Progress

Bezpieczeństwo Aplikacji Biznesowych w OpenEdge 12.8

Piotr Tucholski

Sales Engineer

ptuchols@progress.com

Agenda

- Bezpieczeństwo ma znaczenie
- Jak Progress zabezpiecza Twoje aplikacje
- Zabezpieczenia w OpenEdge 12.8

Progress®

Wróg staje się mądrzejszy. Wspomagany przez sztuczną inteligencję staje się groźniejszy niż kiedykolwiek.

Progress®

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.**

SHODAN | Explore | Downloads | Pricing | http.title:"OpenEdge"

TOTAL RESULTS

288

TOP COUNTRIES

Brazil	53
Argentina	36
Netherlands	35
United States	35
Germany	17

More...

TOP PORTS

9090	228
9443	34
443	12
80	6
9595	2

View Report | Download Results | Historical Trend | View on Map

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwell

OpenEdge Explorer

62.182.12.41
ZAO Aquafon-GSM
Georgia, Sokhumi

```
HTTP/1.1 200
X-Content-Type-Options: nosniff
P3P: CP="NON CUR OUR IND STA"
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe
```

OpenEdge Management

200.110.133.46
sawyer.solutions4mobiles.net
IFX Networks Argentina S.R.L.
Argentina, Buenos Aires

```
HTTP/1.1 200 OK
Date: Thu, 20 Jun 2024 11:06:56 GMT
X-Content-Type-Options: nosniff
P3P: CP="NON CUR OUR IND STA"
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; script-src 'self...
```

OpenEdge Management

186.109.224.159
host159.186-109-224.telecom.net.ar
Apolo -Gold-Telecom-Per
Argentina, Formosa

```
HTTP/1.1 200 OK
Date: Thu, 20 Jun 2024 10:53:17 GMT
X-Content-Type-Options: nosniff
P3P: CP="NON CUR OUR IND STA"
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; script-src 'self...
```

The Security Landscape Is Changing

- Once upon a time, security was “interesting”
- Then customers started asking for it
- Then customers started demanding it
- Then the lawyers started demanding it
- Now the governments are getting involved – ENISA and CISA

  Provide advices, promote digital safety

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?"

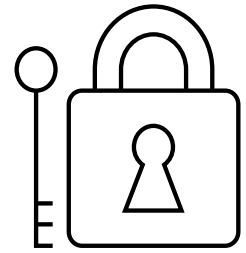
Wszyscy odpowiadamy za bezpieczeństwo naszej aplikacji.

Jak Progress Zabezpiecza Twoje Aplikacje

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

How We Improve Security



- Regular scanning for vulnerabilities
- Security Vulnerability Mitigation
  - In the many open-source libraries when vulnerabilities are identified: update or replace them
  - In our own code when a security scan finds an issue
- OE12 Features: HSM, OAuth2, SAML, Dynamic Data Masking, ESAM, etc.
  - You need to get to OpenEdge 12.8 for the full set
- New (roadmap) Features

ESAM - Securing OE Executables & Libraries

- “External Security Administration Manager” (ESAM), starting with OE12.6
- “Single Source of Truth” - ensures exe’s and libraries are used from a registered, secured, and trusted location (DLC path) for all OE components
  - The DLC path is registered at OpenEdge install time
- Benefit: prevents attackers from directing OpenEdge activities to resources outside the directory scope of the OpenEdge installation

