Progress®

Les Jeudis de Progress

Exceptionnellement Mercredi

Préambule

Laurent Kieffer : laurent@progress.com

20 Mai 2020

Les Thèmes

Thèmes	Date
Accès aux Données OpenEdge et autres : Les possibilités (ODBC , REST,oData etc…) : lien	2 Avril 2020
OE 12 : Les raisons de l'adopter, les contraintes , les bénéfices : lien	16 Avril 2020
Advanced Enterprise Database : Rappel des fonctionnalités et avantages : lien	23 Avril 2020
PCA : Les outils et solutions pour vous aider à renforcer vos plans de continuité en production : lien	30 Avril 2020

Les Thèmes

Thèmes	Date
PASOE : API REST , revue des possibilités (mapped REST , Business entity , Webhandler)	7 Mai 2020
CORTICON + OpenEdge : Pourquoi et comment intégrer un moteur de règles dans vos applications OpenEdge ou autres	14 Mai 2020
La sécurité dans vos Systèmes d'Informations. Ce qu'il faut considérer	20 Mai 2020
OERA ou la nouvelle architecture de référence Progress. Quelles sont les éléments à intégrer (Kinvey, Nativechat…)	28 Mai 2020

Progress Software

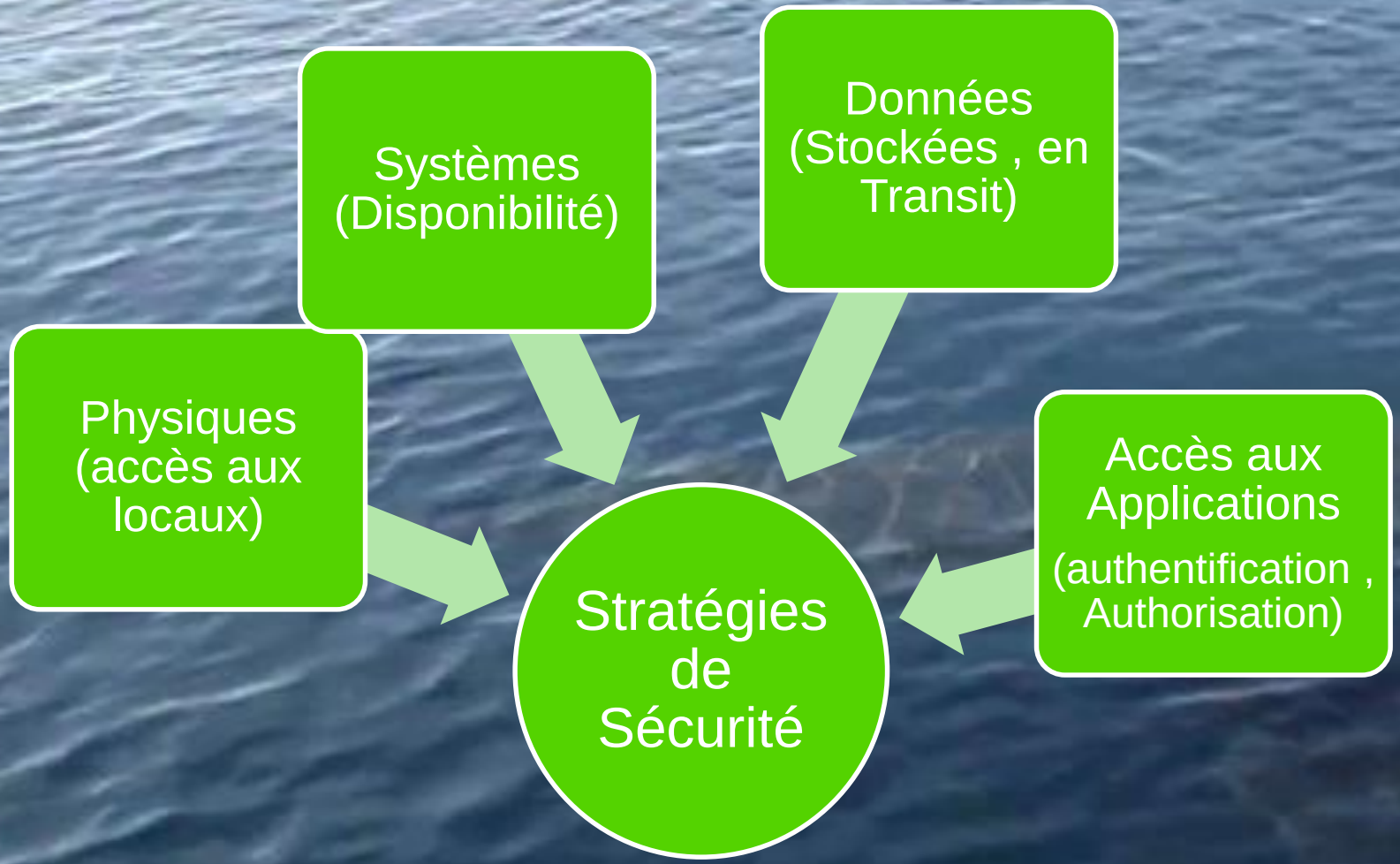
La sécurité dans vos Systèmes d'Informations.
Ce qu'il faut considérer

Mission impossible ?

