Progress

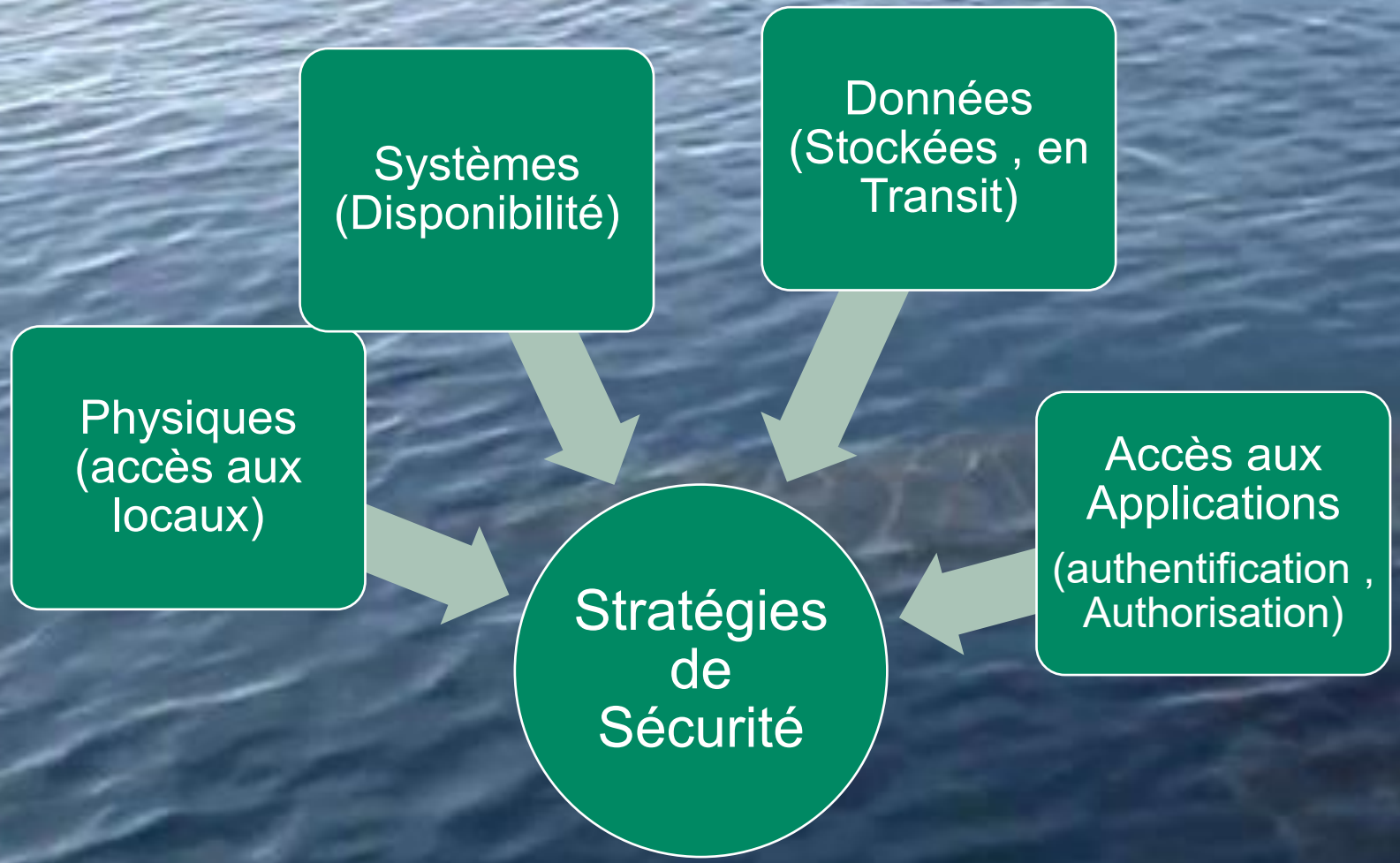
La sécurité dans vos applications OpenEdge : facultative, obligatoire ou indispensable ?

Laurent Kieffer

3 Juin 2025

laurent@progress.com

Sécurité⇔ Une vaste étendue.. avec des risques



Besoin de Sécurité pour ces 2 activités ?

Agenda

- Why Security Matters
- How Progress Helps Secure Your Application
- OpenEdge 12.8 Security Features
  - Demo : PASOE & Keycloak
  - TDE
  - DDM

Progress

The enemy is getting smarter. They’re AI-enabled and they’re relentless.

You Don’t Want This to Be You

Disney **lost 1 terabyte of content** in July 2024 from Slack. Now leaving Slack.

Temu may have **lost 87 Billion data records**. They have not yet confirmed.

DICK’S Sporting Goods had to **shut down email** after an attack.

23andMe **lost genetic information on 6.4 million customers and settled lawsuit for $30M.**

Attack him where he is unprepared, appear where you are unexpected.

- Sun Tzu

Education is Critical

- “But we’re behind the firewall…”
- “...Oooh, you mean test systems need protecting too!”
- “…There was this strange email... I clicked on it…”
- “No one told me...”
- “Wait, isn't that the vendor's job?"

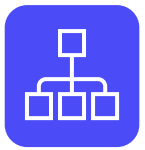
We are all responsible for our application security.

What Is Application Security?

- The set of procedures, industry standards and technological tools used to prevent unauthorized access to application data is known as *business application security*.
- The major areas where there is an IT security focus include:

Disk Storage

Operating System



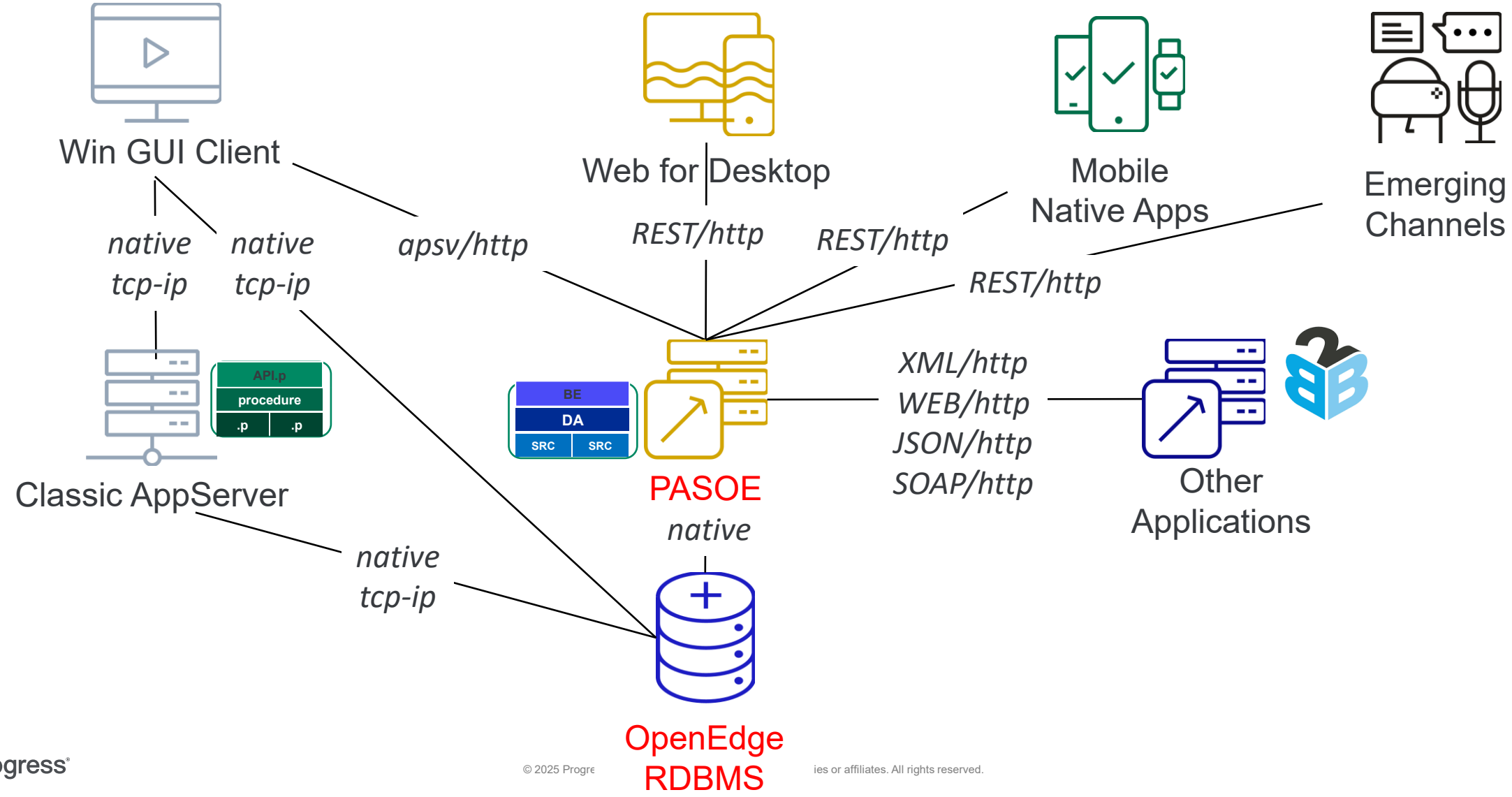
Network Connectivity

Third-Party Integrations

Application Authentication & Authorization

Data

Discovering what is concerned by Security



How Progress Helps Secure Your Application

Our Commitment to You: Platform Security

- An OpenEdge application is a combination of the OpenEdge platform plus the ABL code written by our customers
  - The security of the platform, code written by Progress and 3rd party libraries, is maintained by Progress
  - The security of the application is maintained by OpenEdge customers (developers), in concert with the security features supplied by the platform
- This presentation primarily focuses on application security features

Identity Management

- A set of systems and tools to control the user identities encountered by OpenEdge.
- Provides options to manage identity without the need for application code changes.
- Allows the resources of an information system—including applications and data—to be accessed only by trusted users in a manner that is appropriate for each individual user or group of users.
  - An *authentication system* serves as the gateway for all access to the information system.
  - An *authorization system* determines if and how a user can access the resource.
- Both *could* be built using ABL, however, most prefer to use vendor-supplied solutions (Active Directory, LDAP, etc.) that OpenEdge integrates with

Protecting Data in Motion

- The OpenEdge team balances backward compatibility with eliminating well-known vulnerable protocols, cryptography hashes and encryption

What is TLS?	TLS (formerly SSL) is a point-to-point authenticated connection for secure data communications.		
Purpose	Authentication	Confidentiality	Integrity
Implementation	Digital Certificates	Encryption	Message Digest
Benefits of TLS	Protection against cyber threats like eavesdropping, session hijacking Reduce breach costs and insurance premiums	Interoperability	Compliance and regulatory requirements Build trust with customers

How to Secure Your Application with OpenEdge 12

OpenEdge 12.8 Security Features

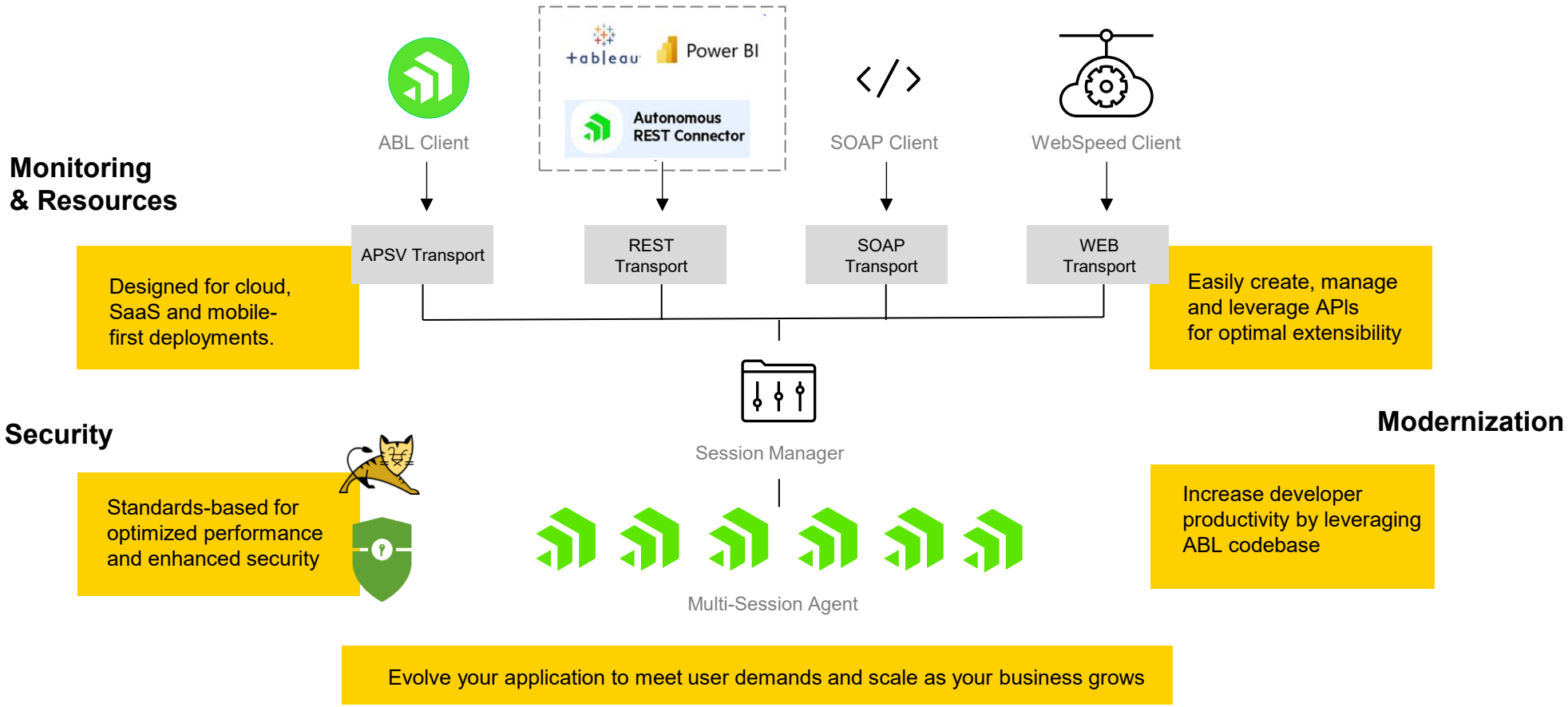
- Progress Application Server (PAS) for OpenEdge
- OpenEdge Authentication Gateway
- OpenEdge Advanced Security
  - Dynamic Data Masking (DDM)
  - Hardware Security Module (HSM)
  - JSON Web Encryption
  - Transparent Data Encryption (TDE)*

The Foundation: PAS for OpenEdge

- Released in OpenEdge 11.5 (December 2014)
- Built on the Tomcat Web Server
- Includes Spring Security Framework
- Foundation for the OpenEdge Authentication Gateway
- The **only** Application Server available in OpenEdge 12