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

Zabezpieczenia w OpenEdge 12.8

OpenEdge 12.8 Security Features

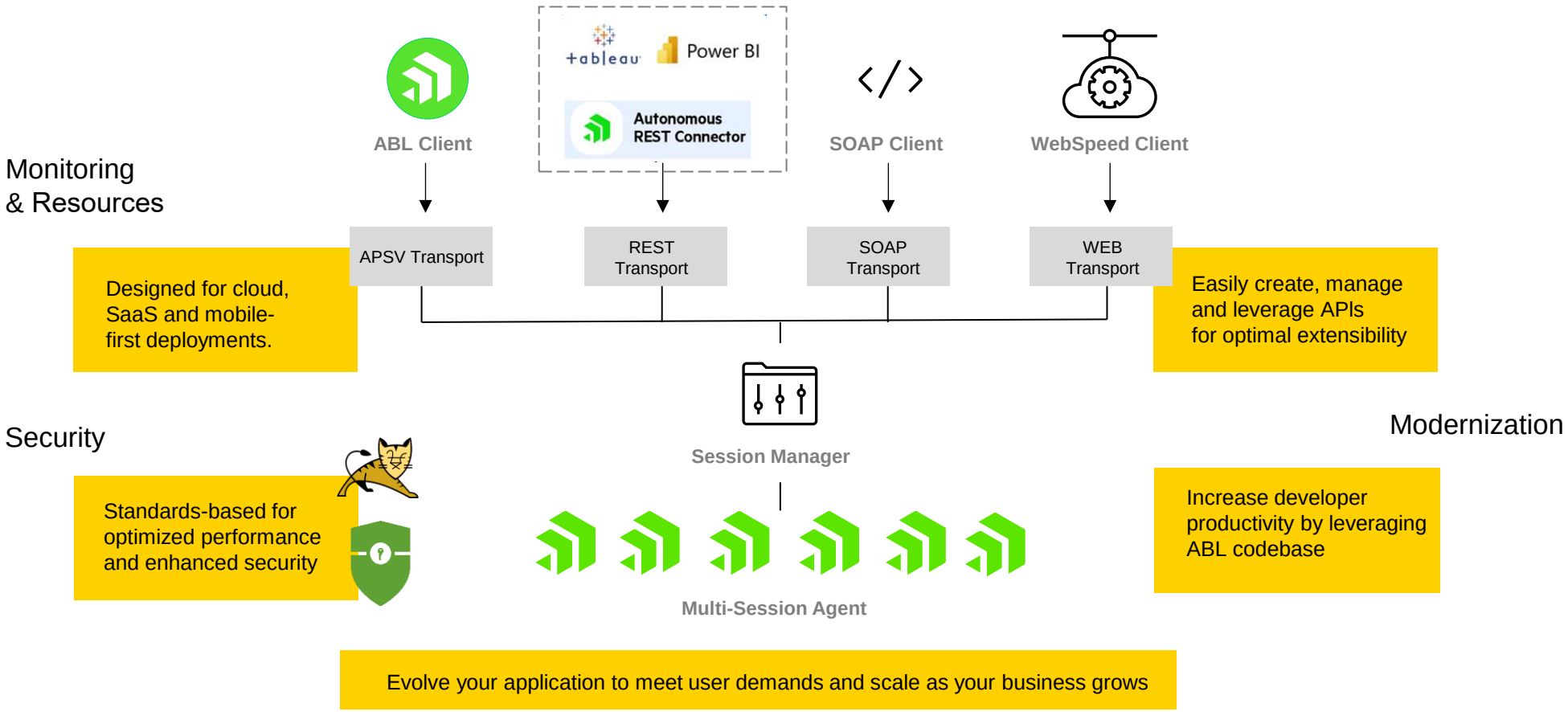
- Progress Application Server for OpenEdge (PASOE)
- OpenEdge Authentication Gateway
- OpenEdge Advanced Security
  - Dynamic Data Masking (DDM)
  - Hardware Security Module (HSM)
  - JSON Web Encryption
  - Transparent Data Encryption (TDE)*

PAS for OpenEdge (PASOE)

- Classic Appserver discontinued since March 2019
- 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

