Progress® OpenEdge®

OpenEdge Advanced Security

WHITEPAPER

Satisfy industry demands, enhance application and data security, and meet regulatory compliance with OpenEdge Advanced Security.

Applications that are trustworthy and safe are essential for enterprises in today's digital world. As a result, there are strict security requirements for all business applications across a wide range of industries and enterprises globally.

Security is top of mind for many organizations, especially if they are in highly regulated industries such as public sector, finance, insurance, and healthcare. Ensuring that their mission critical information is secure and protected at all times is a must for their business operations.

With these customer concerns in mind, Progress OpenEdge introduced Advanced Security. This package is designed to address not only data encryption but also surrounding technologies such as a secure key store via a Hardware Security Module and a standard encrypted data exchange method via JSON Web Encryption.

What is OpenEdge Advanced Security?

Advanced Security allows customers to have the tools they need to strengthen the security posture of their OpenEdge applications. This product includes hardware security module (HSM), JSON web encryption (JWE), and transparent data encryption (TDE). These tools together are a superpower in application security for your critical applications.

By offering solutions for security efforts, OpenEdge Advanced Security provides the additional level of security that enterprises need. Let's take a deep dive into the three main features within the OpenEdge Advanced Security package:

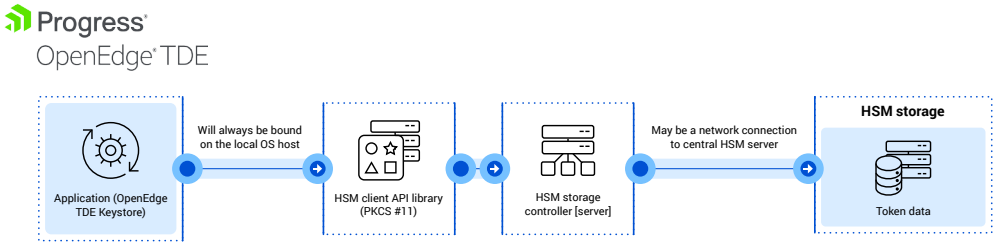
1. Hardware Security Module (HSM)

Hardware Security Module (HSM) is an enterprise-scale physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, and provides strong authentication and other cryptographic functions.

This feature allows you to store all your keys on your server, where users may access them to do their vital business tasks in a secure location.

Numerous industries require the highest level of security when storing and using cryptographic keys. HSM accomplishes this with:

- Tamper-resistant hardware
- Stores and protects keys and makes available to authorized users
- Keys do not need to be loaded into the web/application server memory



2. JSON Web Encryption

With JSON Web Encryption, users can communicate JSON-formatted data securely in a tamper-proof container. The ability to recognize users enables the establishment of certificates that limit who can and cannot access applications. This can be utilized for tasks like application login validation.

There are standards to safeguard user identification in business applications. These measures would be used by organizations to:

- Confirm who is who when trying to access and use varying business applications and data
- Make sure that information is only visible to those who are permitted to view them

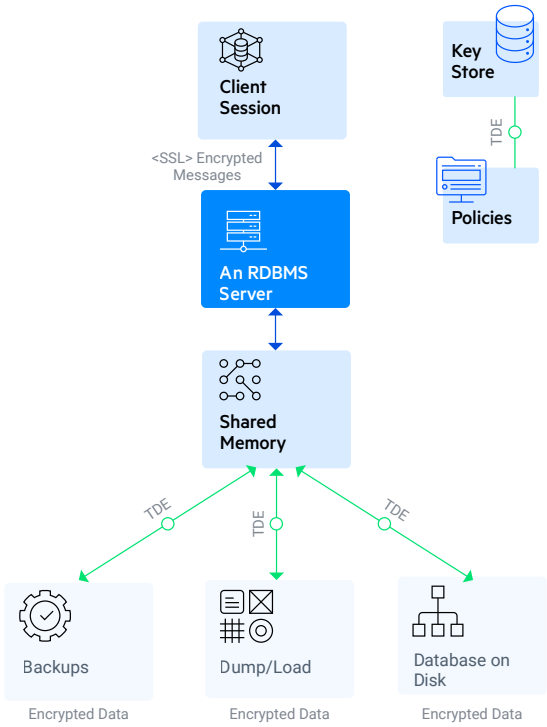
3. Transparent Data Encryption (TDE)

OpenEdge Transparent Data Encryption helps you provide privacy for sensitive data in your application, whether your business is in retail, financial services, healthcare (HIPAA requirements), or any other industry that handles sensitive data. These requirements drive many software initiatives related to sensitive data. With use of this OpenEdge feature, your data will be protected on disk, in backups, and even in binary dump files. Best of all, OpenEdge Transparent Data Encryption requires no changes to your application, user procedures, or DBA management processes. This means the costs to your production operation are truly minimized.

Growing data confidentiality needs are reflected in growing TDE security requirements. TDE provides data confidentiality through the ability of its industry-standard encryption ciphers and security key protection and storage to resist attacks.

Key capabilities include:

- Controlling access to stored private data, or “at rest,” is at the core of the OpenEdge TDE solution.
- Execute at full speed with less than 2% performance degradation while encrypting and decrypting.



Interested In Learning More?

OpenEdge Advanced Security is available for OpenEdge versions 12.6 or later. With this security add-on, you can feel even more secure with your Progress OpenEdge applications.

Check out **Advanced Security** and get started today!

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (NASDAQ: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to build the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com

/progresssw
/progresssw
/progresssw
/progress-software
/progress_sw_

Progress