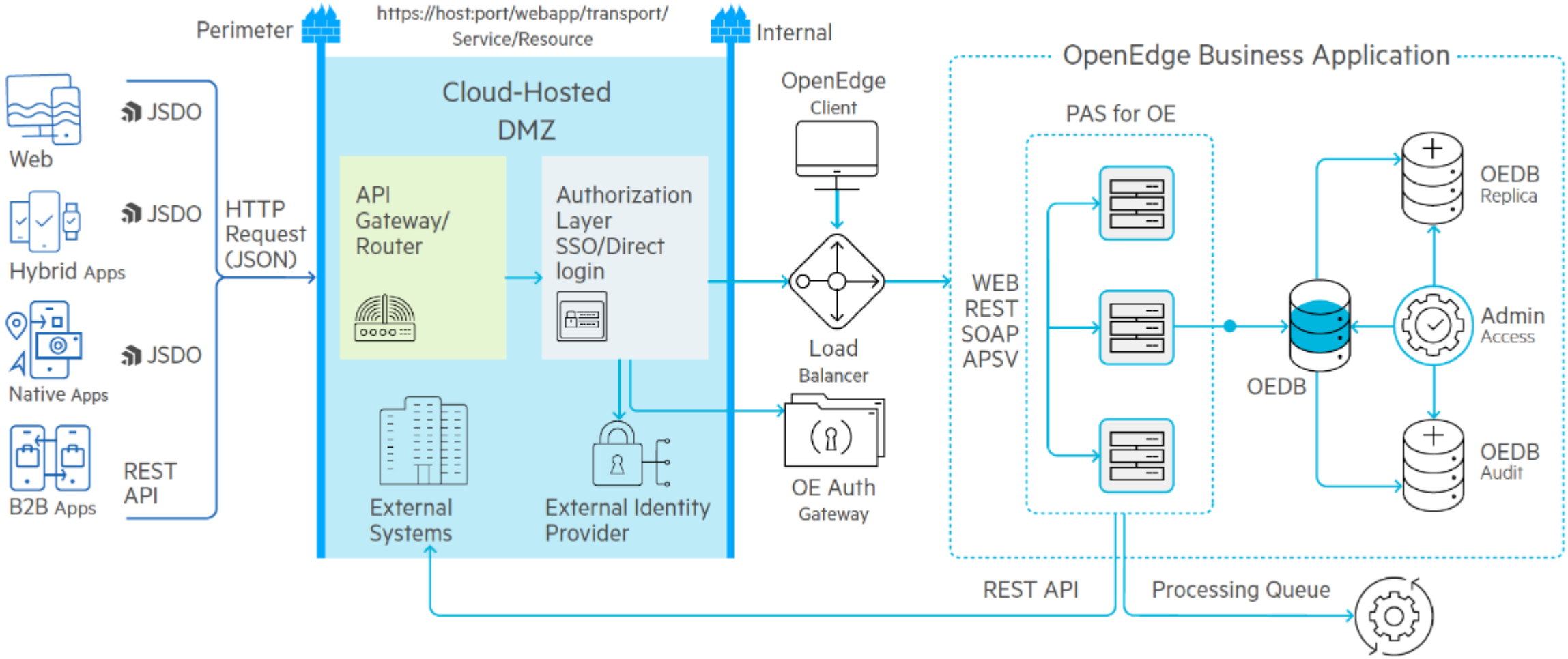
Laurent KIEFFER : laurent@progress.com

20 Mai 2020

Sécurité⇔ Une vaste étendue.. avec des risques



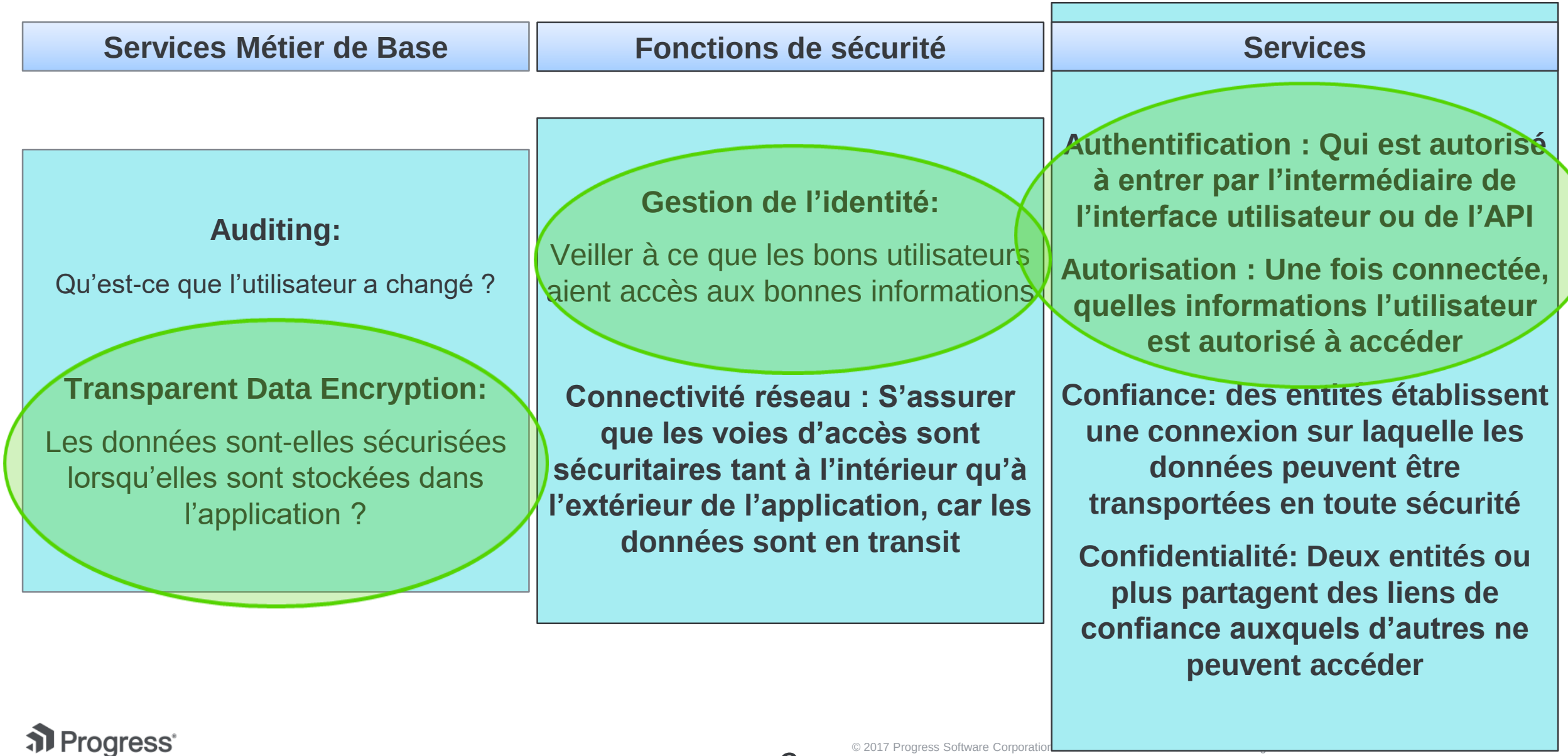
Les architectures modernes



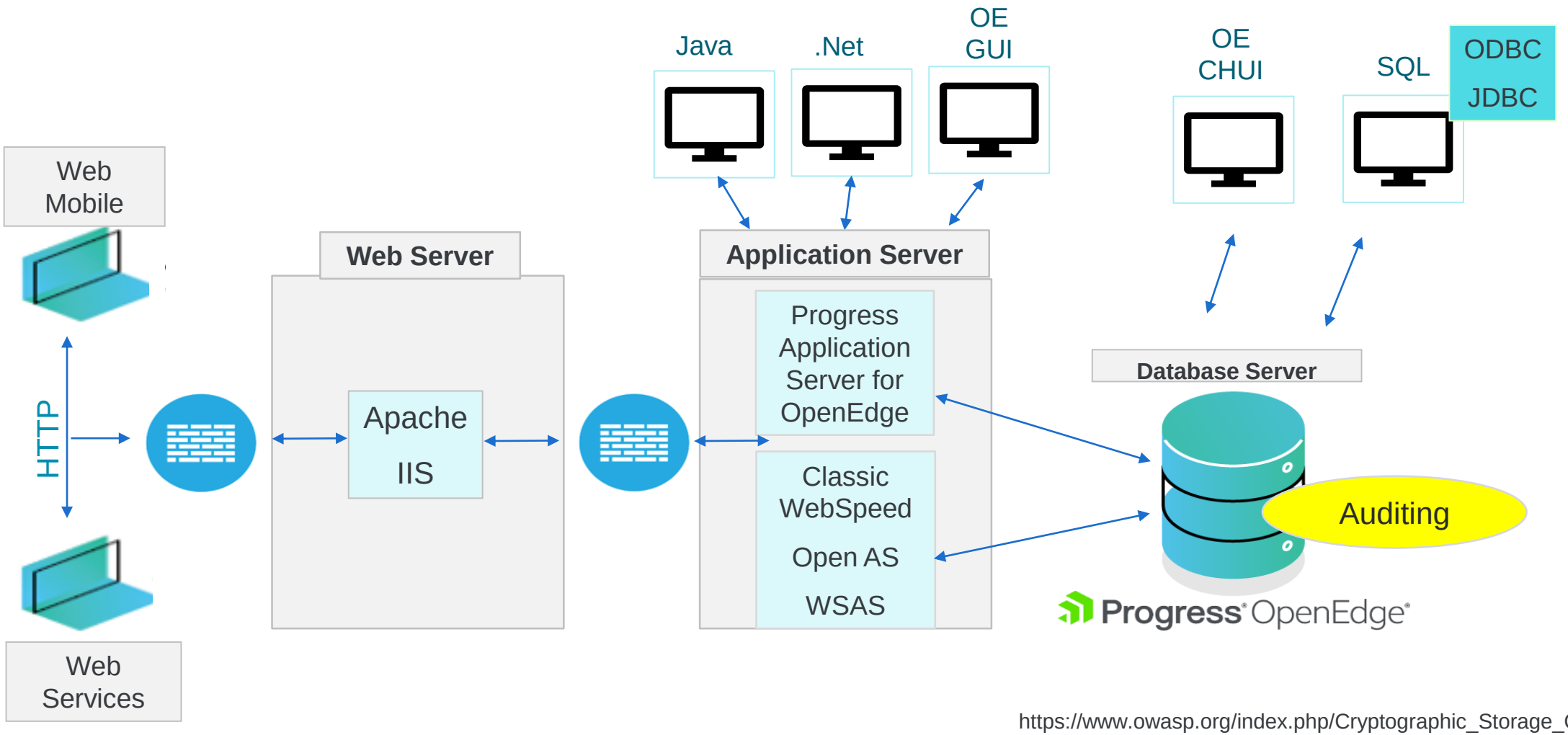
Progress®

Améliorations de la sécurité

Sécurisation des applications métier en cours d'exécution



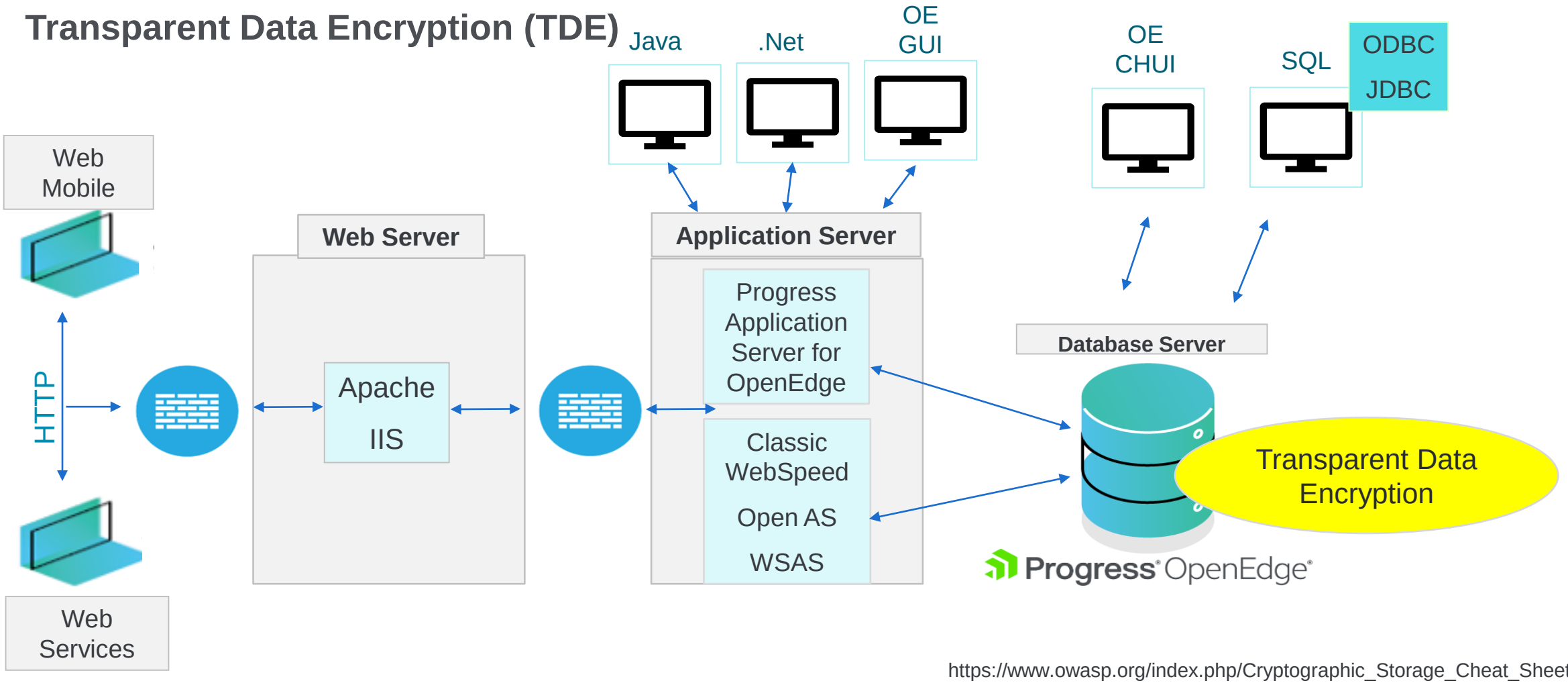
Auditing : qui a accédé et quoi ?