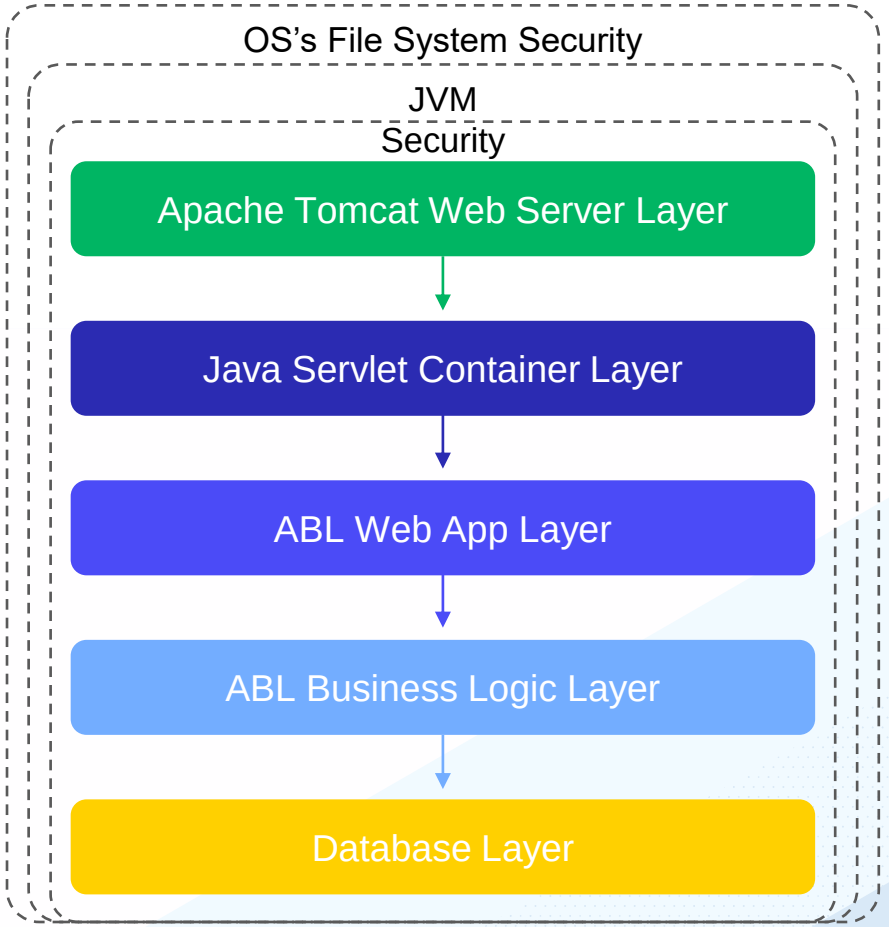
PAS for OpenEdge (PASOE) - architecture

Scalable, Secure and Standards-Based



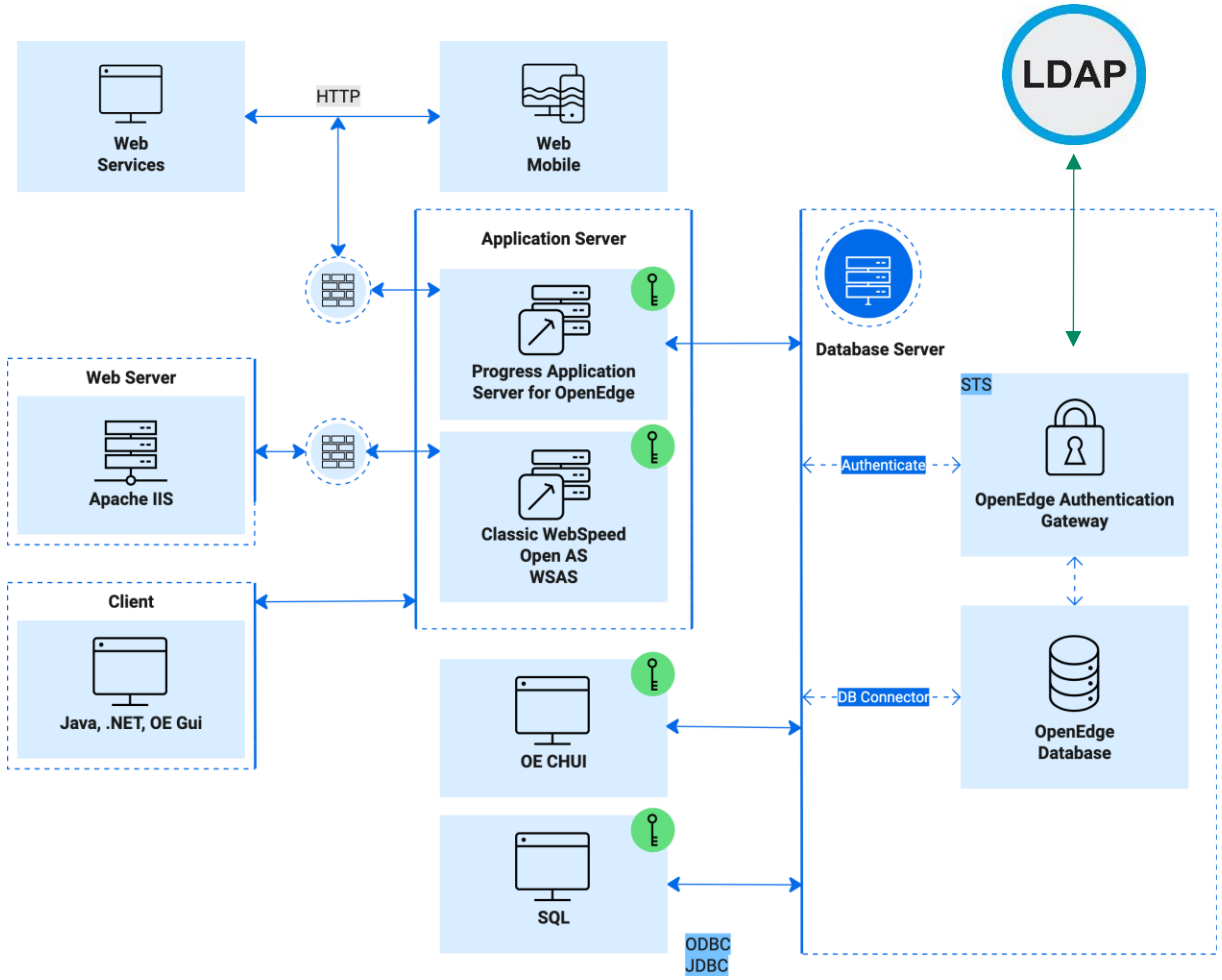
PAS for OpenEdge Security Stack

- Contains 5 layers of protection
- Each layer supports the layers below it from direct attacks and can be configured independently
- Capabilities include:
  - HTTPS TLS
  - Java servlet authentication and authorization
  - Spring-based authentication and authorization
  - Validation of OpenEdge C-P objects
- Java Security Manager, JSSE (Secure Socket Ext.), Java class loader sec., etc.