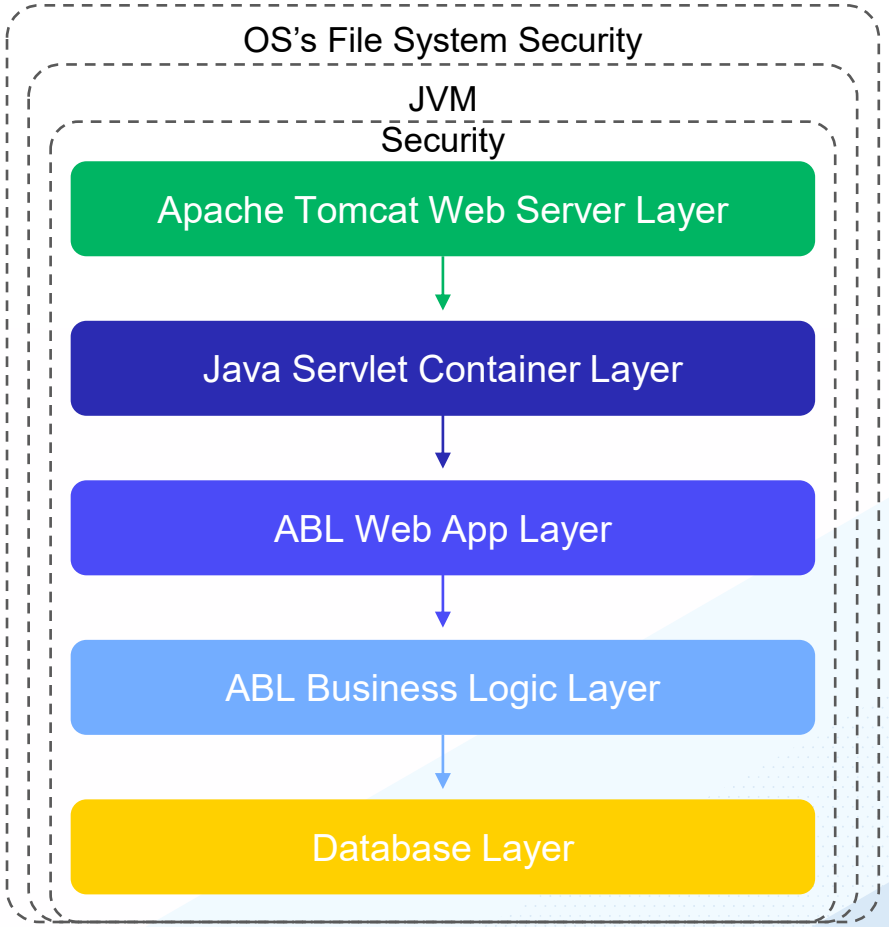
Progress Application Server (PAS) for OpenEdge

Scalable, Secure and Standards-Based



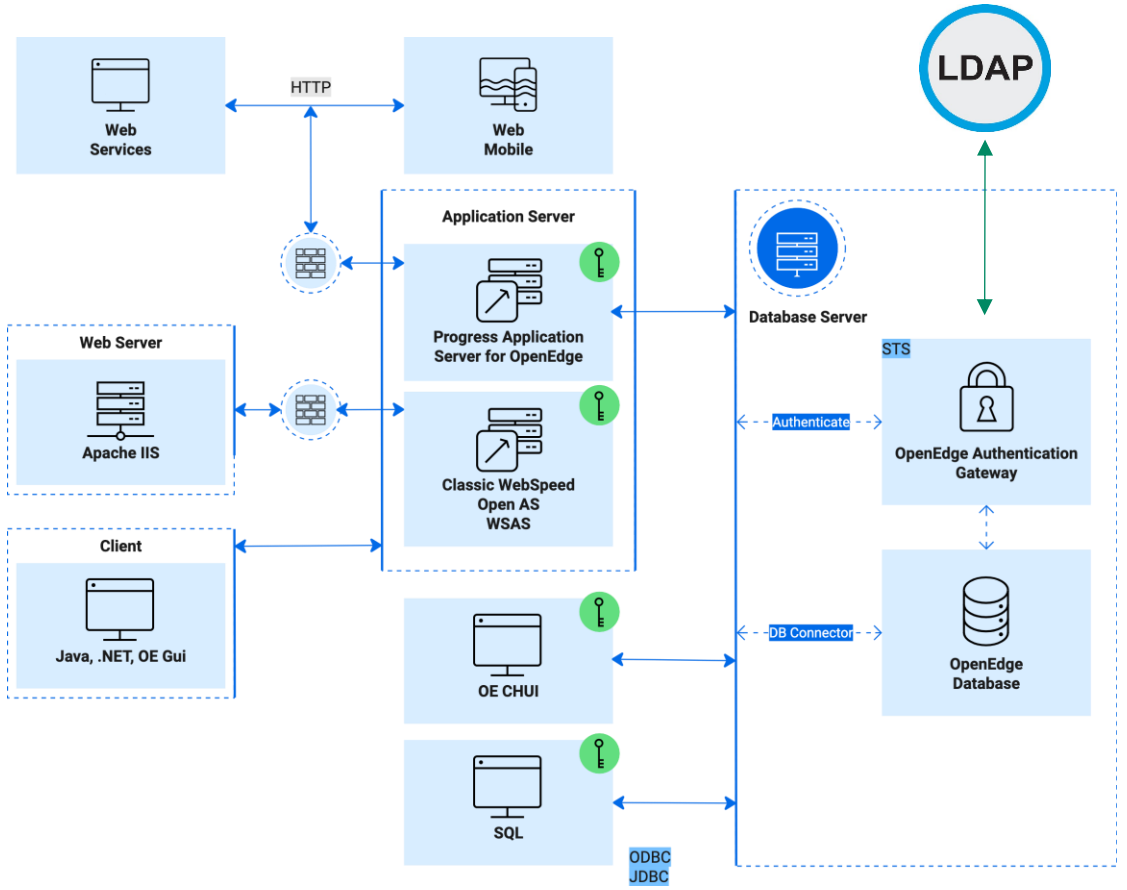
PAS for OpenEdge Security Stack

- Contains 5 layers of protection as shown on the right
- Additional capability includes:
  - HTTPS TLS
  - Java servlet authentication and authorization
  - Spring-based authentication, authorization and HTTP session management
  - Validation of OpenEdge Client Principal objects



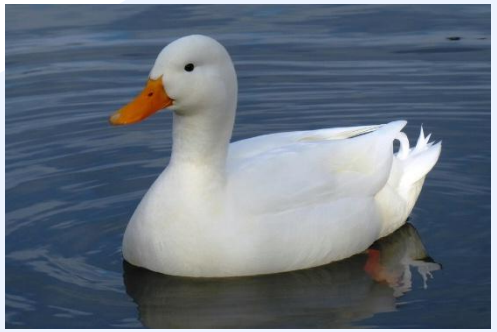
OpenEdge Authentication Gateway

- Facilitates trusted identity management by hardening the security of your OpenEdge application environment
- Redirects all access requests to a secure token service (STS) that confirms user legitimacy and helps protect against malicious data manipulation
- Prevents rogue clients from going around the authentication and accessing the database or other application components directly
- Supports compliance with regulation requirements to minimize business risk



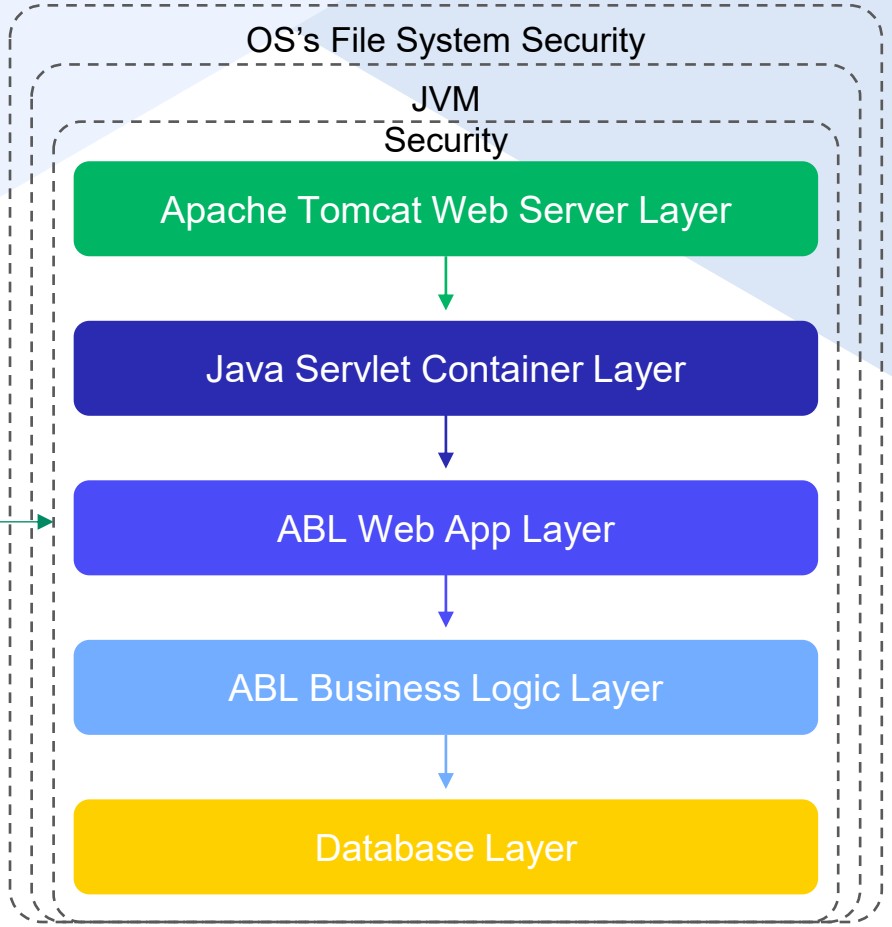
OpenEdge Authentication Gateway Key Features