https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet

Encryptage de Données

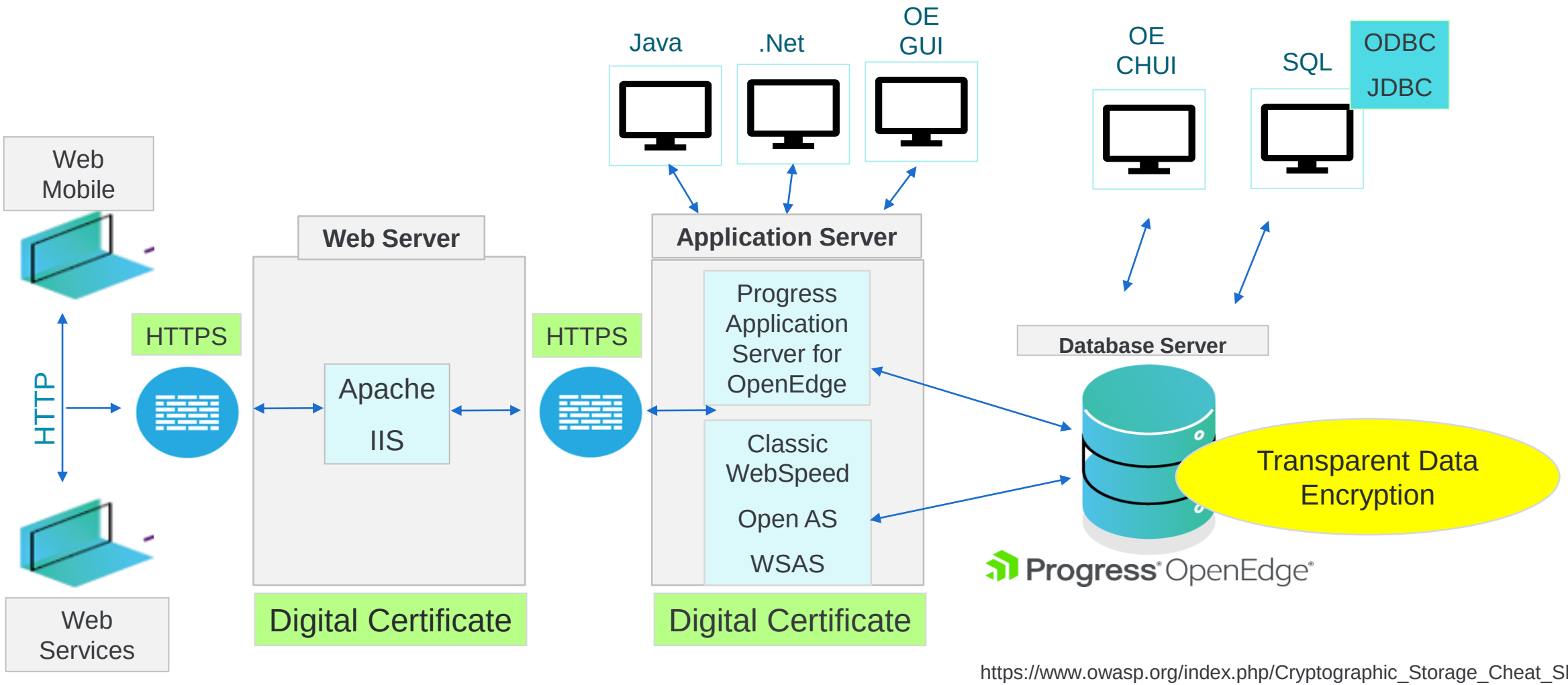
- Chiffrement de disque
- OpenEdge Programmatic Encryption
- Transparent Data Encryption (TDE)



https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet

Données qui entrent et sortent de votre système.

Support for TLS 1.1 and TLS 1.2 is implemented starting with **OpenEdge 11.6**
OpenEdge 10.0B SSL



https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet

OpenEdge Security Evolution

- 10.0 Client Principal
- 10.1 Auditing
- 10.2.B Transparent Data Encryption (TDE)
- 11.0 Multi-tenancy
- 11.2 Single Sign On (SSO)
- 11.5 PASOE
- 11.7 OpenEdge Authentication Gateway
- 11.7 OAuth2 Support
- 12.0 Continued Spring Security Adoption

Client Principal

- Apparait en OE 10.0
  - Beaucoup d’améliorations depuis 10.0
- Représente une session de connexion utilisateur
- Partage une session entre appservers et agents
- Positionne le user id
  - Pour les applications ABL
  - Pour la connexion base de données
- Client Principal ⇔ Token

Utilisation du Client Principal

- Audit logs : enregistre login/logout d'un utilisateur
- Modèle d'authentification interne
- Modèle d'authentification externe
- Les données de Session stockées comme valeur brute
- Une fois les données « scellées », elles ne peuvent pas être modifiées
- Utilisé, entre autre, pour l'enregistrement d'une session client sur un tenant d'une base MultiTenant

Power of Single Sign-On

Ce Que c'est

- Contrôle d'accès pour plusieurs systèmes logiciels, connexes, mais indépendants
- Empêche quiconque de falsifier les informations d'identification

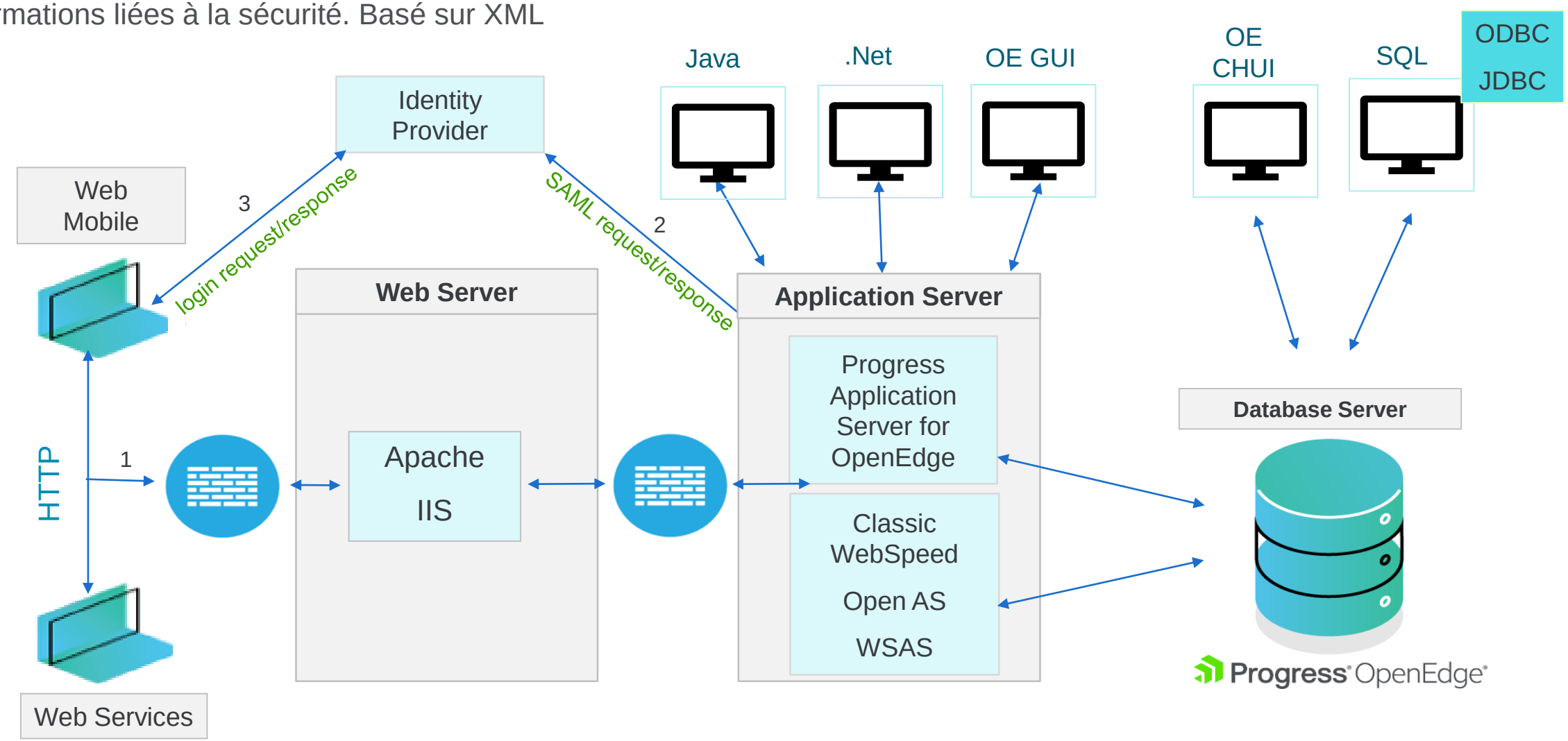
Son importance

- Amélioration de la productivité des utilisateurs et des développeurs
- Même niveau de sécurité par mot de passe partout
- Rapports centralisés
- Facilité d'administration