OpenEdge Authentication Gateway

- 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



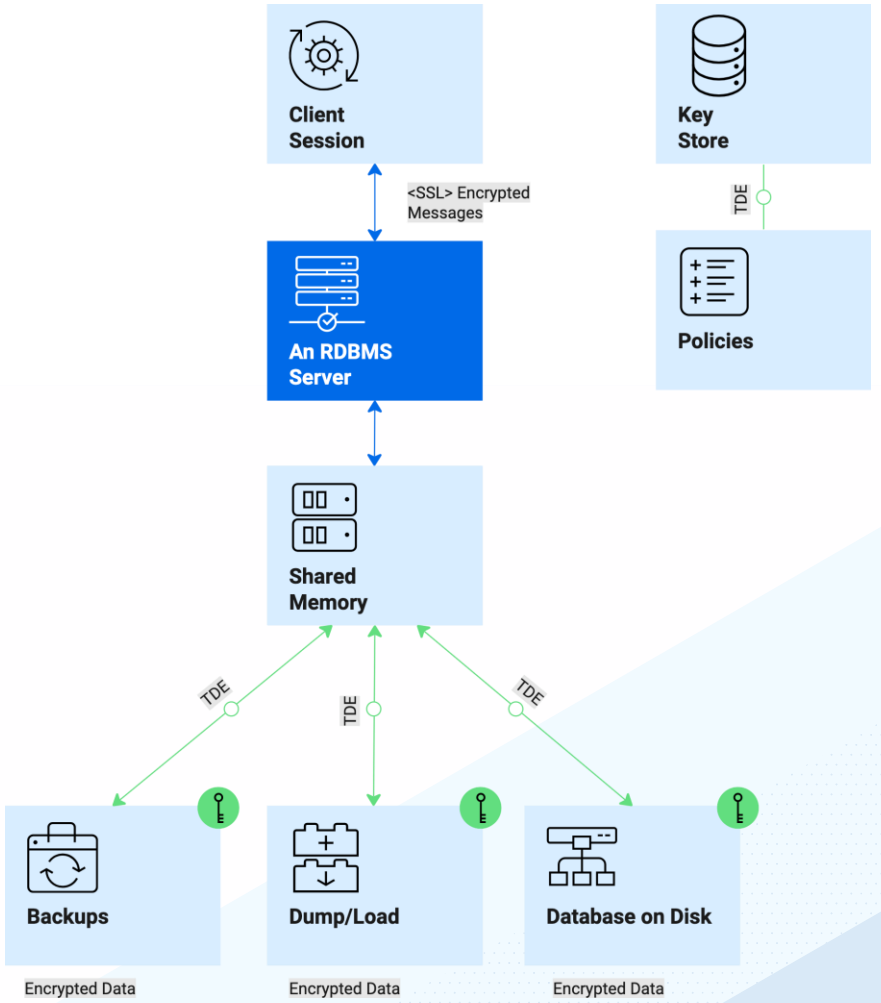
OpenEdge Advanced Security

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

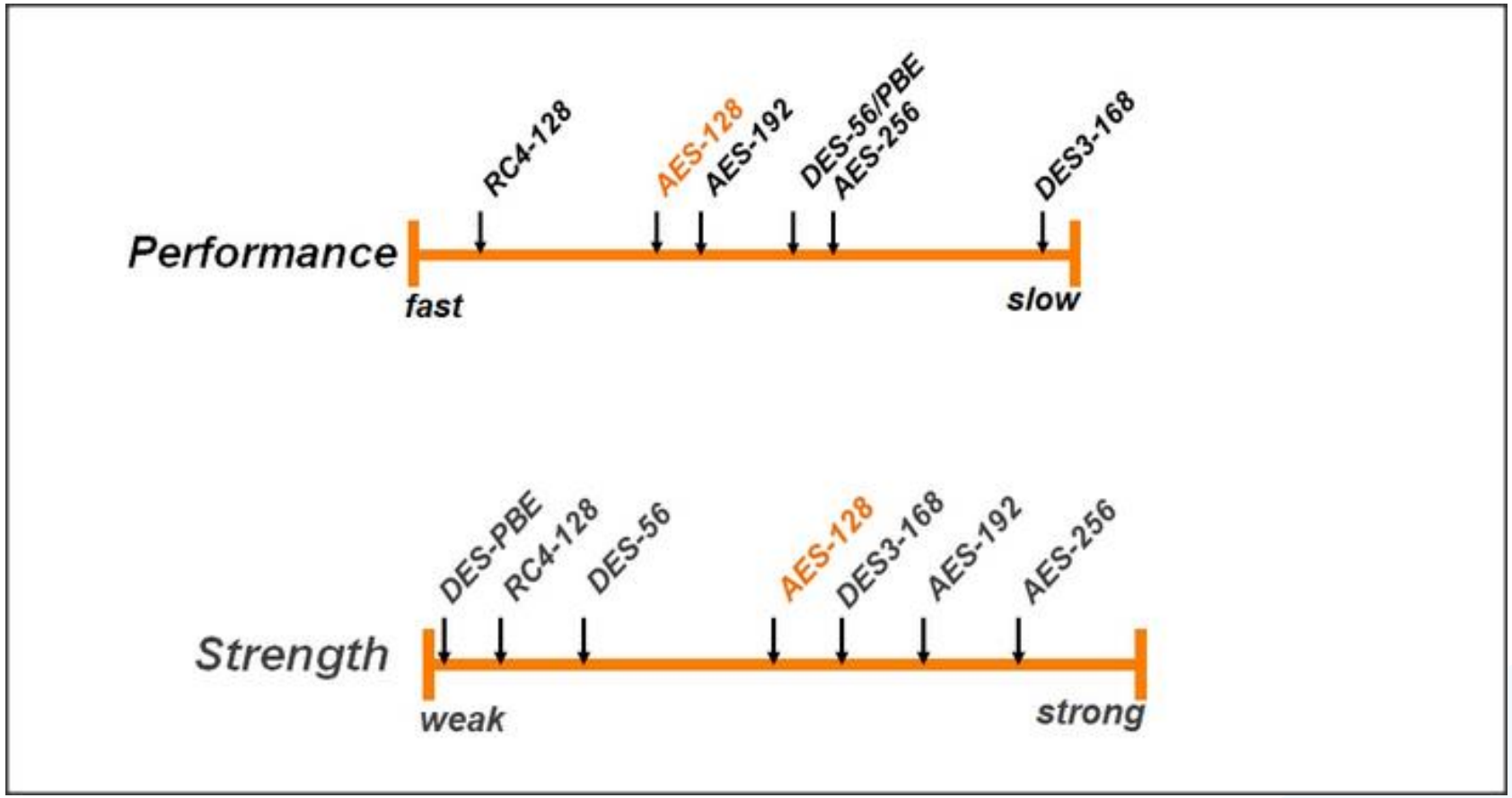
Protecting Data at Rest

