token
Headers	Content-Type: application/x-www-form-urlencoded Authorization: Basic <base_64_clientID_clientSecret> Authorization: Basic XXXXXXXXXXXXXXXXXXXXX
Body	refresh_token=bcd07260-85aa-43fa-9478-768d2ff5cf9c&grant_type=refresh_token

Response	{
	"timeUpdated" : 1483981835209,
	"access_token" : "90551e84-48a4-45d3-b89a-e997071fdbe2",
	"refresh_token" : "335fe479-9a88-4104-91cf-5e7508354656",
	"token_type" : "bearer",
	"scope" : null,
	"expires_in" : 1440
	}

Requesting access to protected resources

HTTP method	GET
URL	https://openapi.ariba.com/api/<service_name>/<version>/{sandbox|prod}/<resource>?<service_query_parameter1=value1>[...&<service_query_parameterN=valueN>] For example, https://openapi.ariba.com/api/approval/v1/{sandbox|prod}/changes?needTotal={true|false}&realm={realm}&offset={offset_value}&limit={limit_value}&lastChangeId={ID}
Headers	Content-Type: application/json Authorization: Bearer <access_token> apikey: <api_key> Accept: application/json
Response	JSON response will include the data requested by your application