16

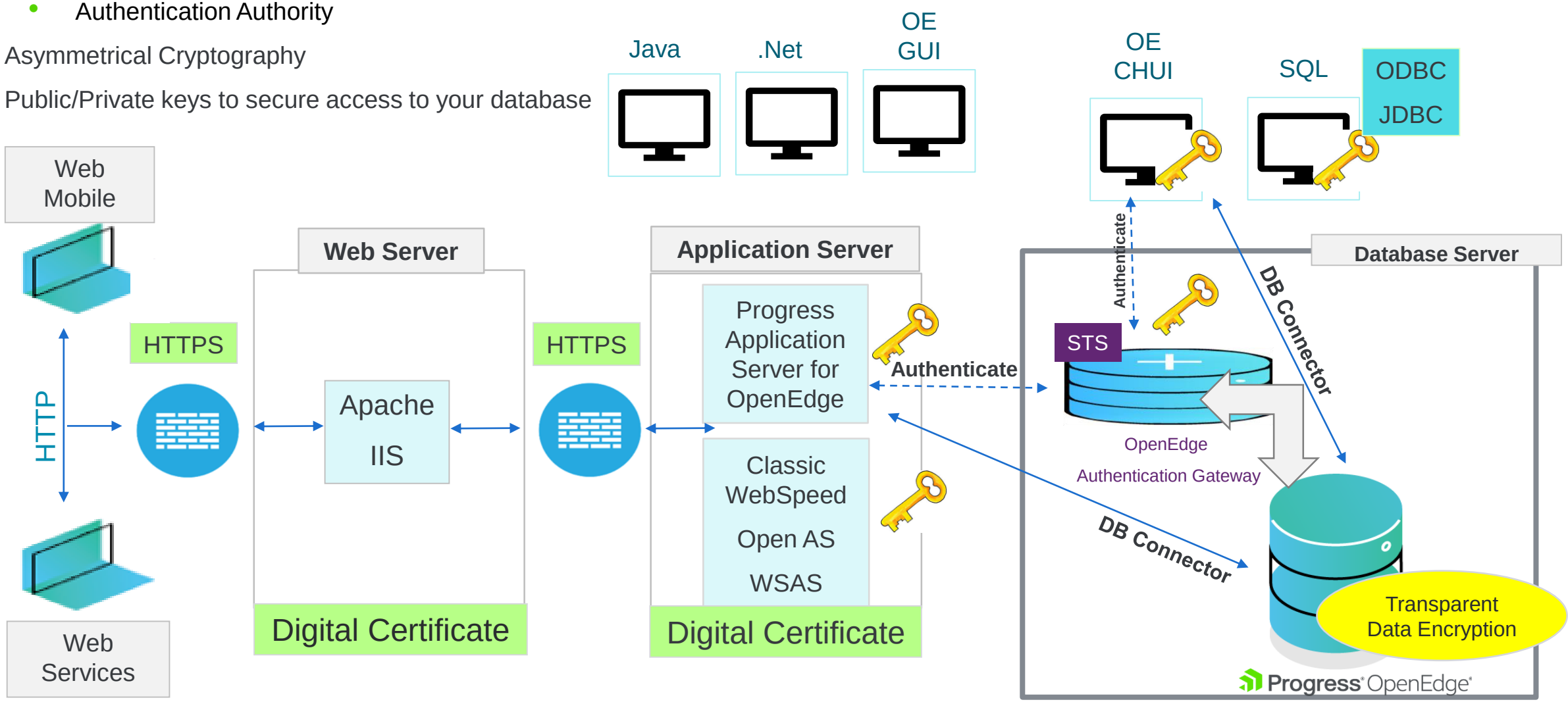
SAML support in PASOE

Security assertion markup language est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. Basé sur XML



OpenEdge Authentication Gateway

- User Authentication
  - Domains, Role Association, CPO Generation, Security Token Service
  - Authentication Authority
- Asymmetrical Cryptography
- Public/Private keys to secure access to your database



Progress®

Demo OE Authentication Gateway

Progress®

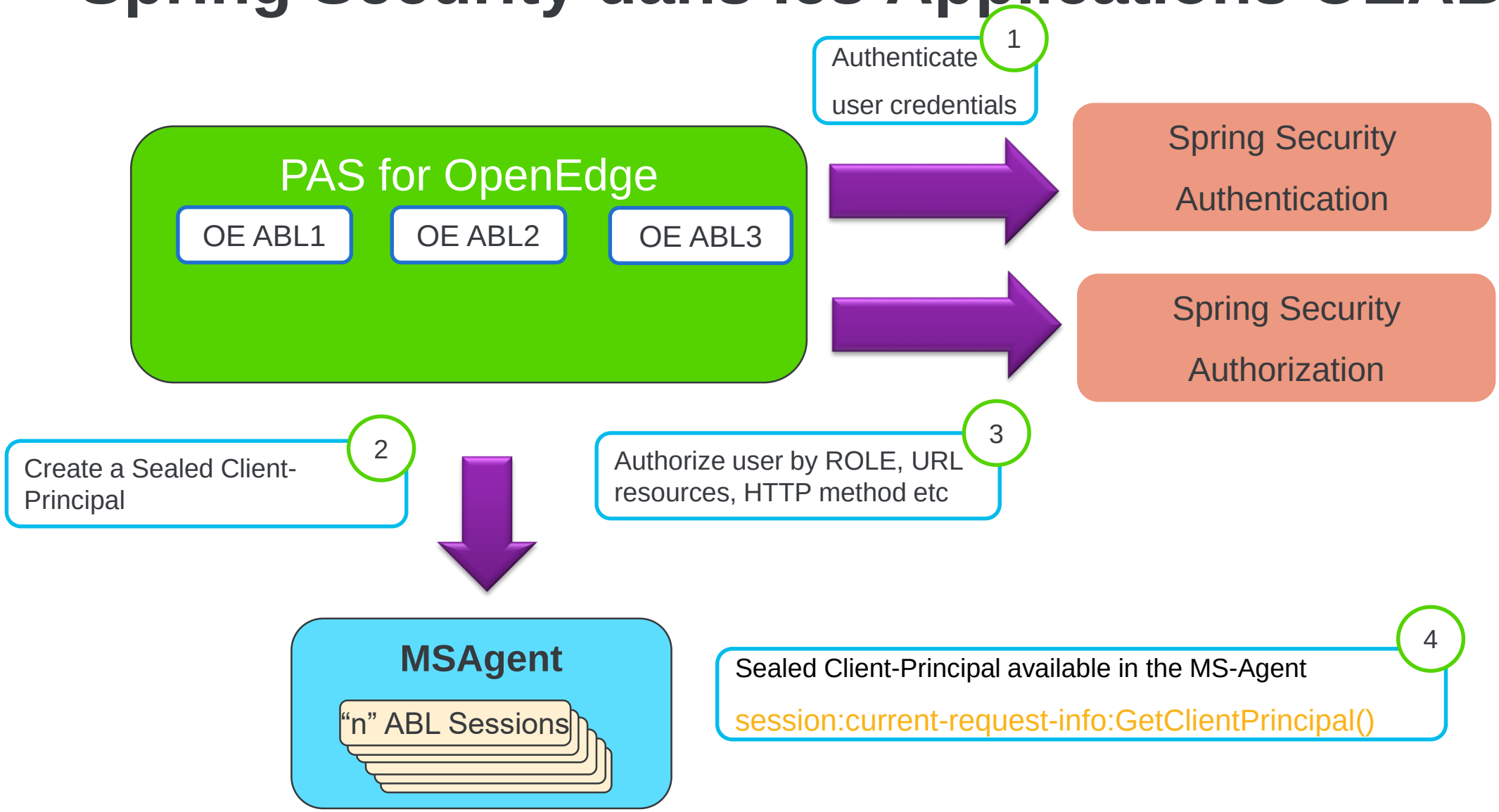
OpenEdge SSO Configuration for LDAP & OAuth2 in PASOE

Spring Security Framework

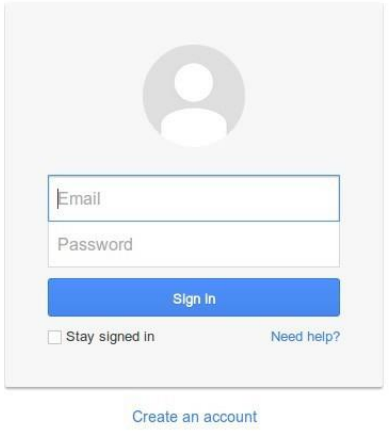
Spring Security est un framework Java / Java EE qui fournit l'authentification, l'autorisation et d'autres fonctionnalités de sécurité pour les applications d'entreprise

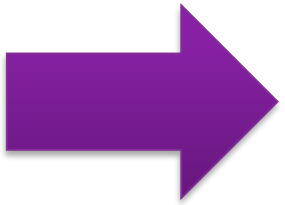
La plupart des applications web modernes nécessite une authentification en vue d’identifier ses utilisateurs et de sécuriser l’accès à d’éventuelles données. C’est dans ce but que Spring Security intervient pour mettre en place une authentification fiable, robuste et facile à intégrer à un projet basé sur Spring.