- Redirects initial access requests to a secure token service (STS) that confirms user legitimacy
- Assigns a standard, strongly encrypted Client Principal token to authenticated clients to act as the data record that helps protect against strong cryptography manipulation
- Client Principal maintains a chain of trust between the token and OpenEdge application
- Makes authorization decisions for trusted users to support proper data access
- Integrates with popular identity-related services such as LDAP and Active Directory



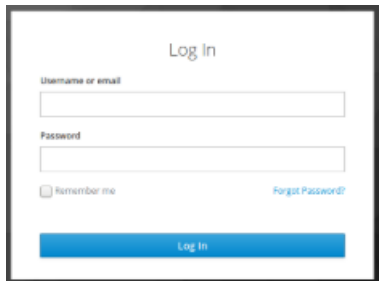
A qui fait on référence avec ces images? Merci de garder votre idée pour la fin de la présentation ?

Démo PASOE Sécurité Webapp



PASOE : Exemple de Sécurisation

- PASOE : Resource Server
  - Secure APIs , Back end access
- Client Application : Application Web
- Authorization Server (IDP) : Keycloak



1 Login

2 JWT Token

KEYCLOAK

Web for Desktop

3 Authorization Bearer Token

PASOE

4 Public Key Verification

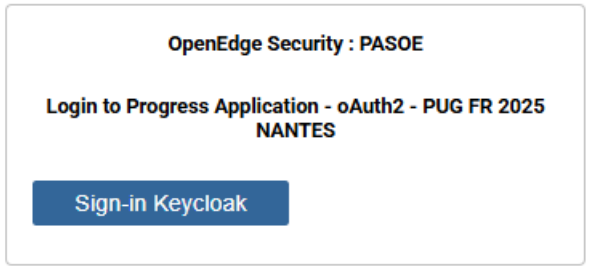
http://localhost:8080/auth/realms/loulou/protocol/openid-connect/certs

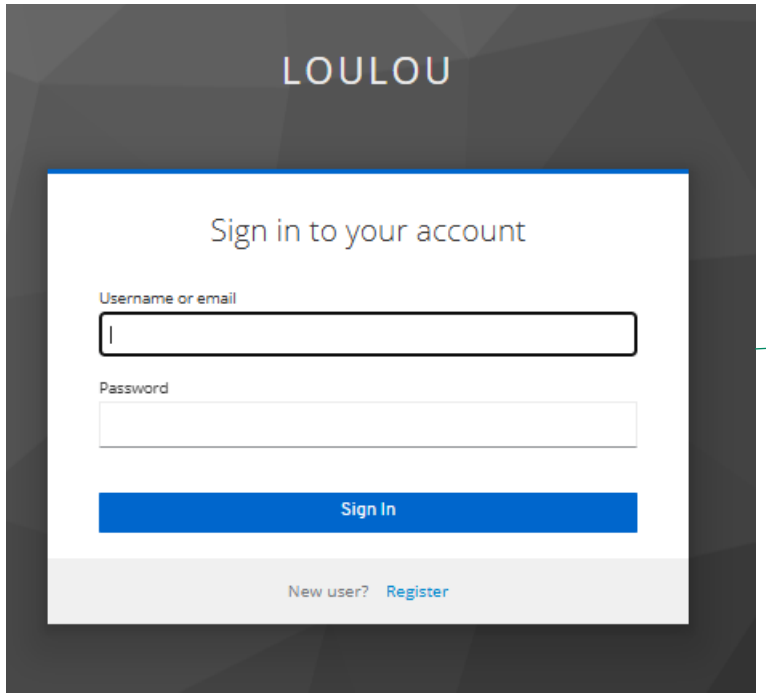

```
{"kid": "NNj_N_ySDycNQUIZyJJW-2Hk2AnNU3ZBfkDeA87XSiw",
```



```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "NNj_N_ySDycNQUIZyJJW-2Hk2AnNU3ZBfkDeA87XSiw"
}
```

http://localhost:9010/KCClient/static/oauth/loginPage.html





CustNum	Customer Name	Address
1	Lift Tours	276 North Drive
2	Urpon Frisbee	Rattipolku 3
3	Hoops	Suite 415
4	Go Fishing Ltd	Unit 2
5	Match Point Tennis	66 Homer Pl
6	Fanatical Athletes	20 Bicep Bridge Rd
7	Aerobics valine Ky	Peltolantie 3
8	Game Set Match	Box 60
9	Pihtiputaan Pyora	Putikontie 2
10	Just Joggers Limited	Fairwind Trading Est
11	Keilailu ja Biljardi	Vattuniemenkuja 8 A
12	Surf Lautaveikkoset	Venemestarinkatu 35
13	Biljardi ja tennis	Urheilutie 1
14	Paris St Germain	113, avenue du Stade
15	Hoopla Basketball	87 Calumnet St
16	Thundering Surf Inc.	354 Market St.
17	High Tide Sailing	178 Schooner Hill
18	Antin Metsastysase	Vanhainkodinkuja 1
19	Buffalo Shuffleboard	155 Carolina Ave
20	Espoon Pallokeskus	Sinikalliontie 18

1

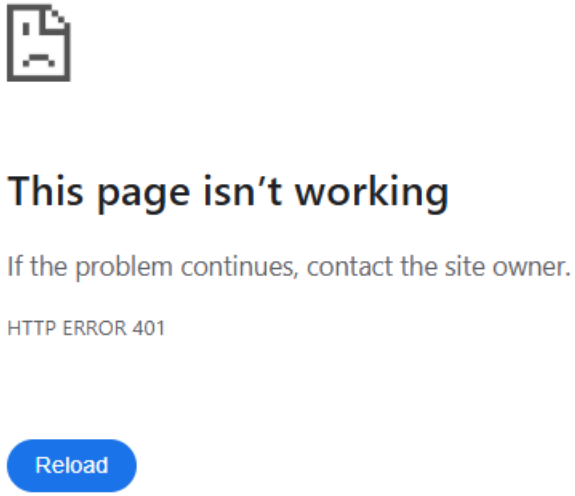
Logout

http://localhost:9010/RestKeycloak/rest/RestKeycloakService/beCustomer


```
{
  "dsCustomer": {
    "prods:hasChanges": true,
    "ttCustomer": [
      {
        "CustNum": 1,
        "Country": "USA",
        "Name": "Lift Tours",
        "Address": "276 North Drive",
        "Address2": "",
        "City": "Burlington",
        "State": "MA",
        "PostalCode": "01730",
        "Contact": "Gloria Shepley",
        "Phone": "(617) 450-0086",
        "SalesRep": "HXM",
        "CreditLimit": 66711,
        "Balance": 903.64,
        "Terms": "Net30",
        "Discount": 35,
        "Comments": "This customer is on credit hold.",
        "Fax": "",
        "EmailAddress": ""
      },
      {
        "CustNum": 2,
        "Country": "Finland",
        "Name": "Urpon Frisbee",
        "Address": "Rattipolku 3",
        "Address2": "",
        "City": "Oslo",
        "State": "Uusima",
        "PostalCode": "45321",
        "Contact": "Urpo Leppakoski",
        "Phone": "(603) 532 5471",
        "SalesRep": "DKP",
        "CreditLimit": 27611,
        "Balance": 437.63,
        "Terms": "Net30",
        "Discount": 35,
        "Comments": "Ship all products 2nd Day Air.",
        "Fax": "",
        "EmailAddress": ""
      },
```

http://localhost:9010/RestKeycloak/rest/RestKeycloakService/beCustomer

- Après expiration du Token (60s)