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.



TDE – The Cipher



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

Dynamic Data Masking - example

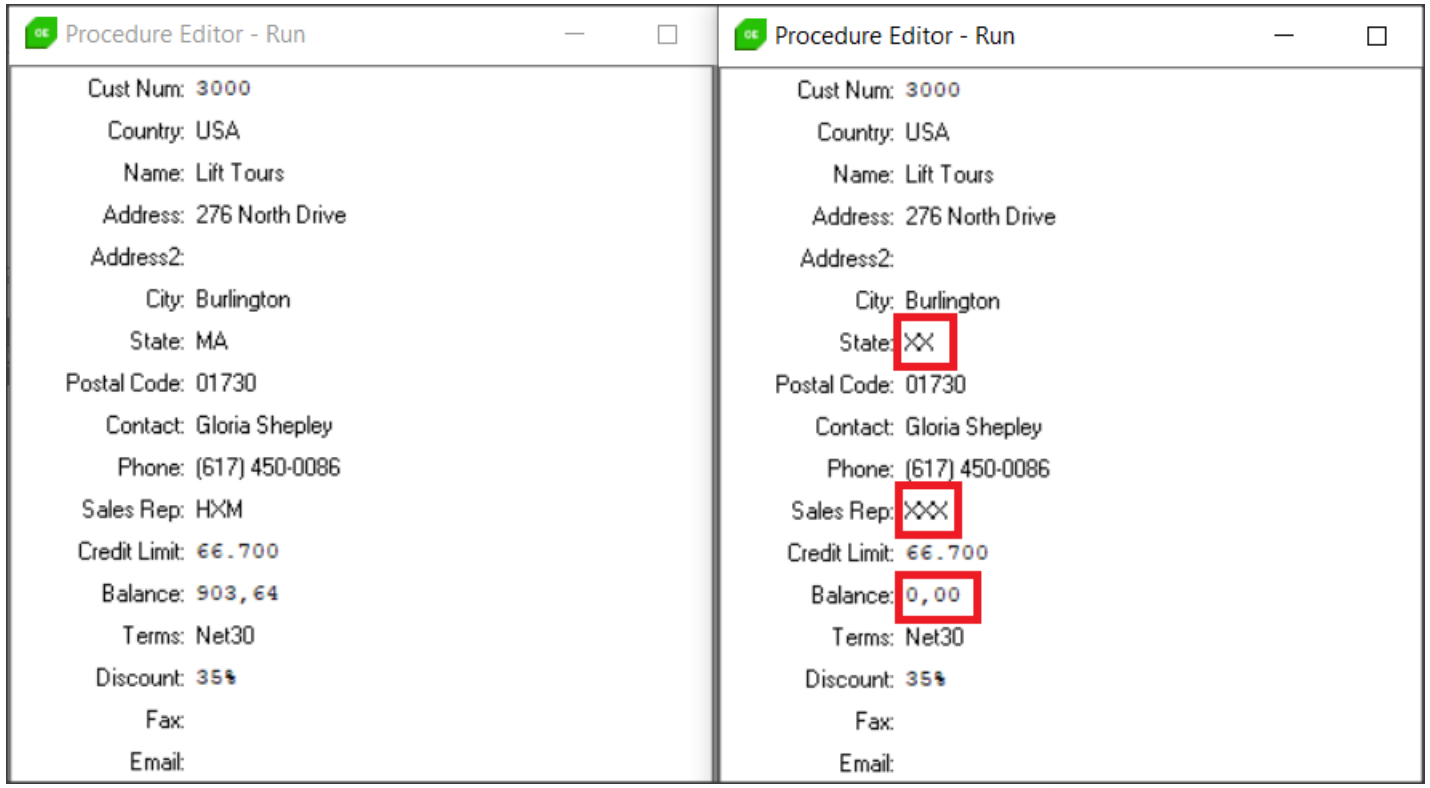
Association authorization tag with the role.

```
USING OpenEdge.DataAdmin.*.

VAR DataAdminService service.
VAR IAuthTag oTag.
VAR LOGICAL lReturn.

service = NEW DataAdminService (LDBNAME("DICTDB")).

     oTag = service:NewAuthTag("#DDM_SEE_ContactInfo").
     oTag:RoleName = service:GetRole("myRole"):Name.
     oTag:description = "To see contact info".
     lRETURN = service:CreateAuthTag(oTag).
```