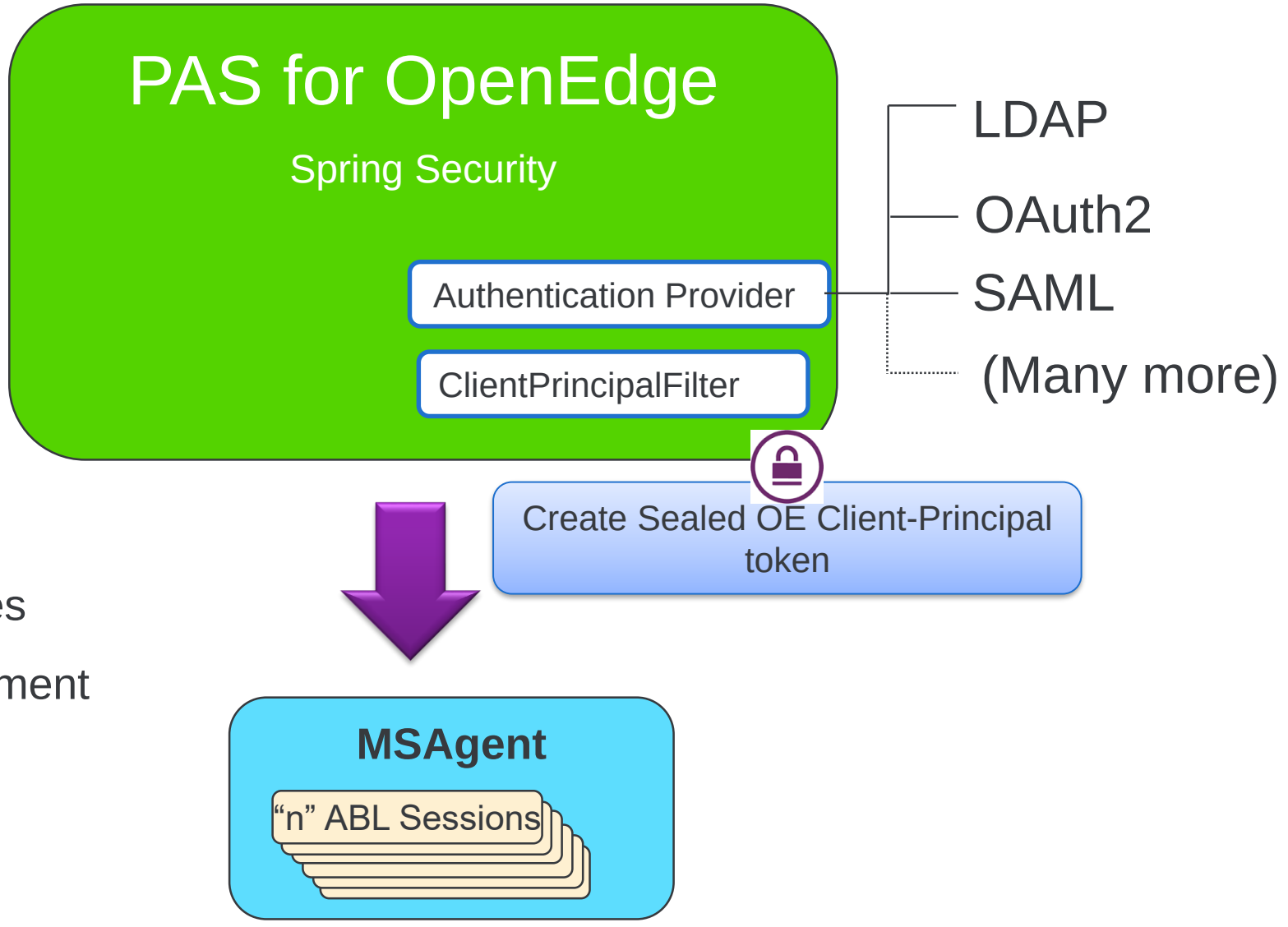
Spring Security dans les Applications OEABL



PASOE Spring Security – Comment ca marche







Authentication Provider authenticates users across multiple Identity management sources.

PASOE Authentification LDAP

LDAP

- What is LDAP
  - LDAP (Lightweight Directory Access Protocol) is an open and cross platform protocol used for directory services authentication.
  - LDAP runs over TCP/IP.

- What is an LDAP Server
  - The LDAP server hosts directory information, process queries and updates the LDAP information directory.

LDAP Configuration

oeablSecurity.properties

ldap.url=ldap://vm-pasoeldap:10389
ldap.manager-dn=uid=admin,ou=system
ldap.manager-password=secret

LDAP Connection details

ldap.root.dn=dc=progress,dc=com

Directory to look for the user

ldap.usersearch.searchSubtree=true
ldap.usersearch.filter=(uid={0})

User search options

ldap.grouprole.attribute=cn
ldap.groupsearch.searchSubtree=true
ldap.groupsearch.filter=(uniqueMember={0})

Group search options

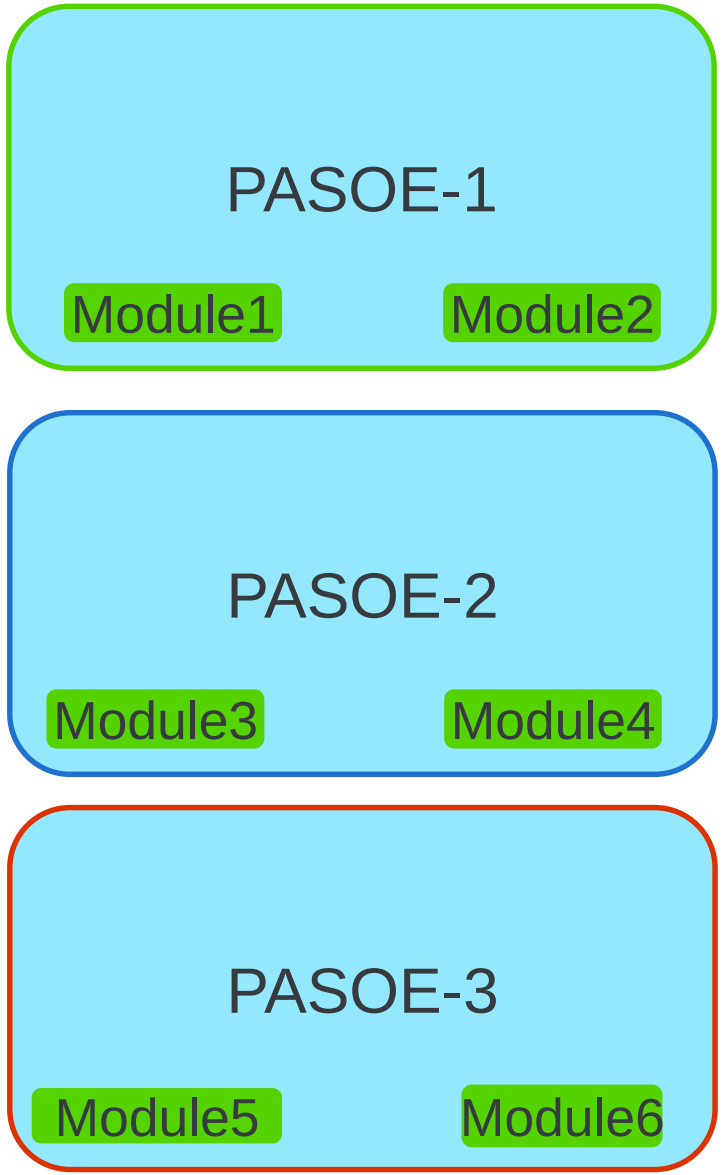
https://knowledgebase.progress.com/articles/Article/How-to-configure-OERealm-LDAP-authentication-with-PASOE

HTTP SSO avec PASOE

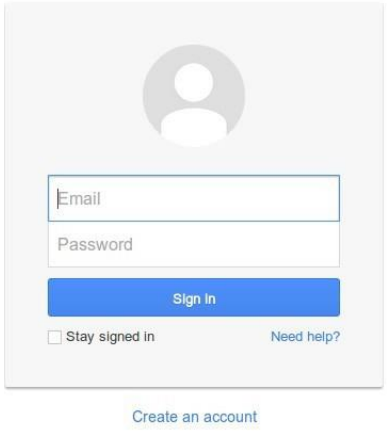
Need for HTTP SSO

Consider

- An application with 6 different modules is distributed across 3 different PASOE Instances.
- Every webapp is configured to work with same authentication and authorization.
- Login to the application once and access all my modules(web app's) without a need to login again.