Admin-cli

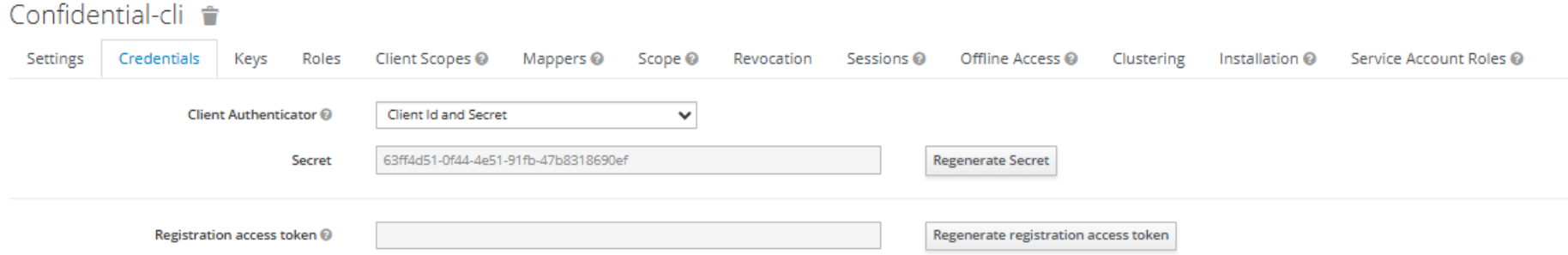
Settings | Keys | Roles | Client Scopes | Mappers | Scope | Revocation | Sessions | Offline Access | Installation

Client ID	admin-cli
Name	${client_admin-cli}
Description	
Enabled	ON
Always Display in Console	OFF
Consent Required	OFF
Login Theme	
Client Protocol	openid-connect
Access Type	public
Standard Flow Enabled	ON
Implicit Flow Enabled	OFF
Direct Access Grants Enabled	ON
OAuth 2.0 Device Authorization Grant Enabled	OFF
Root URL	
* Valid Redirect URIs	*
Base URL	
Admin URL	
Web Origins	http://localhost:9010
Backchannel Logout URL	
Backchannel Logout Session Required	OFF
Backchannel Logout Revoke Offline Sessions	OFF

Confidential-cli

Settings | Credentials | Keys | Roles | Client Scopes | Mappers | Scope | Revocation | Sessions | Offline Access | Clustering | Installation | Service Account Roles

Client ID	confidential-cli
Name	
Description	
Enabled	ON
Always Display in Console	OFF
Consent Required	OFF
Login Theme	
Client Protocol	openid-connect
Access Type	confidential
Standard Flow Enabled	ON
Implicit Flow Enabled	OFF
Direct Access Grants Enabled	ON
Service Accounts Enabled	ON
OAuth 2.0 Device Authorization Grant Enabled	OFF
OIDC CIBA Grant Enabled	OFF
Authorization Enabled	OFF
Root URL	
* Valid Redirect URIs	*
Base URL	
Admin URL	http://localhost:8080
Web Origins	
Backchannel Logout URL	
Backchannel Logout Session Required	ON
Backchannel Logout Revoke Offline Sessions	OFF



1 Connect

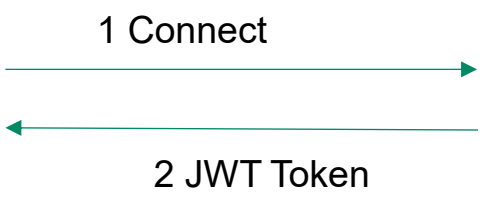
2 JWT Token

POST http://192.168.1.71:8080/auth/realms/loulou/protocol/openid-connect/token

Params Body • Headers Auth • Vars Script Assert Tests Docs

Key	Value
client_id	admin-cli
username	lulu
password	lulu
grant_type	password


```
{
  "access_token":
"eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJOTmpfTl95U0R5Y05RVUlaeUpKVy0ySGsyQW
5OVTNaQmZrRGVBODdYU2l3In0.eyJleHAiOjE3NDcxMzczMjUsImlhdCI6MTc0NzEzNzE0NSwianRpIjoi
YTVmN2EzNzctMWZkMi00Y2JlLTg0MjgtZTEwMjRiNTIwZDNiIiwiaXNzIjoiaHR0cDovLzE5Mi4xNjguMS4
3MTo4MDgwL2F1dGgvcmVhbG1zL2xvdWxvdSIsInN1YiI6IjcyY2ZhODA3LTIyMGUtNGVlNi1iMGIzLTM3
OWI3NzRhZGFkYSIsInR5cCI6IkJlYXJlciIsImF6cCI6ImFkbWluLWNsaSIsInNlc3Npb25fc3RhdGUiOiJlZD
NmYTJlNi01YzJkLTQ2ZmQtYmY0MS01MGEyZThhNDBmZTUiLCJhY3IiOiIxIiwic2NvcGUiOiJlbWFpbCB
wcm9maWxlIiwic2lkIjoiZWQzZmEyZTYtNWMyZC00NmZkLWJmNDEtNTBhMmU4YTQwZmU1IiwiZW1h
aWxfdmVyaWZpZWQiOmZhbHNlLCJuYW1lIjoibHVsdSBsdWx1IiwicHJlZmVycmVkX3VzZXJuYW1lIjoib
HVsdSIsImdpdmVuX25hbWUiOiJsdWx1IiwibG9jYWxlIjoiZW4iLCJmYW1pbHlfbmFtZSI6Imx1bHUiLCJlb
WFpbCI6Imx1bHVAcHJvZ3Jlc3MifQ.RdjyRadUajkSmGIDFJTq5-
qSfp9e0nEon8dsjP0F6iJLxU1syHPSKnMgjo6V4HZwzEOi3Pz2LPhBixYwNzJsnMafEStAyxaWjV8XSCeC
Li4f3AdkTRCJAffNFpsTDXTeRZPE_H2nqPkyE6zSJR7B4fHSR_oMB7zZYM0p2H0aGP68hPtdGAq5YQ
RK-
JL2umCpvTrIveWNVsAGmFXINV3ForUyaa1upKFFTkcfbscwgHGFntBxfxtmfcwSANIbBLPT7IIMg4tuRba
c2ubAGl1zkFBH1_8qiV4Mu9A1bEum-9bebD_00A3GaJK9Wja5xlFsti1gFRN49eBKMWsjmXtRwQ",
  "expires_in": 179,
  "refresh_expires_in": 1799,
  "refresh_token":
"eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICIxZmRkNjUyOS1hZTRjLTQ3ZDUtYjU1Ny0wYWN
iY2I2YjQxY2IifQ.eyJleHAiOjE3NDcxMzg5NDUsImlhdCI6MTc0NzEzNzE0NSwianRpIjoiODA2Yjk5OTMtM
GM5OS00MjMwLTgyMmMtNDQxY2Q3ODdiMWI0IiwiaXNzIjoiaHR0cDovLzE5Mi4xNjguMS43MTo4MDg
wL2F1dGgvcmVhbG1zL2xvdWxvdSIsImF1ZCI6Imh0dHA6Ly8xOTIuMTY4LjEuNzE6ODA4MC9hdXRoL3
JlYWxtcy9sb3Vsb3UiLCJzdWIiOiI3MmNmYTgwNy0yMjBlLTRlZTYtYjBiMy0zNzliNzc0YWRhZGEiLCJ0e
XAiOiJSZWZyZXNoIiwiYXpwIjoiYWRtaW4tY2xpIiwic2Vzc2lvbl9zdGF0ZSI6ImVkM2ZhMmU2LTVjMmQt
NDZmZC1iZjQxLTUwYTJlOGE0MGZlNSIsInNjb3BlIjoiZW1haWwgcHJvZmlsZSIsInNpZCI6ImVkM2ZhM
mU2LTVjMmQtNDZmZC1iZjQxLTUwYTJlOGE0MGZlNSJ9.vwDMe_AREg1qiBA6ww76AdArp2hoCBaB2
V9h7fC2p2w",
  "token_type": "Bearer",
  "not-before-policy": 0,
  "session_state": "ed3fa2e6-5c2d-46fd-bf41-50a2e8a40fe5",
  "scope": "email profile"
}
```



