

Security protection component for Engineering Applications

The Client

The customer is a business unit of a NYSE listed company, which is a leading oilfield services company supplying technology, project management and information solutions that optimize performance for their customers working in the international oil and gas industry.

The Challenge

The project involved development of protection component for customer's services engineering applications.

The Solution

The protection component provides security to the Well Services Engineering Applications [WSEA]. It provides WSEA with the capability to check if the user has the requisite authorization to access the given application. Authorization of the user will involve verification of the user's details against the LDAP server. Once authorized by the WPC, the user would gain access to WSEA in a secure manner. The protection component has been designed and developed as a lightweight, non-visual COM server that will be digitally signed to ensure data integrity. It is signed with a certificate issued by company's CA and the certificate is validated against the root CA for issuer name and subject name. When invoked, the protection component first ensures that the user has been logged in with Entrust. Then the component will determine whether the user is connected or not to the network. If connected, the user is verified against the LDAP criteria provided. If the user is not connected to the network, the protection component will locate the encrypted document, decrypt it, verify the expiry date and time and will then authorize the user to access the WSEA

The Benefits

A comprehensive security system was delivered to the customer that will check for authentication, authorization and integrity. Authentication, authorization provided using entrust and LDAP. Integrity using PKI concepts [public key private key encryption].

The Technology