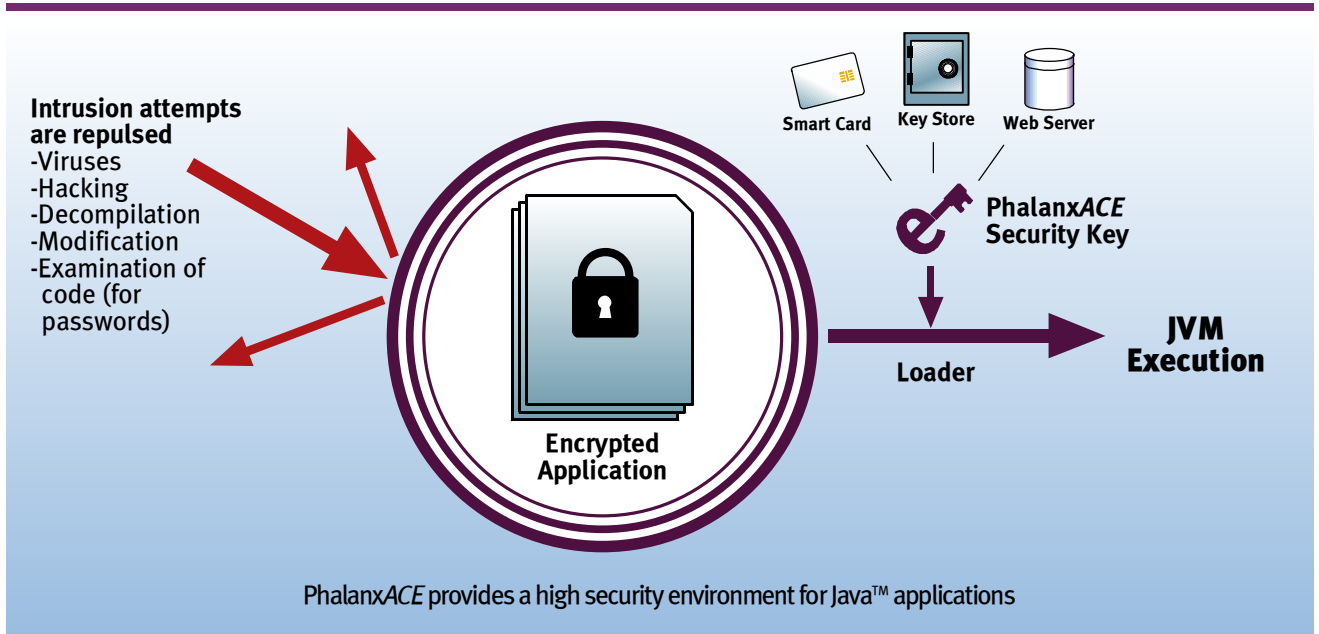


PhalanxACE

Phalanx Application Code Encryption [ACE] provides a high security environment for Java™ applications by encrypting the compiled code – a vulnerable yet often overlooked security area. PhalanxACE stops viruses, hacking, decompilation, modification and examination of the binary code thereby preventing malignant applications, access to passwords and sensitive information, circumvention of license systems and breach of intellectual property rights



PhalanxACE is designed to provide security, virus protection, access control and intellectual property protection. In today's pervasive computing and networked environments security has become the number one concern.

ACE focuses on an often neglected area: the compiled code. The compiled code itself can be the target of hacking attempts in the form of disassembly, examination and modification.

PhalanxACE prevents unauthorized execution, disassembly and examination of compiled Java™ code, thus giving protection in six main areas:

▶ ACE prevents execution of the code unless user has access to the key.

▶ Prevents hacking into the software that would circumvent license restriction and make illegal copies.

▶ Stops access to the dissembled source code and algorithms within the application, thus protecting the intellectual property of the company.

▶ Protects information within the application that could otherwise be used to gain access to databases and other computer systems.

▶ Provides virus protection. After infection an application will be prevented from executing.

▶ Stops tampering with compiled application code.

PhalanxACE works by encrypting the entire application. The application is decrypted on the fly as it is loaded into memory.

Without access to the key it is impossible for unauthorised parties to execute an application or even gain access to its binary code.

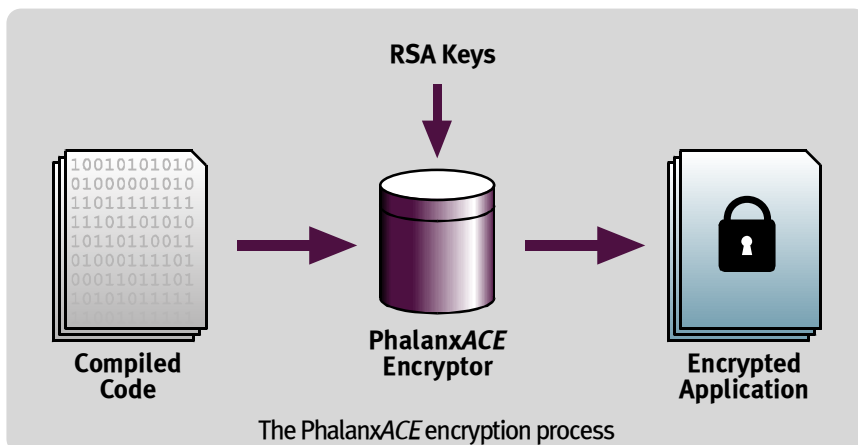
A smart card, key store or a central control server serves as a repository for the encryption key.

Who should use PhalanxACE?

▶ Applications managing high security or sensitivity information such as in finance, health, government and military.

▶ Companies wishing to protect their applications from hacking or decompilation to prevent illegal copies or access to proprietary algorithms.

ACE is used on Endeavour's Payment Gateway application to provide a level of protection that is unprecedented in payment gateways.



Web: www.e-i-b-s.com Email: info@e-i-b-s.com