Params Body • Headers Auth • Vars Script Assert Tests

Docs Form URL Encoded

Key	Value	
client_id	confidential-cli	☑ 🗑
client_secret	63ff4d51-0f44-4e51-91fb-47b831	☑ 🗑
grant_type	client_credentials	☑ 🗑


```
{
  "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJ
OTmpfTl95U0R5Y05RVUlaeUpKVy0ySGsyQW5OVTNaQmZrRGVBODdYU2l3In0.eyJleHAiO
jE3NDc3NDAzNTYsImlhdCI6MTc0Nzc0MDI5NiwianRpIjoiY2RiNjViNDAtODY0NC00MWN
iLWFiZTUtMjBhZDY2ZDg1NDYxIiwiaXNzIjoiaHR0cDovL2xvY2FsaG9zdDo4MDgwL2F1d
GgvcmVhbG1zL2xvdWxvdSIsImF1ZCI6ImFjY291bnQiLCJzdWIiOiI3NzJjYTJiZi03ODR
iLTQ0YzUtYTYwMS1jNzJjNTA5ZmFkZTIiLCJ0eXAiOiJCZWFyZXIiLCJhenAiOiJjb25ma
WRlbnRpYWwtY2xpIiwiYWNyIjoiMSIsInJlYWxtX2FjY2VzcyI6eyJyb2xlcyI6WyJkZWZ
hdWx0LXJvbGVzLWxvdWxvdSIsIm9mZmxpbmVfYWNjZXNzIiwidW1hX2F1dGhvcml6YXRpb
24iXX0sInJlc291cmNlX2FjY2VzcyI6eyJhY2NvdW50Ijp7InJvbGVzIjpbIm1hbmFnZS1
hY2NvdW50IiwibWFuYWdlLWFjY291bnQtbGlua3MiLCJ2aWV3LXByb2ZpbGUiXX19LCJzY
29wZSI6ImVtYWlsIHByb2ZpbGUiLCJjbGllbnRJZCI6ImNvbmZpZGVudGlhbC1jbGkiLCJ
lbWFpbF92ZXJpZmllZCI6ZmFsc2UsImNsaWVudEhvc3QiOiIxNzIuMjIuMC4xIiwicHJlZ
mVycmVkX3VzZXJuYW1lIjoic2VydmljZS1hY2NvdW50LWNvbmZpZGVudGlhbC1jbGkiLCJ
jbGllbnRBZGRyZXNzIjoiMTcyLjIyLjAuMSJ9.QtfICyj2eHQzEAlS3S9rBlZYP71OEyCP
mMRZDfFc56-tZ2JmuXcQg8aLctBhcx40AEMm466OI7ioraJk4fQ29xFzmOrcUEysBipG6D
LZ5sOusMUEvA1QGM5h_YtEppWM9AYcCbZzHrkgLVpYicmhEejnHd7twSasWYEjacEHUBsX
wSCo21ZZ0qfL1QOJdU3j6xoTfQ_YU7cJBBc4soRO6_gc7FP2wOHUoZsx2xkvtlUYs2cGiV
85A6Cxeaa1-yKmfx2rH-6LF3TFCUYtH1_rWgFJlEj9DLjUc96L65fjhXnoB4DypT6x22rk
J_q8--rpQ_QgXUVAGgwPXjVNmgE_Dg",
  "expires_in": 60,
  "refresh_expires_in": 0,
  "token_type": "Bearer",
  "not-before-policy": 0,
  "scope": "email profile"
}
```

Jwt.io

Encoded PASTE A TOKEN HERE


```
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiw
ia2lkIiA6ICJOTmpfTl95U0R5Y05RVUlaeUpKVy
0ySGsyQW5OVTNaQmZrRGVBODdYU2l3In0.eyJle
HAiOjE3NDcxMzczMjUsImlhdCI6MTc0NzEzNzE0
NSwianRpIjoiYTVmN2EzNzctMWZkMi00Y2JlLTg
0MjgtZTEwMjRiNTIwZDNiIiwiaXNzIjoiaHR0cD
ovLzE5Mi4xNjguMS43MTo4MDgwL2F1dGgvcmVhb
G1zL2xvdWxvdSIsInN1YiI6IjcyY2ZhODA3LTIy
MGUtNGVlNi1iMGIzLTM3OWI3NzRhZGFkYSIsInR
5cCI6IkJlYXJlciIsImF6cCI6ImFkbWluLWNsaS
IsInNlc3Npb25fc3RhdGUiOiJlZDNmYTJlNi01Y
zJkLTQ2ZmQtYmY0MS01MGEyZThhNDBmZTUi
Y3IiOiIxIiwic2NvcGUiOiJlbWFpbCBwcm9maWx
lIiwic2lkIjoiZWQzZmEyZTYtNWMyZC00NmZkLW
JmNDEtNTBhMmU4YTQwZmU1IiwiZW1haWxfdmVya
WZpZWQiOmZhbHNlLCJuYW1lIjoibHVsdSBsdWx1
IiwicHJlZmVycmVkX3VzZXJuYW1lIjoibHVsdSI
sImdpdmVuX25hbWUiOiJsdWx1IiwibG9jYWxlIj
oiZW4iLCJmYW1pbHlfbmFtZSI6Imx1bHUiLCJlb
WFpbCI6Imx1bHVAcHJvZ3Jlc3MifQ.RdjyRadUa
jkSmGIDFJTq5-
qSfp9e0nEon8dsjP0F6iJLxU1syHPSKnMgjo6V4
HZwzEOi3Pz2LPhBixYwNzJsnMafEStAyxaWjV8X
SCeCLi4f3AdkTRCJAffNFpsTDXTeRZPE_H2nqPk
yE6zSJR7B4fHSR_oMB7zZYM0p2H0aGP68hPtdGA
q5YQRK-
JL2umCpvTrIveWNVsAGmFXINV3ForUyaa1upKFF
TkcfbscwgHGFntBxfxtmfcwSANIbBLPT7IIMg4t
uRbac2ubAGl1zkFBH1_8qiV4Mu9A1bEum-
9bebD_00A3GaJK9Wja5xlFsti1gFRN49eBKMWsj
mXtRwQ
```


Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE


```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "NNj_N_ySDycNQUIZyJJW-2Hk2AnNU3ZBfkDeA87XSiw"
}
```


PAYLOAD: DATA


```
{
  "exp": 1747137325,
  "iat": 1747137145,
  "jti": "a5f7a377-1fd2-4cbe-8428-e1024b520d3b",
  "iss": "http://192.168.1.71:8080/auth/realms/loulou",
  "sub": "72cfa807-220e-4ee6-b0b3-379b774adada",
  "typ": "Bearer",
  "azp": "admin-cli",
  "session_state": "ed3fa2e6-5c2d-46fd-bf41-
50a2e8a40fe5",
  "acr": "1",
  "scope": "email profile",
  "sid": "ed3fa2e6-5c2d-46fd-bf41-50a2e8a40fe5",
  "email_verified": false,
  "name": "lulu lulu",
  "preferred_username": "lulu",
  "given_name": "lulu",
  "locale": "en",
  "family_name": "lulu",
  "email": "lulu@progress"
}
```


Subject (whom the token refers to)

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key in SPKI, PKCS #1,
  X.509 Certificate, or JWK stri
  ng format.
  ,
  Private Key in PKCS #8, PKCS #
  1, or JWK string format. The k
  ey never leaves your browser.
```

3 Authorization Bearer Token

GET http://localhost:9010/RestKeycloak/rest/RestKeycloakService/beCustomer?filter=name begins 'lift'

Params 1 Body • Headers 1 Auth • Vars Script Assert Tests Docs

Key	Value	
Authorization	Bearer eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIi	

Response Headers 12 Timeline Tests 200 OK 627ms 430B


```
{
  "dsCustomer": {
    "prods:hasChanges": true,
    "ttCustomer": [
      {
        "CustNum": 1,
        "Country": "USA",
        "Name": "Lift Tours",
        "Address": "276 North Drive",
        "Address2": "",
        "City": "Burlington",
        "State": "MA",
        "PostalCode": "01730",
        "Contact": "Gloria Shepley",
        "Phone": "(617) 450-0086",
        "SalesRep": "HXM",
        "CreditLimit": 66711,
        "Balance": 903.64,
        "Terms": "Net30",
        "Discount": 35,
        "Comments": "This customer is on credit hold.",
        "Fax": "",
        "EmailAddress": ""
      }
    ],
    "prods:before": {}
  }
}
```

Activate.p : Claims ➔ pasoe log

```
VAR HANDLE hCP.
var int i, propertyCount.
VAR CHAR propertyName.

hCP = SESSION:CURRENT-REQUEST-INFO:GETCLIENTPRINCIPAL ().
propertyCount = NUM-ENTRIES (hCP:LIST-PROPERTY-NAMES ()).
DO i = 1 TO propertyCount:
   propertyName = ENTRY(i, hCP:LIST-PROPERTY-NAMES ()).
   MESSAGE "  "  propertyName hCP:GET-PROPERTY
(propertyName).