Need for HTTP SSO



User login

PASOE-1

Module1 Module2

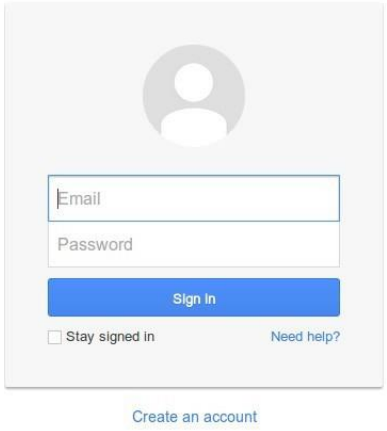
PASOE-2

Module3 Module4

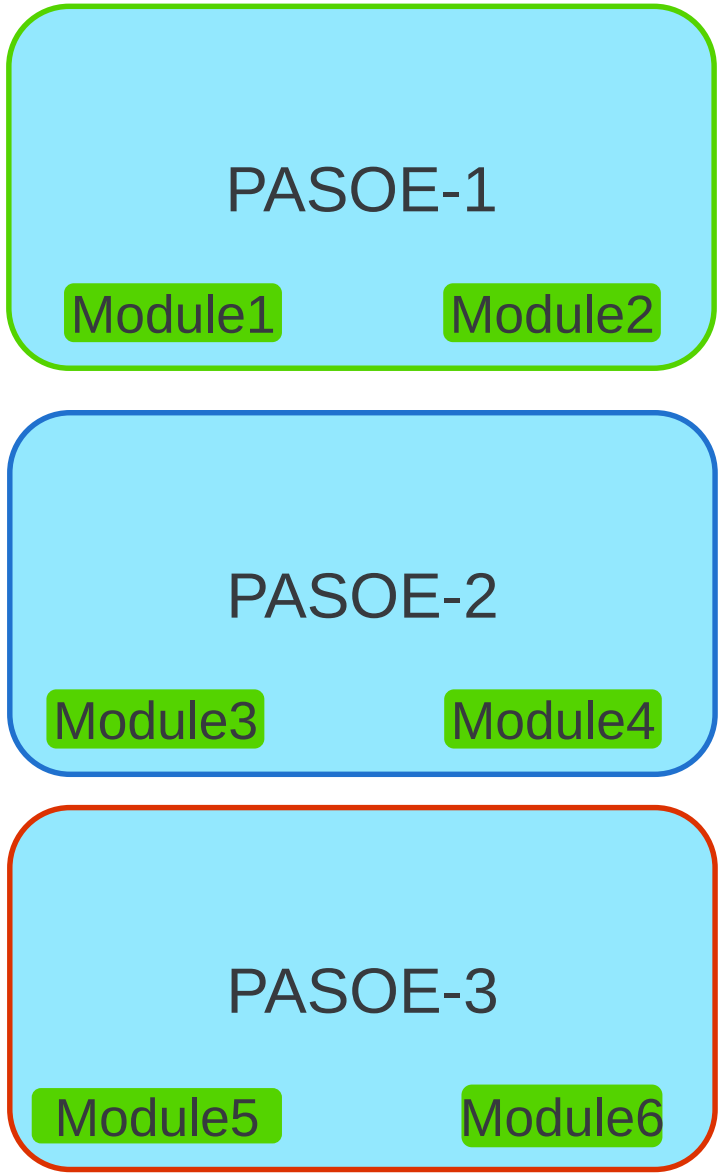
PASOE-3

Module5 Module6

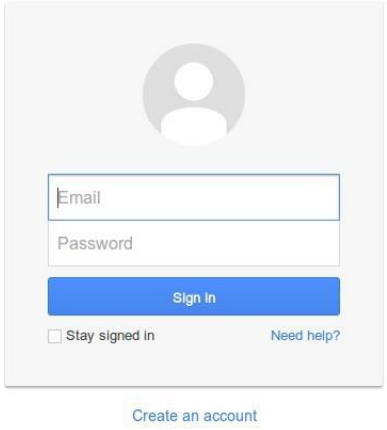
Need for HTTP SSO



Validate Client-Principal token

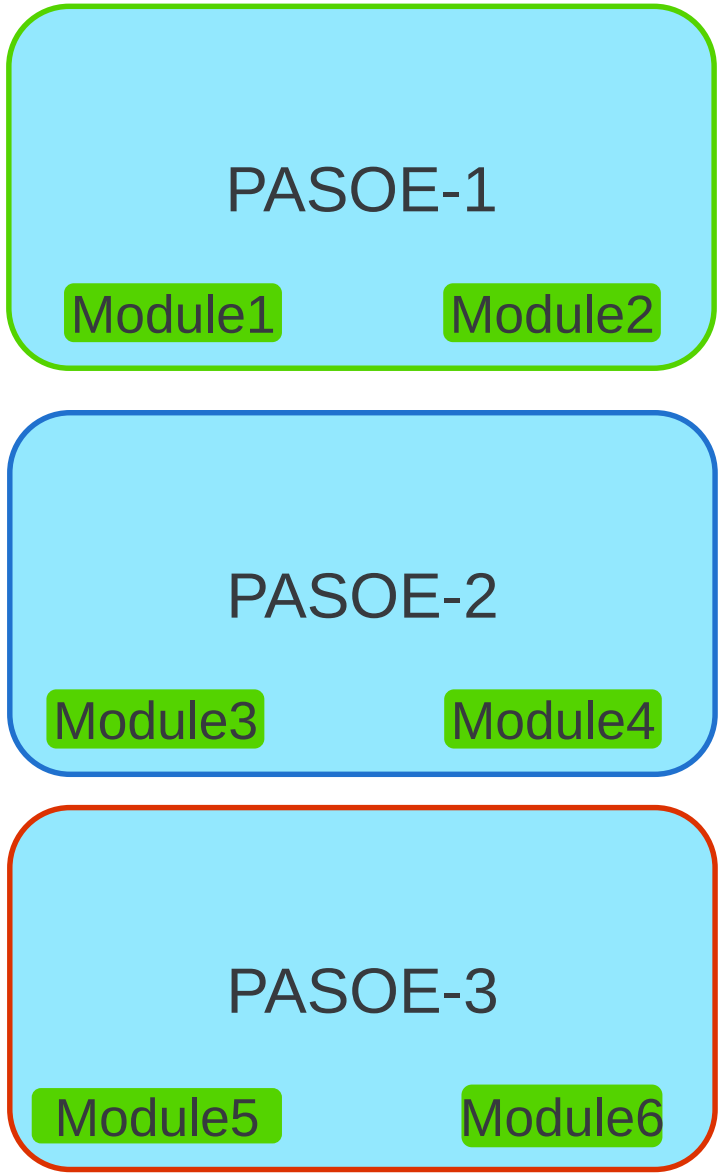


Need for HTTP SSO



Single Sign-On (SSO) est un processus d'authentification qui permet à un utilisateur d'accéder à plusieurs applications avec un seul ensemble d'informations d'identification de connexion.

Validate Client-Principal token



PASOE HTTP SSO

- Requirements to execute this approach
  - **Token producers** that would create Client-Principal tokens that could be stored in a HTTP world.
  - **Token consumers** would could validate the tokens created by the token producers.
  - Regenerate or **refresh the token** on need.

OAuth2 et utilisation dans PASOE

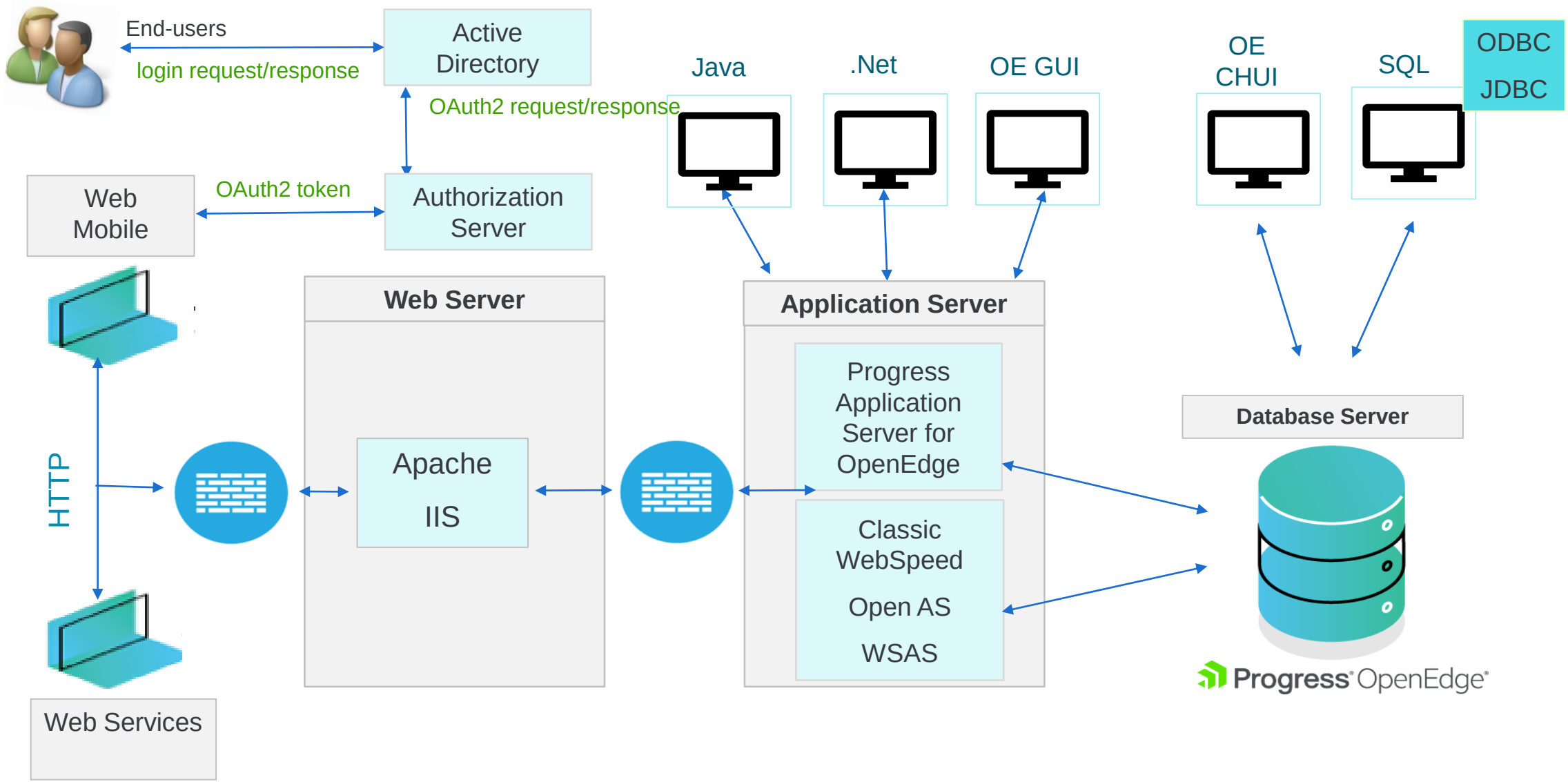
OAuth2

- OAuth 2 est un framework d'autorisation qui permet aux applications d'obtenir un accès limité aux comptes d'utilisateurs sur un service HTTP, tels que Google, AWS, Azure, Github, etc. sans exposer les informations d'identification des utilisateurs.
-
- Il délègue essentiellement l'authentification de l'utilisateur au service qui héberge le compte utilisateur
- ***Progress Application Server (PAS) pour OpenEdge Spring Security comprend la prise en charge de la validation et de l'utilisation d'un serveur de ressources de la norme OAuth 2.0 JSON Web Tokens (JWTs) et des JWT personnalisés.***