Defining the mask.

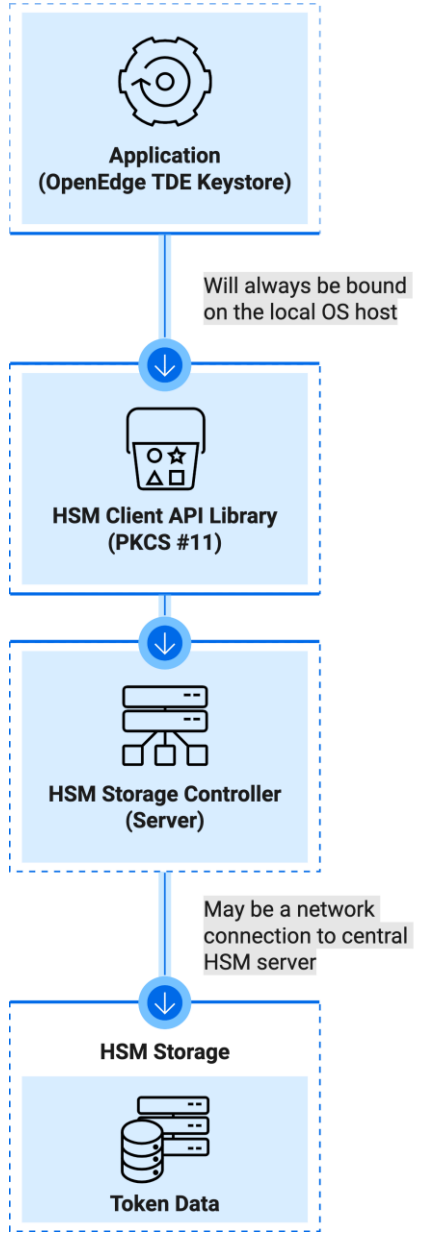
```
USING OpenEdge.DataAdmin.DataAdminService FROM PROPATH.

DEFINE VARIABLE service AS DataAdminService NO-UNDO.
DEFINE VARIABLE lResult AS LOGICAL NO-UNDO.

service = NEW DataAdminService(LDBNAME("DICTDB")).
lResult = service:setDDMConfig("Customer","Balance","D:","#DDM_SEE_ContactInfo").
```

Dynamic Data Masking - example



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)


Progress®