END.

MESSAGE "  Roles " hCP:ROLES.
```

Debugging configuration

- $Catalina_base/ablapps/abl-app-name/conf/logging-ablapp.xml
  - <logger name="org.springframework.security.oauth2" level="debug" />
  - <logger name="org.springframework.security.jwt" level="debug" />
  - <logger name="org.springframework" level="debug" />
  - <logger name="com.progress.appserv.services.security" level="debug" />

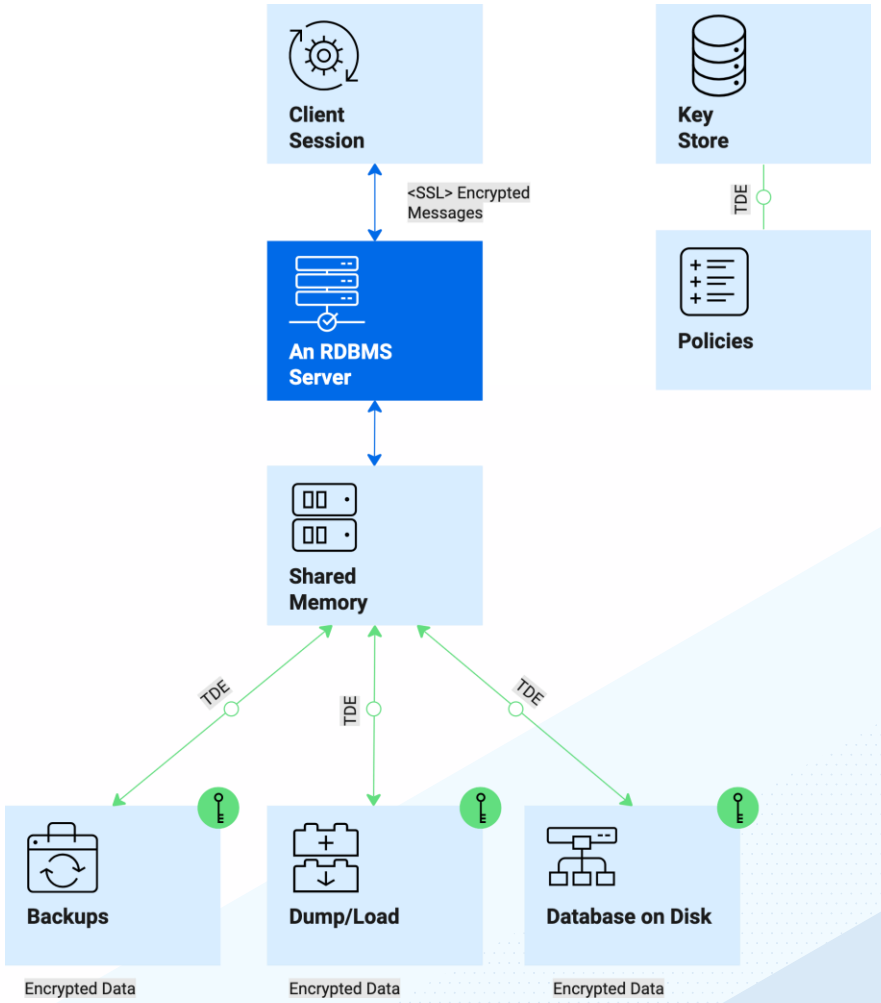
OpenEdge Advanced Security

- A collection of security capabilities including:
  - Transparent Data Encryption (TDE)
  - Dynamic Data Masking (DDM)
  - Hardware Security Module (HSM)
  - JSON Web Encryption (JWE)

Protecting Data at Rest

Transparent Data Encryption (TDE)

- Controls access to OpenEdge Database information stored at rest, including backups and binary dumps.
- At runtime, data is unencrypted in memory so that no changes to the application business logic, user procedures, or DBA management processes, are required
- Promotes data confidentiality using industry-standard encryption ciphers, security key protection and storage to help resist attacks.



Dynamic Data Masking (DDM)

Organizations must meet regulations and prevent sensitive information from being viewed by unauthorized users.

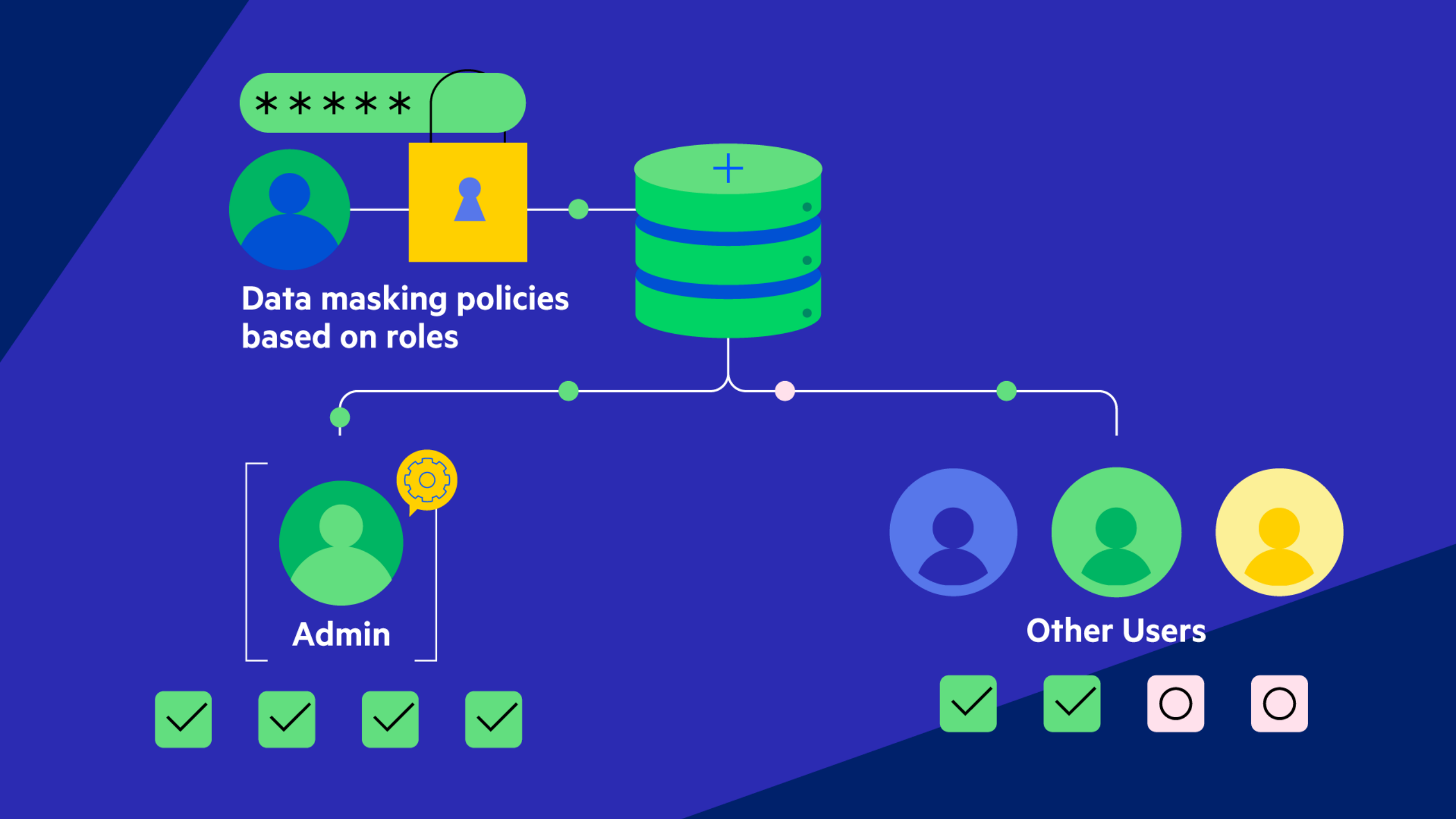
- ✓ No code changes
- ✓ No changes to underlying data
- ✓ Configuration-based
- ✓ High performance, high availability

Authorized

First Name	Last Name	Credit Card
Liam	Smith	4532 1234 5678 9012
Noah	Jones	6011 2345 6789 0123
Emma	Brown	5100 9876 5432 1098
Olivia	Johnson	3712 3456 7890 1234

Unauthorized

First Name	Last Name	Credit Card
Liam	Smith	XXXXXXXXXXXX9012
Noah	Jones	XXXXXXXXXXXX0123
Emma	Brown	XXXXXXXXXXXX1098
Olivia	Johnson	XXXXXXXXXXXX1234


*****
Data masking policies based on roles
Admin
Other Users

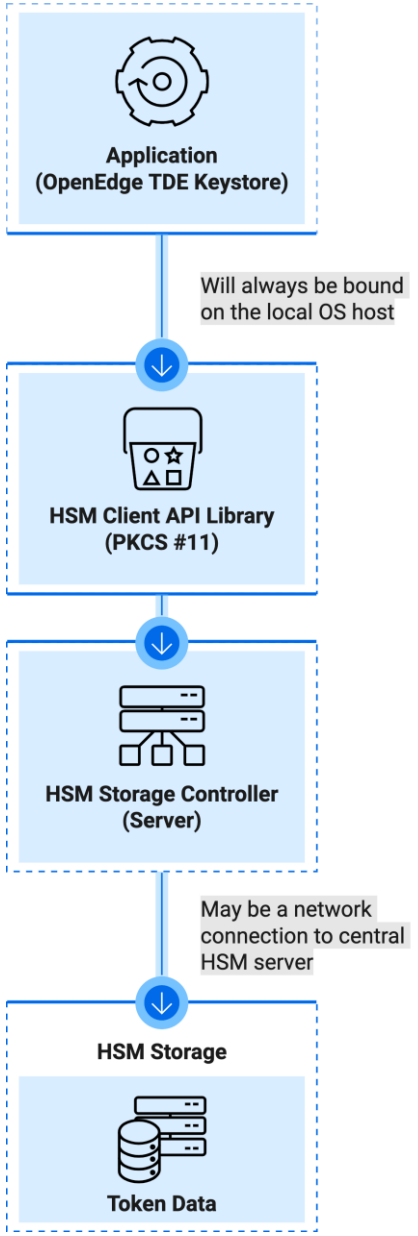
First Name	Last Name	Email	SSN	DOB	Password
Marisol	Everhart	marisol.everhart@example.com	###-##-6789	XXX-05-15	MASKED
Declan	Hawthorne	declan.hawthorne@example.com	###-##-4321	XXX-09-28	MASKED
Seraphina	Sterling	seraphina.sterling@example.com	###-##-9123	XXX-12-03	MASKED
Kellan	Carmichael	kellan.carmichael@example.com	###-##-3456	XXX-07-19	MASKED
Azura	Blackwood	azura.blackwood@example.com	###-##-1987	XXX-04-10	MASKED
Finnegan	Montague	finnegan.montague@example.com	###-##-7654	XXX-11-25	MASKED
Amara	Fairchild	amara.fairchild@example.com	###-##-3219	XXX-08-07	MASKED
Daxton	Ashford	daxton.ashford@example.com	###-##-7891	XXX-02-14	MASKED
Liora	Sinclair	liora.sinclair@example.com	###-##-1234	XXX-06-30	MASKED
Thaddeus	Harrington	thaddeus.harrington@progress.com	###-##-4567	XXX-10-22	MASKED

Dynamic Data Masking Key Features

- **Audit Events and User States:** You can use the audit events to track the DDM activities and changes, such as enabling, disabling, activating and deactivating DDM, as well as adding, modifying and deleting DDM rules.
- **AVM Support for DDM:** You can use the DDM authorization tags to grant or deny access to the sensitive data for different users and roles.
- **Dump and Load DDM Data:** Whether you're transitioning from development to production or any other scenario, this capability helps support the integrity of your DDM-enabled data.
- **Database User Notify Integration:** When you load DDM schema changes into a live database, OpenEdge uses its database user notification system to alert other connected clients of the change.

Hardware Security Module (HSM)