OAuth2 Grant types

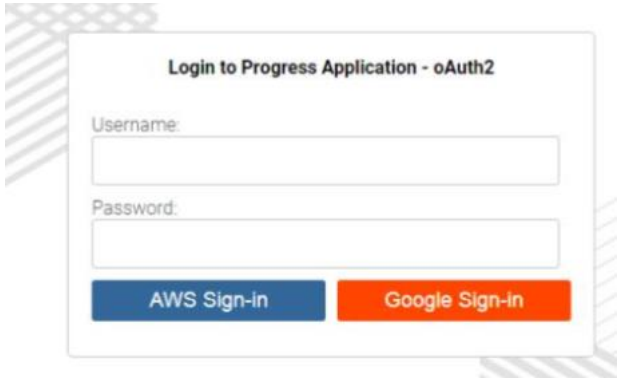
- L’autorisation de l’utilisateur dans OAuth2 est effectuée en affichant une interface fournie par le service à l’utilisateur.
- Ceci est fait par divers «Grant Types» fournis par les serveurs d’autorisation
- Chacun a son propre flux
  - **Authorization Code** – Browser based apps prompting to login
  - **Resource Owner Password Grant** – Exchange credentials for access token
  - **Client Credentials** – Application request for access token not on behalf of user
  - **Implicit** – Return the access token without any authorization code

OAuth2 support in PASOE



Authorization Code Grant - Google

1. Click on “Google Sign-in”



Client App

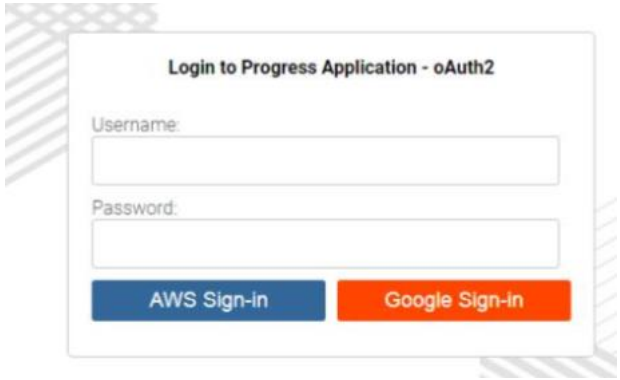
Authorization Server

apiKey = 'CIzaSyCw6ZxuFaw2asd242as5Hh3rPPro1cNaCSI’;

ClientId = ‘164311755842-oc8r2fmq31dgu0sj15bhs6okaajvq7l5.apps.googleusercontent.com’;

Authorization Code Grant - Google

1. Click on “Google Sign-in”
2. Validate Client Identity



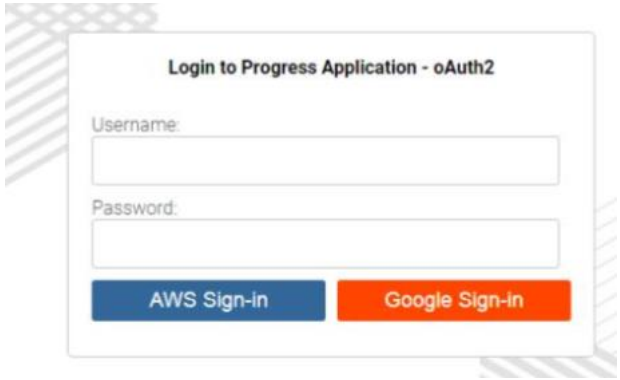
Client App

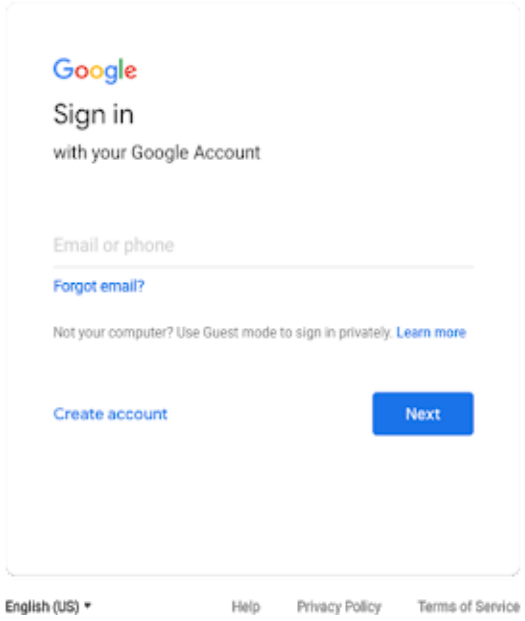
Authorization Server

apiKey = 'CIzaSyCw6ZxuFaw2asd242as5Hh3rPPro1cNaCSI’;

ClientId = ‘164311755842-oc8r2fmq31dgu0sj15bhs6okaajvq7l5.apps.googleusercontent.com’;

Authorization Code Grant - Google





1. Click on “Google Sign-in”
2. Authorize the Client
3. Provide login Page

Client App

Authorization Server

apiKey = 'CIzaSyCw6ZxuFaw2asd242as5Hh3rPPro1cNaCSI’;

ClientId = ‘164311755842-oc8r2fmq31dgu0sj15bhs6okaajvq7l5.apps.googleusercontent.com’;

Authorization Code Grant - Google

1. Click on “Google Sign-in”
2. Authorize the Client
3. Provide login Page
4. Validate Credentials and return Authorization code.

Authorization code

Client App

Authorization Server

apiKey = 'CIzaSyCw6ZxuFaw2asd242as5Hh3rPPro1cNaCSI’;

ClientId = ‘164311755842-oc8r2fmq31dgu0sj15bhs6okaajvq7l5.apps.googleusercontent.com’;

Authorization Code Grant - Google

1. Click on “Google Sign-in”
2. Authorize the Client
3. Provide login Page
4. Validate Credentials and return Authorization code.
5. Request for accesstoken

POST – https://google.com/token

clientId=164311755842&

client_secret=asfk202asdfjasdfajsdf234&

grant_type=authorization_code&

code=**<authcode>**

Client App

Authorization Server


apiKey = 'CIzaSyCw6ZxuFaw2asd242as5Hh3rPPro1cNaCSI’;

ClientId = ‘164311755842-oc8r2fmq31dgu0sj15bhs6okaajvq7l5.apps.googleusercontent.com’;

Authorization Code Grant - Google

1. Click on “Google Sign-in”
2. Authorize the Client
3. Provide login Page
4. Validate Credentials and return Authorization code.
5. Request for accesstoken

accesstoken=<JWT format>

refreshtoken=<token>

Idtoken=<temporary token>

expiration

Client App

Authorization Server


apiKey = 'CIzaSyCw6ZxuFaw2asd242as5Hh3rPPro1cNaCSI’;

ClientId = ‘164311755842-oc8r2fmq31dgu0sj15bhs6okaajvq7l5.apps.googleusercontent.com’;

JWT Token


```
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiAiNzk2NWJ
iYTQtYjY1ZC00MjEyLWFkYzctNmJkMjdlZmYxODB
lIiwidG9rZW5fdXNlIjogImFjY2VzcyIsInNjb3B
lIjogIlBTQ1VzZXIiLCJpc3MiOiAiaHR0cHM6Ly9
ub2RlLXBhc29lIiwiY2xpZW50X2lkIjogIjEyMzQ
1Njc4OSIsImlhdCI6IDE1ODUyNTIyOTUsImV4cCI
6IDE1ODUyNTU5MjUsImp0aSI6ICJlbjJkazRhbmF
vczRnb3dza2N3MDgwc29ndzA0YzAiLCJhdWQiOiA
icGFzb2Uub3BlbmVkZ2UucHJvZ3Jlc3MtdXNlcnM
uY29tIiwiZW1haWwiOiAiaXR0LWRldkBwcm9ncmV
zcy5jb20iLCJ1c2VybmFtZSI6ICJwYXNvZSJ9.Bu
xJCNN4J1q_KJGNDUb4MoBngatAoxdmIi3nzCqrYw
g
```


Claims

Information about the user and additional details.

JWT Token Decoded

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256"
}
```

PAYLOAD: DATA

```
{
  "sub": "7965bba4-b65d-4212-adc7-6bd27eff180e",
  "token_use": "access",
  "scope": "PSCUser",
  "iss": "https://node-pasoe",
  "client_id": "123456789",
  "iat": 1585252295,
  "exp": 1585255925,
  "jti": "en2dk4anaos4gowskcw080sogw04c0",
  "aud": "pasoe.openedge.progress-users.com",
  "email": "itt-dev@progress.com",
  "username": "pasoe"
}
```

→ issuer

→ Issue at

→ Unique ID of JWT

→ Intended recipients of JWT token

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

OAuth2 - Actors

Client / User-Agent

Authorization Server

Resource Owner

End-user logging-in to the application and providing limited access to this details.

Resource Server

PASOE

OAuth2 - Actors

Client / User-Agent

JavaScript application running in a browser.

Authorization Server

Resource Owner

Resource Server

PASOE

OAuth2 - Actors

Client / User-Agent

Authorization Server

Resource Owner

A Web Service that basically validates the token and provides data services to the Resource Owner.

Resource Server

PASOE

OAuth2 - Actors

Client / User-Agent

Responsible for authenticating the Resource owner, provide access tokens to the client and validate the token if required.

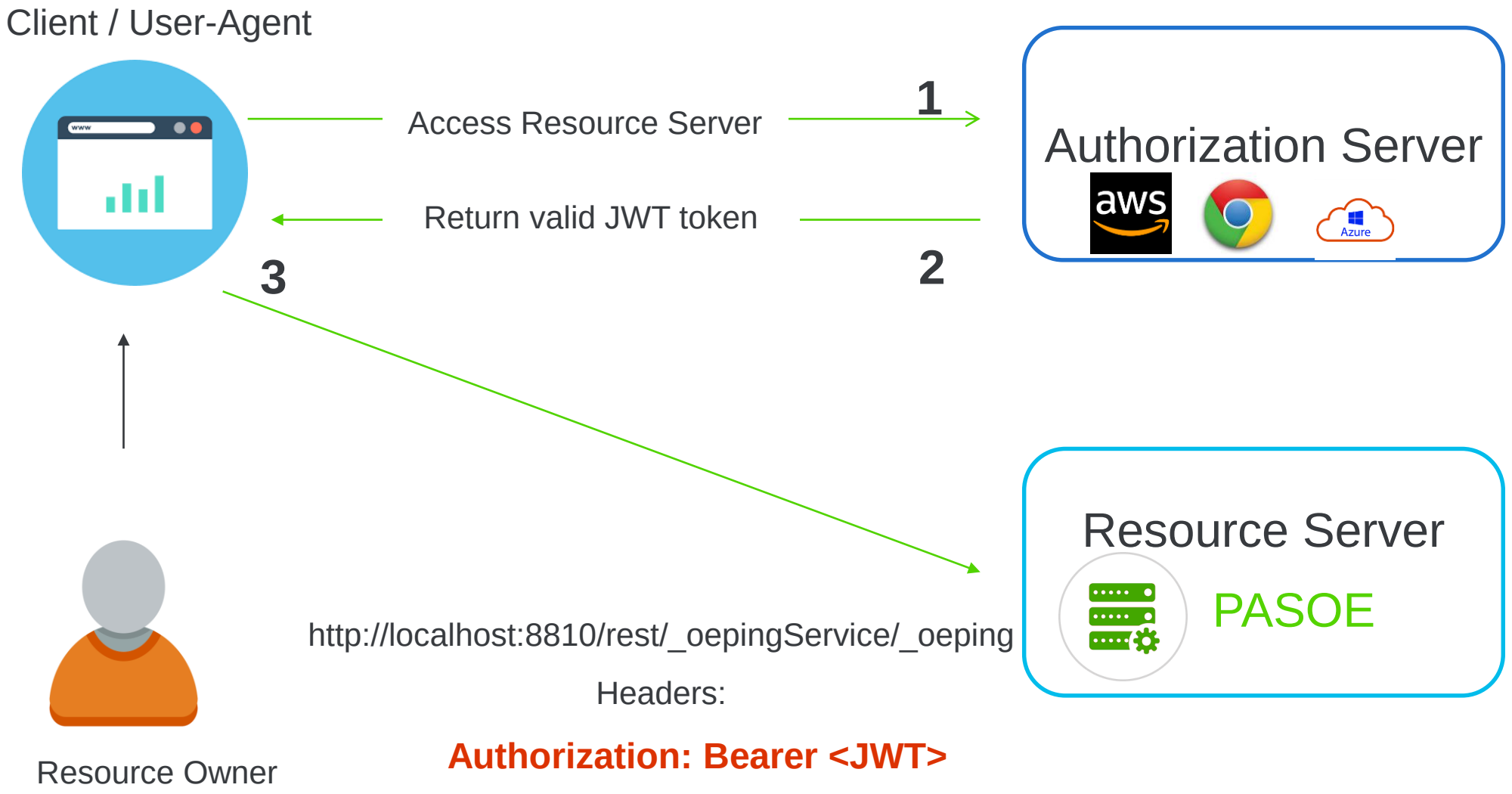
Authorization Server

Resource Owner

Resource Server

PASOE

OAuth2 - Roundtrip



OAuth2 validation in PASOE

http://localhost:8810/rest/_oepingService/_oeping

Headers:

Authorization: Bearer <JWT>

PASOE

OAuth2 AuthProvider

- Validate the JWT token signature
  - HMAC - Hash-based Message Authentication Code
  - RSA - RSA Algorithms using Certificates
  - JWK – Json Web Keyset
    - https://www.googleapis.com/oauth2/v3/certs
- Convert the JWT token to Client-Principal
- Authorization of the scope of the user with the resource URI's.

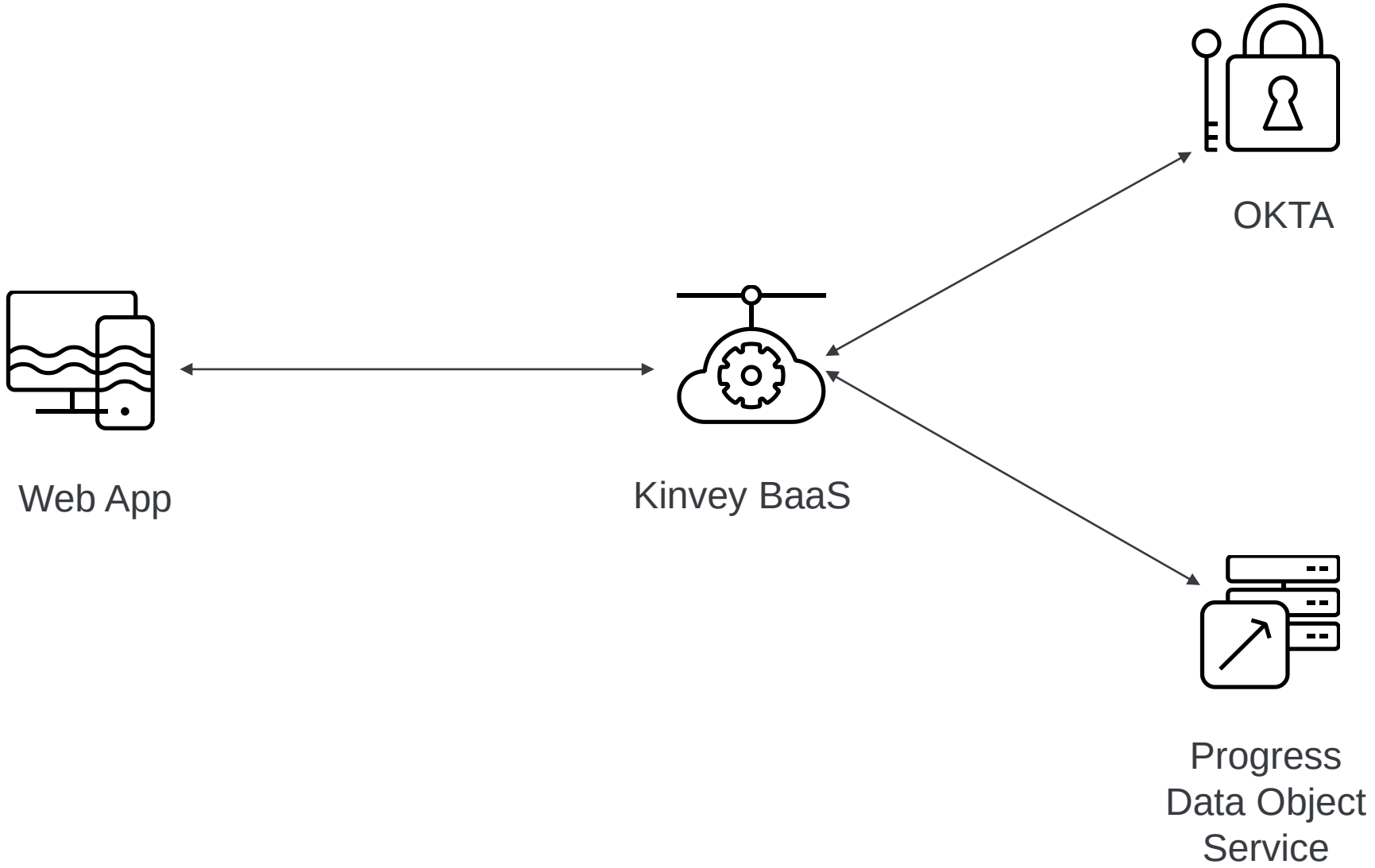
Spring Security en bref

- Configuration Spring Security revue en 11.7
  - Pas besoin d’éditer des fichiers XML
  - Configuration basée sur des fichiers “property”
- Support SAML
- Support OAUTH2
- OE Authentication Gateway intégré
- Support “Wildcard” (caractères génériques) et SNI (Server Name Indication)
- Mise à jour des “ciphers” (12.0)

Quelques liens utiles

- Kbase
  - SAMPLE FOR PASOE SUPPORT FOR JWT AND OAUTH 2.0
- Liste provider oAuth
  - https://en.wikipedia.org/wiki/List_of_OAuth_providers
  - Quelques provider courants ：OKTA , KEYCLOAK , GOOGLE , FACEBOOK, AMAZON , GITHUB
- Progress Documentation
  - Authentication with OAuth2 and JWT

Vidéo Kinvey pour accéder à Progress Data Object Service via OAuth2



Security HealthCheck

Progress Services

- Survey
- Education
- Implementation

Implementation

Phase I

- Survey
- Discussion and identification of any security vulnerabilities
- Recommendation of a customized project plan and statement of work

Phase II

- Client-Principle Object
  User Credential Storage
  Single Sign On
- Security Domains
  Authentication Gateway
  OpenEdge Realm
- 3rd Party Authentication
  Spring Security Setup
  Enable TLS

* Hours vary based on strategic goals and state of the application.

Prochaines Formations Virtuelles (Francais)

Thèmes	Dates
Administration de base de Données (DBA) R.12.x https://www.progress.com/services/education/instructor-led/europe/openedge-database-administration-bootcamp	27-30 Avril
Formation ABL GUI https://www.progress.com/services/education/instructor-led/europe/progress-abl-gui-bootcamp-france	25-29 Mai
Optimisation des performances des bases de données OpenEdge https://www.progress.com/services/education/instructor-led/europe/openedge-database-performance-tuning	25-27 Mai
Programmation Orientée Objet Avancée conforme OERA https://www.progress.com/services/education/instructor-led/europe/advanced-object-oriented-programming-in-oera	8-10 Juin
Progress Academy Avancée https://www.progress.com/services/education/openedge/advanced-openedge-academy	8-12 Juin
Progress Application Server for OpenEdge (PASOE) https://www.progress.com/services/education/instructor-led/europe/progress-application-server-for-oe-admin	15-17 Juin

Progress®

Q&R


Progress®