- An enterprise-scale physical computing device that:
  - Helps safeguard and manage digital keys
  - Performs encryption and decryption functions for digital signatures
  - Provides strong authentication and other cryptographic functions
  - Allows you to store all your keys on your server, where users may access them to do business tasks in a more secure location
- Numerous industries require the highest level of security when storing and using cryptographic keys. HSM supports this with:
  - Tamper-resistant hardware
  - Stored and protected keys made available to authorized users
  - Keys that do not need to be loaded into the web/application server memory



JSON Web Encryption (JWE)

- With JSON Web Encryption (JWE), users can communicate JSON-formatted data securely in a tamper-proof container
  - Enables the establishment of certificates that limit who can and cannot access applications via user recognition
  - Can be used for tasks like application login validation
- Standards to safeguard user identification in business applications enable organizations to:
  - Confirm who is who when trying to access and use varying business applications and data
  - Keep information visible to only those permitted to view it

Progress Supports Compliance with Security Regulations

- It ultimately is up to you to utilize the available security features provided by OpenEdge so that your application is compliant:
  - General Data Protection Regulation (GDPR)
  - European Union Directive on Data Protection (EU-DPD)
  - Payment Card Industry-Data Security Standard (PCI-DSS)
  - Sarbanes-Oxley (SOX)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - California Consumers Privacy Act (CCPA)

Démo TDE

Etapes pour encrypter

- prodb sports2000 sports2000
- prostrct add sports2000 encrypt_policy.st
- proutil sports2000 -C enableencryption
  - Br0wnbag! (Admin) 0nePr0gress! (User)
- proutil sports2000 -C epolicy manage area encrypt "Cust_Data" -Passphrase
- proutil sports2000 -C epolicy manage area update "Cust_Data" –Passphrase
- proutil sports2000 -C epolicy manage table encrypt "Pub.Family" -Passphrase
- proutil sports2000 -C epolicy manage table update "Pub.Family" -Passphrase

Démo DDM

Don’t Let This Be You

31%

Increase in cyber attacks year over year in **Europe**

30%

Of web application vulnerabilities, 30% were due to **security misconfigurations**

84%

Percentage of critical infrastructure incidents where initial access vector **could have been mitigated**

25.7%

Of the top 10 attacked industries, **manufacturing** received 25.7% of all incidents.

IBM, X-Force Threat Intelligence Index, 2024

Alors la Sécurité

- Facultative , Obligatoire ou Indipensable ?

URL et liens utiles

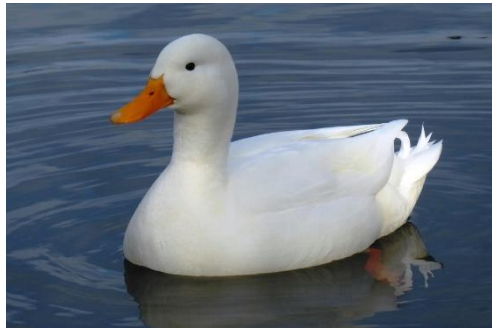
- https://github.com/lkieffer2002/PUG2025FR
- https://github.com/mabihan/keycloak-angular-multi-tenant
  - Image Docker avec Keycloak
  - A besoin d'un Dockerfile

```
FROM quay.io/keycloak/keycloak:15.0.0
COPY scripts/startup.sh /opt/jboss/startup-scripts/startup.sh
COPY scripts/create-client.sh /tmp/create-client.sh
```

- Sample with google oAuth2 : https://community.progress.com/s/article/Sample-for-PASOE-Support-for-JWT-and-OAuth-2-0
- https://community.progress.com/s/article/How-to-configure-PASOE-to-use-keyCloak-as-an-OAuth-2-0-authentication-server
- https://docs.progress.com/bundle/openedge-pasoe-oauth2-quickstart/page/Configure-PAS-for-OpenEdge-to-use-OAuth2.html

Questions ?

Qui a trouvé et pourquoi ?




Progress®